정보 윤리 소책자

목차

(*)는 정보 윤리 디지털 비디오 소품 집 2, 그렇지 않으면
정보 윤리 디지털 비디오 소품 집 3의 내용입니다.

본 교재는 과학 연구 비용 (20500823)의 지원을 받아 개발.

비밀번호 잊어버렸으면 어떻게하지?

【 목표와 포인트】

1. 패스워드의 이용과 관리 방법에 대해 이해한다.

   - 패스워드의 관리 방법에 대해 이해한다.
   - 패스워드의 암호화와 통신의 암호화의 차이를 인식한다.

2. 본인임을 인증하는 ID와 그렇지 않은 ID를 구별하여, 본인 인증에 사용하는 ID 관리의 중요성에 대해 배운다.

   - 대학교 컴퓨터 시스템의 ID, 패스워드 발급 절차는 왜 웹이나 메일을 이용하지 않는지를 이해한다.

3. ID와 패스워드로 인증하는 것의 이점과 문제점에 대해 생각한다.


이런..
이럴 줄 알았으면, 더 간단한 걸로 했을 텐데....
안됐네 카즈야...
정보센터에 연락해보는게 좋지 않을까?
귀찮을 텐데..


그런말 하지 말고 그냥 빨리 연락해!
번.호.아...!!!
잠깐.. 잠깐만... 이게 확실해!!


포기
그만 두시지..
비밀 번호가 다릅니다
알았어.. 직접 정보센터에 물어보겠어..
XXXX-XX-XXXO
반짝!
띠..띠..띠..
뚜..뚜..뚜뚜
띠띠.. 띠..
앗!


자... 잠깐...!! 카즈야...!! 지금 뭐하는거야!!
뭐..야... 정보센터에 직접 메일 보내려고 했지?
안돼.. 핸드폰으로 연락하면...
메일도 학교 메일이 아니면 안 돼고!


그런데 학교 메일을 쓸 수 없어서 좀 곤란하단 말야...
아, 그럼 내 메일로 보낼래?
아... 안돼!! 이화..


이화 메일로 카즈가 보내는 것도 안돼!
알았어! 직접 전화할께!
전화도 똑같아.. 안돼!!
빠.직...
뭐.. 뭐야....
그게말야..


이렇게 중요한
패스워드와
같은경우는
본인이 직접가지
않으면 안돼
전화를 걸면
목소리 만으로
본인인지
알수가 없잖아..
그래서
직접 본인이
정보센터에
가야해


알았어...
잘~
다녀와~


저기..
실례합니다..
패스워드를
잊어 버렸는데
알 수 있을까요?

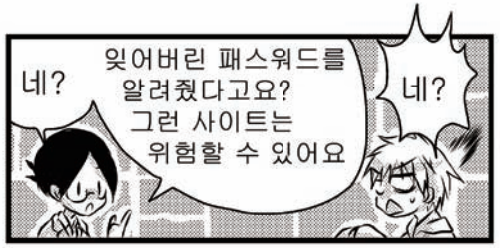

정보센터는 패스워드를
관리하고 있지만,
학생의 패스워드는
모릅니다.
재발행은
가능해요
네?
재발행이요?
그런데, 정보센터면
패스워드를 알고
있지 않나요?


패스워드는
본인 이외에는 몰라요.
우리 직원이 알게 되면
문제가 생길 수 있어요.
아..
네...
재발행
이요...

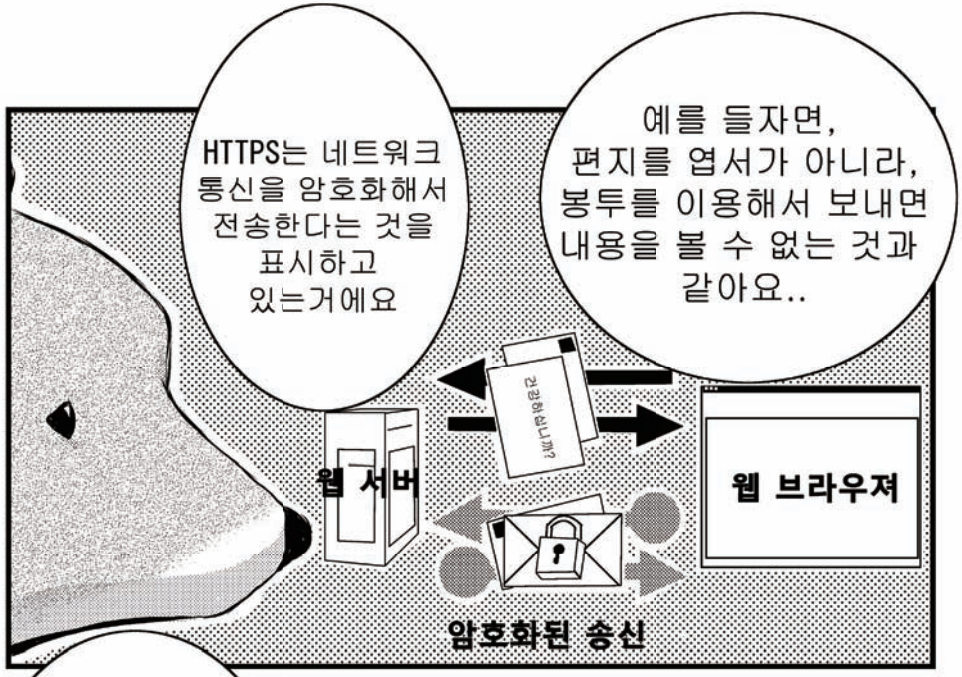

네, 재발행은
가능해요.
재발행하려면
학생증이 필요한데,
가져오셨어요?
아..
학생증이요..
네..


미도리
카즈야..
네~


카즈야군은
언제부터
패스워드를
잊어 버린거에요?
네?
그게..
언제부터
인지는...
거기다
패스워드
재발행을
너무 쉽게
생각하는거
아니에요?
잠깐!
카즈야군!
패스워드가
뭐라고
생각하는
거에요?



정보센터처럼 많은 사람의 개인정보를 관리하고 있는 곳에서는 개인정보보법이나 보안정책에 따라 관리하지 않으면 안돼요..

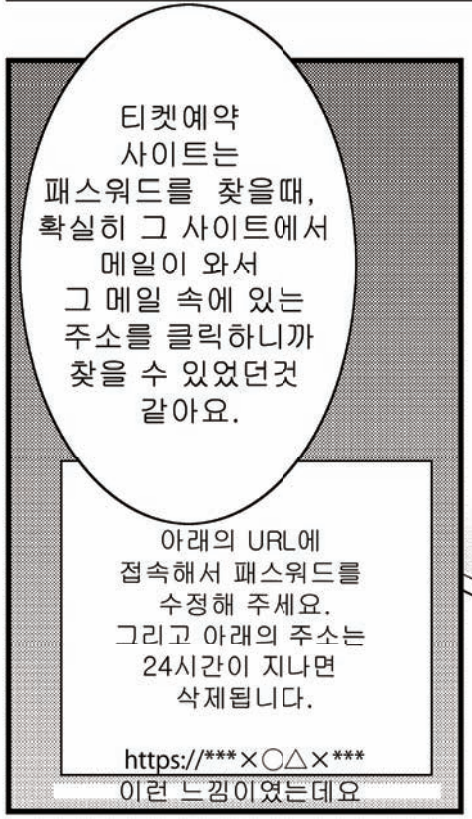


그러나, 시스템이 패스워드를 어떻게 관리하고 있는지는 또 다른 이야기에요

암호화된 패스워드는 원래 시스템에 기록되어 있어요

그러니까, 예를 들어 관리라자고 하더라도 해독할 수가 없어요


아..
알겠어요..
그렇지만..
대학의 패스워드도,
메일이나 웹을 이용하면
더 간단히 찾을 수 있지
않을까요?
패스워드 재발행
학생번호와
메일주소를
입력해주세요
이런 느낌


티켓예약
사이트는
패스워드를 찾을때,
확실히 그 사이트에서
메일이 와서
그 메일 속에 있는
주소를 클릭하니까
찾을 수 있었던것
같아요.
아래의 URL에
접속해서 패스워드를
수정해 주세요.
그리고 아래의 주소는
24시간이 지나면
삭제됩니다.
https://***×○△×***
이런 느낌이였는데요


카즈야군은
경험이
많은 것
같네요...


?
그건, 취급하는
정보의 종류에
달렸어요


티켓예약 사이트
같은 곳에서 정보를
주고 받는 것은
메일이나 웹에서
받는게 더 편할지도
몰라요..
그렇지만, 학교나
은행, 병원에서
처리하고 있는 정보는
예를 들어, 성적이나,
예금, 병명 등과
같은 정보는..
예약할때,
증명서를 보일
필요는
없으니까요
안전하게
관리하지
않으면
안 되겠죠?


아.....


아...
그런것
같아요..
그렇죠?

간단한 비밀번호로 중대한 사건!

【 목표와 포인트】

1. 패스워드의 중요성과 그 결정 방법에 대해 이해한다.

   - 패스워드가 해킹 당하면 어떤 피해를 입을 가능성이 있는지 이해한다.
   - 패스워드는 보통 어떤 방법으로 해킹 당하는지 이해한다.
   - 안전한 패스워드를 어떻게 정하는지 이해한다.

2. 시스템적으로 좋은 패스워드를 선정해도 약점이 있으면 해킹 당한다. 소셜엔지니어링이나 다른 시스템간에 같은 패스워드를 설정하는 문제에 대해 이해한다.


그래? 근데 자주 있는 일이, 자기 생일이나 전화번호나..
그리고... ID랑 비밀번호를 똑 같이 한다거나..


그게..
ID를 알아내면 비밀번호도 ...
혹시 이화~ 너 비밀 번호가...
생일이라던가?!

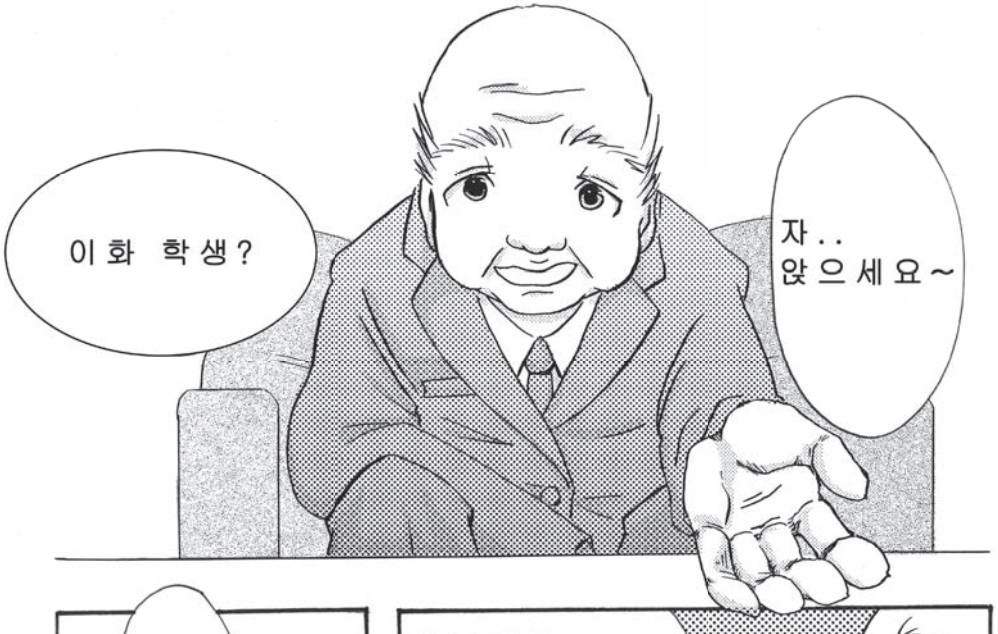

그.... 그건... 아냐!!
음... 그래도 조심해야할꺼야~!
안녕~~


아무래도 비밀번호는 변경해야겠다
ID또는 비밀번호가 틀렸습니다.
OK


아…
뭐야~
방금전까진
됐었는데!
아…
비밀
번호는
맞는데!
뭐지.
아…
아…
나도
정보센터에
가야만
하나….
아…
왜 바뀌지..


긴급호출
경제학부
리카학생
실례합니다~
방금 비밀번호를
쓸 수 없게
됐는데요..


잠깐
안으로
들어
오시겠어요?
아..
이화씨
네?
무슨일...
무슨일
이세요??


이화 학생?
자..
앉으세요~

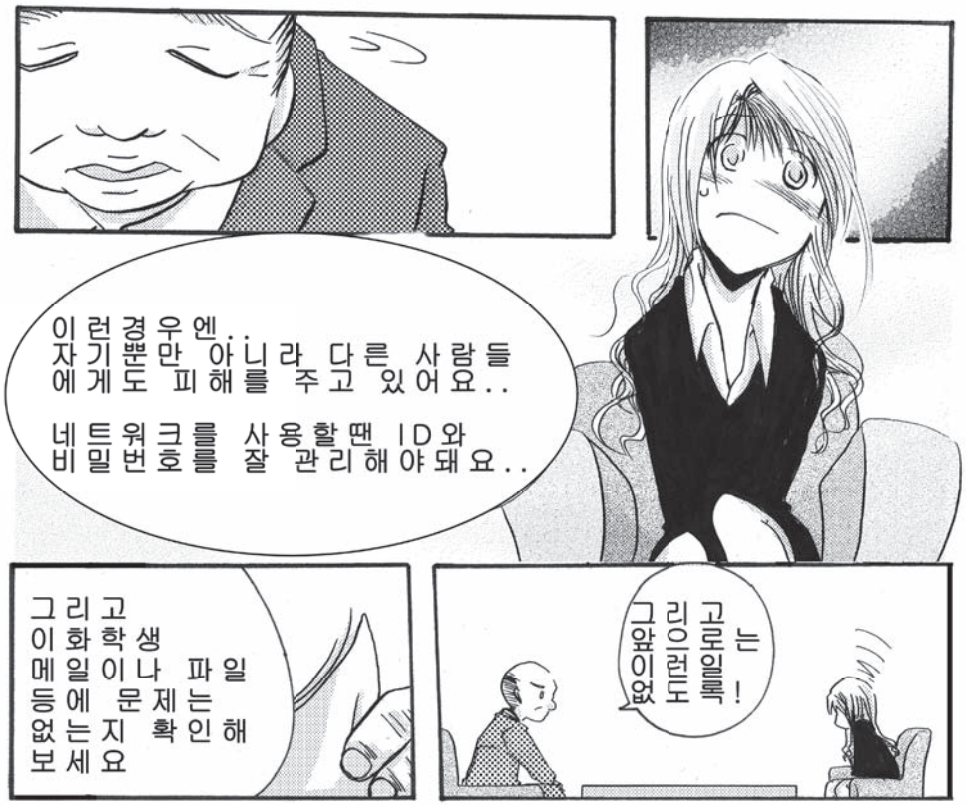

네..


방금전에
이화학생 ID를
정지 시켰어요.
네!?
정.지.
라구요?
무슨 말씀
이세요?

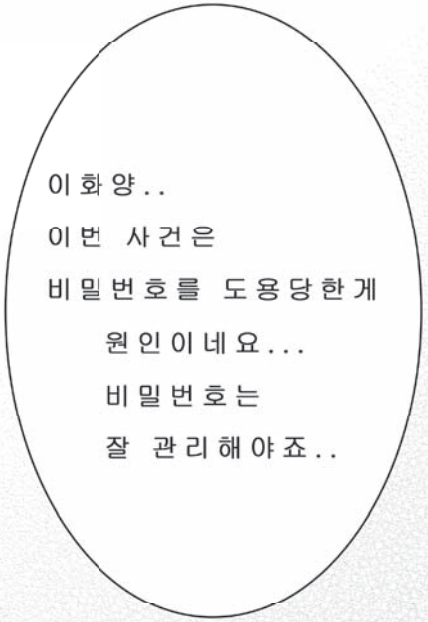

사실, 방금전에 삼우교육대학교에서
연락이 왔어요. 이상한 불법엑세스가
있다는 연락이 와서 조사를 해보니,
이화 학생의 ID가 쓰였어요.
그래서 일단 정지를 시켰습니다.
불법
엑세스요
?!
무슨
말씀인지
잘모르겠
어요..


제..
ID가
도용
됐다구요?
이화학생의
ID와
비밀번호를
훔쳐서
악용한것
같아요.
이화 학생이
한게 아니라면
누군가가
학생 ID를
도용한거네요..
어머..
이화양..
사태가 꽤
심각한 것
같아요?

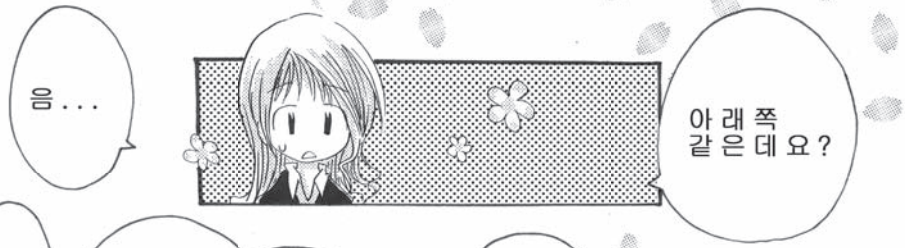

접수처
ID나 비밀번호가
적힌 종이를 잃어
버렸다거나..
뭔가 짐작되는
일은 없어요?
특히
없는데요
쉬운
비밀번호
였다거나
다른사람
에게 가르
쳐준적은?
아..
그건..
역시..
누군가가 이화학생 ID를
사용해서 메일이나 파일을
읽어 봤을지 몰라요.
사실은
이틀전쯤에
같은 시간에 다른 두
기계에서 ID가 이용된
기록이 있어요.
아.. 그런일이...
저 어떻게 해야하죠?


이런경우엔..
자기뿐만 아니라 다른 사람들에게도 피해를 주고 있어요..
네트워크를 사용할땐 ID와 비밀번호를 잘 관리해야돼요..
그리고 이화학생 메일이나 파일 등에 문제는 없는지 확인해 보세요
그리고는 앞으로는 이런일이없도록!


네~ 조심하겠습니다

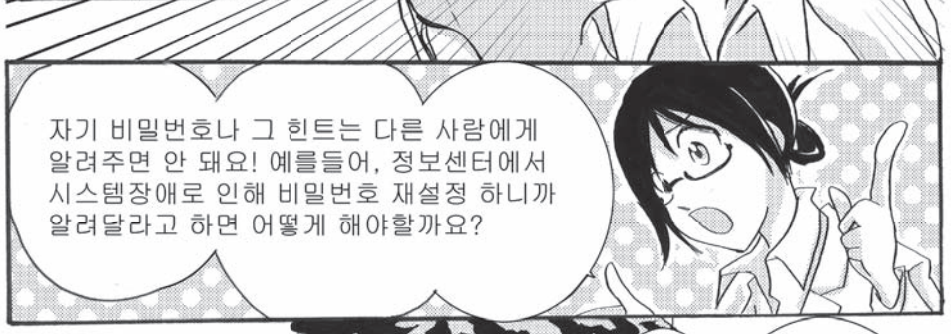

이화양..
이번 사건은
비밀번호를 도용당한게
원인이네요...
비밀번호는
잘 관리해야죠..


네~ 잘 알겠습니다!
그럼, 문제하나 내볼까요?
둘중에 어떤 비밀번호가 좋을까요?
rika1130
R1i3A1KO
맞춰 보세요


음...
아래쪽 같은데요?


딩동~
비밀번호가 도용될 수 있는 방법을 알아보면,
우선 개인적인 정보에서 예를 들어 ID나 이름, 생일 등이 있어요.
생일은 학생증이나 블로그 같은곳에서 알아낼지도 모르죠..
또한, 사전에있는 단어를 추측해서 비밀번호가 될 가능성이 있는것을 조합해 보는 경우도 있어요
그러니까.. 좋은 비밀번호 설정은...
개인적인 정보는 사용하지 않고
사전에 있는 단어는 쓰지 않는다!
그리고 길고 대문자와 소문자 숫자를 섞어서 쓰는것입니다.
그래서 위쪽의 비밀번호는 적당하지 않아요
rika -> 이화의이름

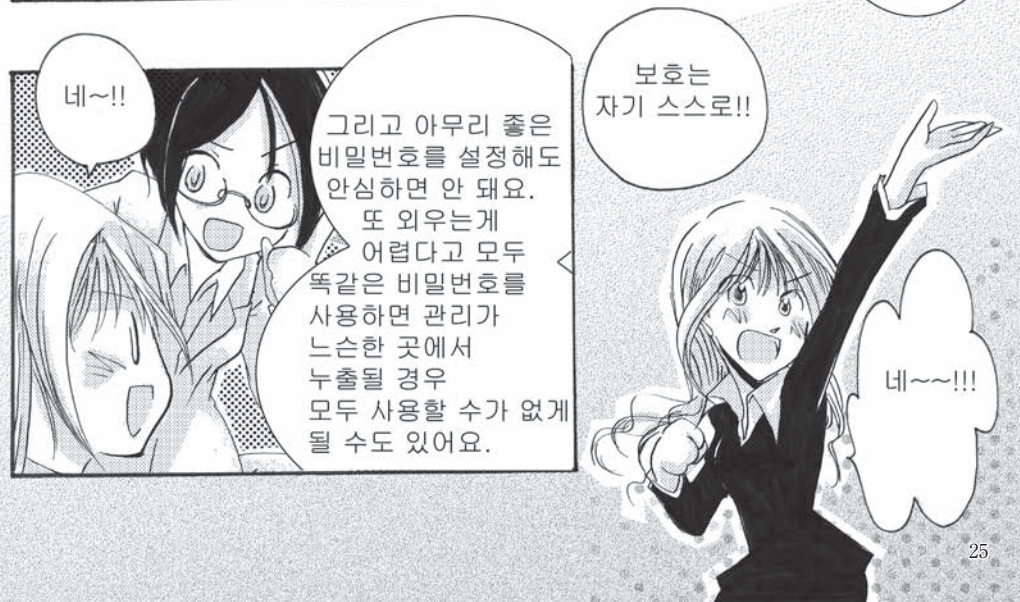

알고는 있었는데요.
제가.. 건망증이
심해서 외우기 쉽게
ID와 똑같이...
안 돼!
안 돼!


자기 비밀번호나 그 힌트는 다른 사람에게
알려주면 안 돼요! 예를들어, 정보센터에서
시스템장애로 인해 비밀번호 재설정 하니까
알려달라고 하면 어떻게 해야할까요?


센터직원
이면..
알려줄것
같은데..
그건..
안 되는
거죠?
맞아요!!
절대로 가르쳐 주면 안 돼요!
시스템장애인척하며
비밀번호를 알아내는 방법
등으로 비밀번호를 부정하게
취득하는 수법을
소셜엔지니어링
(Social Engineering)
이라고 해요.


아무리 좋은
비밀번호도 남에게
그냥 알려주면
끝이에요...
네....
이번엔 이화양의
비밀번호가 도용
당해서
그 ID로 삼우교육
대학교의 시스템이
공격을 받았어요.


그건 [부정엑세스 행위금지 등에 관한 법률]
에서 금지되어 있는 위법행위에요.
이화양은 피해자이긴 하지만 가해자이기도해요
비밀번호가 도용당하면 부정엑세스 뿐만
아니라 다음과 같은 심각한 문제를 가져올
수도 있어요.
- 부정엑세스
- 넷옥션 사기
- 취업취소등의 허위메일
- 게시판에서의 비방글
그러니까
비밀번호는
잘 관리해
주세요!


네~!!
그리고 아무리 좋은
비밀번호를 설정해도
안심하면 안 돼요.
또 외우는게
어렵다고 모두
똑같은 비밀번호를
사용하면 관리가
느슨한 곳에서
누출될 경우
모두 사용할 수가 없게
될 수도 있어요.
보호는
자기 스스로!!
네~~!!!

【자료】

용어

정보보안

조직이 가지고 있는 여러 가지 정보를 안전하게 관리하기 위한 규칙을 어떻게 만들까를 생각한다. 정보를 안전하게 지키려면 조직으로서 정보취급방법규칙을 결정하여 의사소통을 도모하는 것이 반드시 필요하다. 또, 다수의 멤버가 있는 경우에는, 지켜야 할 규칙들을 문서로 만들 필요가 있다. 정보보안대책에서는 정보보안대책 본연의 자세에 대한 조직으로서 대책(방침이나 목표)을 결정하여 거기에 따른 자세한 규칙을 순서대로 정해서 문서화 한다.

암호

특정인에게만 전하기 위해, 그 특정인 이외에는 아무도 모를 듯 한 방법으로 전하고 싶은 것을
나타내는데 그것을 암호라고 한다. 암호 전의 메시지를 평문, 암호화한 후의 메시지를 암호화라고 부른다. 또, 암호문을 원래 메시지로 돌아가는 것을 복호화라고 한다. 암호화나 복호화를 할 때는 키가 필요하지만 이 키가 공통인 것을 공통키 암호(대상키 암호, 비밀키 암호), 짝을 이루는 다른 키를 사용하는 것을 비대칭키 암호(공개키 암호) 라고 한다.

소셜 엔지니어링

사람의 허점을 노려서 패스워드 등을 부정하게 취득하는 방법. 본편에서는 시스템관리자로 가장하여 패스워드를 묻기 시작하려고 하는 예를 들었지만, 그 이외에도 여러 가지 수법이 있으므로 주의해야 한다. 예를 들면, 보안에서 유명한 기업으로 가장해, “보안에 관계된 중요한 일이므로 이 URL에 접근해 주세요. 첨부파일를 읽어주세요.” 등과 메일을 보내 가짜 사이트로 유도하는 예도 있다. 다른 확실한 수단을 이용하고, 그 정보가 사실인지, 아이디나 패스워드 등의 정보를 정말로 넣을 필요가 있는지 등, 침착하게 판단해야 한다.

부정접근행위금지 등에 관한 법률

인증정보의 부정취득을 막기 위해, 2001년에 시행되었다. 타인의 아이디로 무단 로그인을 하면, 그 밖에 아무것도 하지 않고 로그인 한 것만으로도 법률위반이 된다. 무단 로그인을 당한 쪽은 피해자이지만, 그 아이디로 이루어진 행위에 의해, 가해자로도 될 수 있다. 간편한 패스워드는 피할 것. 친구 사이 아이디를 빌려 쓰는 것도 엄금한다.

패스워드 관리

우리는 오늘날의 정보사회에서 여러 가지 시스템으로 아이디나 패스워드를 이용하고 있다. 아이디와 패스워드의 관리 방법은 각 시스템에 따라 다르지만, 정보보안대책을 정한 신뢰할 수 있는 기관에서는, 본인만 알 수 있게 암호화되고 관리되고 있다. 그러나 그렇지 않은 수상한 시스템이 존재하는 것도 사실이다. 각 아이디의 중요성의 차이를 생각하지 않고, 무엇이든지 같은 패스워드를 설정하면 관리가 잘된 시스템으로부터 패스워드가 뚫리게 되므로 주의해야 한다.

인터넷 이용 시, 패스워드 [재사용]이 대다수

2011년 6월 16일 갱신　ITmedia
http://www.itmedia.co.jp/news/1106/16/news024.html
유출된 약 4만 명의 이용자계정을 분석한 결과, 동일한 사용자라고 판단되는 2천개 이상의 계정 중 92% 이상이 두 가지 경우에 동일한 암호를 재사용하고 있었다. 또 다른 유출 데이터에서 일반 전자메일 계정이 있는 88건을 추출하였고 이중 70%의 사용자가 동일한 암호를 재사용하고 있었다. 분석 결과, 암호에 포함된 문자열을 확인하고 숫자, 대문자, 소문자 등을 조합하고, 소문자 같은 한 종류만을 이용한 암호를 설정한 경우가 절반 가까이 있었다. 자세한 내용은 위를 참조한다. 당신은 괜찮습니까?

인터넷 서비스 부정 이용 (정보처리추진기구보안센터 2012년 1월)

정보처리추진기구 시큐리티센터는 2011년을 정리하며 인터넷 서비스 부정 이용을 다루었다. 부정 이용의 원인으로는 바이러스 감염이나 피싱 등이 있으며, 피해 확대의 원인으로는 동일한 ID와 패스워드의 재사용이 거론되고 있다.
앞으로는 패스워드를 재사용하는 사람을 대상으로, 지금까지는 표적이 되지 않았던 무료 서비스를 포함하여, ID, 패스워드 재사용을 하지 않기, 쉬운 암호 사용 안 하기 등을 안내할 예정이다.

인터넷에서의 암호 【암호화】

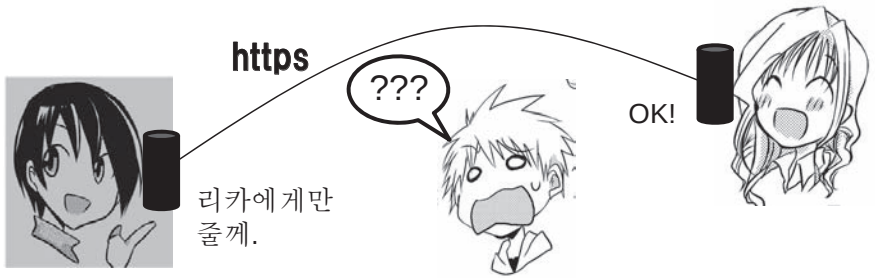
암호는 훨씬 예전부터 누군가에게 비밀의 메시지를 보내기 위한 것 등에 사용되어 왔다.
제2차세계대전에서 암호해독의 역사는 상징적인 것이다. 오늘날 인터넷상에서는 정보를 안전하게 교환하는 것 등에 암호가 사용되고 있다. 공개키 암호 등 암호방식의 대책은 생략하지만 본편에 있듯이 패스워드의 암호화와 통신의 암호화의 차이를 생각해보자. 당연 이야기지만, 패스워드는 시스템 상에서 보존되고 있는데 비해, 통신에서는 상대가 존재하여 상대에게 메시지를 전할 필요가 있다.

패스워드 암호화

입력한 문자열을 시스템 상에 보존하고 있는 것과 비교하여 인증을 실시한다. 구체적으로는 패스워드로 입력한 문자열을 요약함수 등을 사용해 요약한 값과 인증 서버상의 패스워드 요약값을 비교한다. 요약 값으로부터 원래로 되돌리지 못하고, 또, 다른 문자열로부터 똑같은 요약 값을 만드는 것은 더없이 곤란한 방식을 사용한다.

통신의 암호화

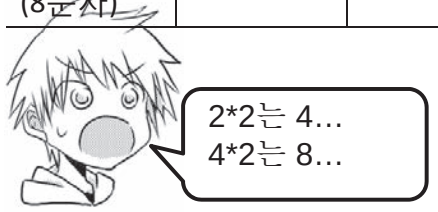
신용카드암호를 온라인 쇼핑몰 사이트에서 입력하는 경우 등에서는 안전하게 통신을 하는 것이 필요하다. 인터넷 상에서는 제3자의 통신 데이터가 도청될 가능성이 있기 때문에 도청되어도 해독할 수 없게 메시지를 암호화한다. 물론, 통신상대에게 도착한 시점에서 그 메시지를 복원(복호화) 한다.



당신의 패스워드는 숫자만으로 되어있지는 않겠지요?

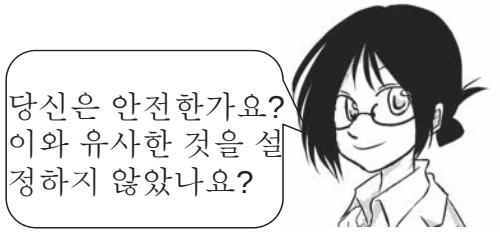
패스워드는 대문자, 소문자, 숫자 등을 혼재시키는 것이 좋다. 패스워드를 은행의 비밀번호등과 같이 생각해서 숫자만으로 설정한 사람은 패스워드를 변경하도록 하는 것. 만약, 1초에 10만 번의 빠르기로 패스워드를 생성하고 해독을 시도했다고 가정하면 각각 어느 정도의 시간에 모든 패스워드를 시험할 수 있을까. 아래와 같이 공란에 계산결과를 넣어보자. 물론, 이것들은 단순한 기준에 지나지 않지만 대문자. 소문자. 숫자를 조합하는 중요성을 생각해 보는 것이 필요하다.

	숫자	영어 (소문자)	전체영어	영어와 숫자
문자의 종류	10	26	52	62
2문자 조합	10＊10	26＊26	52＊52	62＊62
4문자 조합	10^4 1만	26^4 약 46만	52^4 약 730만	62^4 약 1480만
8문자 조합	10^8 1억	26^8 약 2100억	52^8 약 50조	62^8 약 220조
16문자 조합	10^{16}	26^{16}	52^{16}	62^{16}
해독시간 (4문자)	0.1초	약 5초		약 150초
해독시간 (8문자)	약 17분	약 24일	약 17년	



취약한 ID와 패스워드
【유출정보의 분석 등으로부터】

정보유출피해가 있었던 패스워드를 분석한 결과이다. 공격자를 유인하기 위해서 일부러 취약한 시스템을 인터넷 상에 두어, 공격자의 공격수법을 조사한 것 도 있다. 이러한 공격자는 보통, 리카가 걱정하는 것 같이 개인적인 메일이나 파일을 읽는 것에 목적이 없다. 해킹한 아이디와 패스워드를 이용하여 연쇄적인 부정 이용을 하는 것으로, 개인의 경우에는 금전을 노리거나 기업 등에 대해서는 정보를 노리거나 한다. 또한 봇(bot)이라고 불리는 컴퓨터 바이러스 장치 네트워크를 통해 감염된 컴퓨터를 조종하거나 가짜 웹사이트를 구축하기도 한다. 이것은 암호를 도난 당하는 것으로 가해자가 될 가능성을 의미하고 있다.
비록 시스템에 중요한 데이터가 없다 하더라도 쉬운 설치 암호를 설정하지 말라는 것이다. 공격자에게 공격 당한 암호의 예는 다음과 같다.

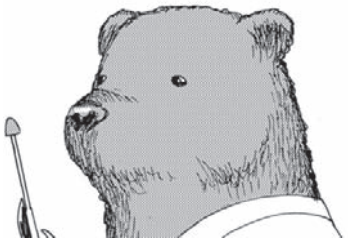


취약한 패스워드의 예

ID와 같은 패스워드

123456, password, 0, 1, qazwsx, admin, test, 123qwe, 1qaz2wsx, qwerty, 123qaz, 1234, 12345, psswd, 123, 이와 같은 조합, 등

Web에서 붙여 넣기 한 레포트는 NG【전편】



【 목표와 포인트】

1. 인용의 구체적인 방법을 이해하여 레포트 등에서 적절한 인용을 할 수 있다.

    - 아오야마 선배는 아이코의 레포트에 대해 무엇이 문제라고 지적하고 있는가? 아오야마 선배의 지적을 항목별로 나누어 쓰고 그것에 대해 당신은 어떻게 생각하는지 구체적인 의견을 서술한다.
    - 인용과 복사의 차이에 대해 당신의 의견을 서술한다.

2. 일본의 저작권법을 이해하고 그 중, 인용에 대해 이해한다.

    - 인용이라고 인지되기 위한 구체적인 조건을 조사한다.

3. 저작권에 관한 국제 조약과 해결상황을 조사해 파악한다.

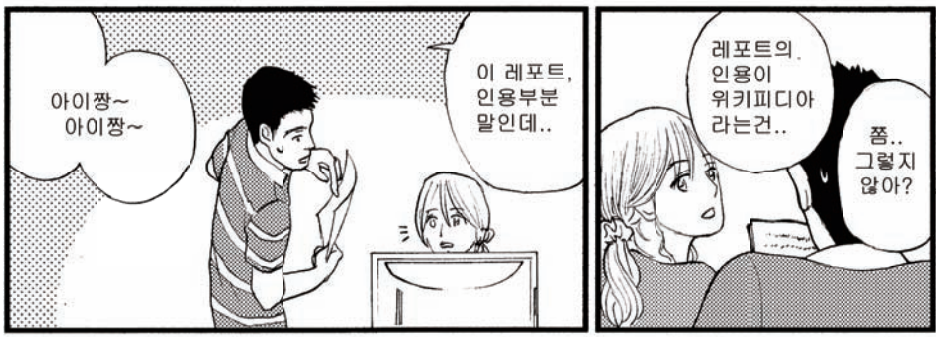
    - 각국의 저작권법에 있어 저작물의 기간이나 권리제한규정의 내용을 조사한다.


그것보다..
아이짱은 어느정도 진척이 있어?
좀 보여줄 수 있어?
응~ 물론~

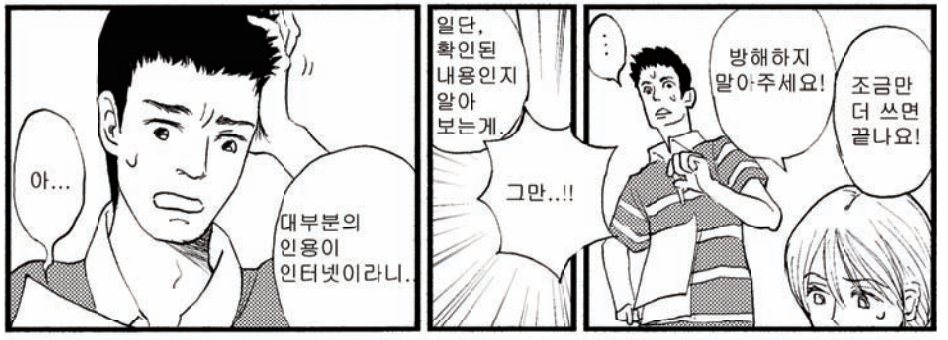

땡큐~
어! 아이짱!
이거 아이짱 아냐~!


오~ 진지한 분위기~
하지만 아이짱은 한폭의 그림 같구나~
역시 이번 무대의 주인공은...
아.오. 야.마.상;;


리카짱~
시끄럽게 하면 안돼요~
지금 한창 레포트 쓰는 중이라구요!
레포트?
....


아이짱~ 아이짱~
이 레포트, 인용부분 말인데..
레포트의 인용이 위키피디아라는건..
쯤.. 그렇지 않아?


위키피디아라면 인터넷 프리 백과사전 말하는거야?
응~~
그리고, 이 인용부분은..
이건 누가썼는지 모를 인터넷의 기록들이잖아..
....
그리고 이건, 서명이나 저작자의 표시가 없잖아.


아...
대부분의 인용이 인터넷이라니..
일단, 확인된 내용인지 알아보는게..
그만..!!
방해하지 말아주세요!
조금만 더 쓰면 끝나요!


무서워..
하지만 여기저기서 베낀 내용을
모아서써서
이건...
아이짱의 레포트라고 부를 수 있을까...?
됐어요!

생각해보자

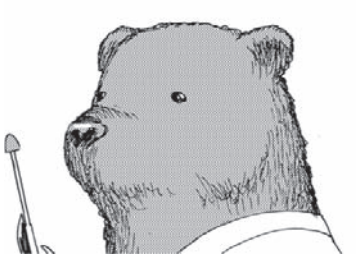
- 아오야마 선배가 아이코의 리포트에 대한 지적한 문제점을 항목별로 써보자.
- 나열한 각 항목에 대해 당신은 어떻게 생각하십니까? 구체적인 의견을 설명해보자.
- 인용과 복사의 차이에 대해 당신의 의견을 써보자.

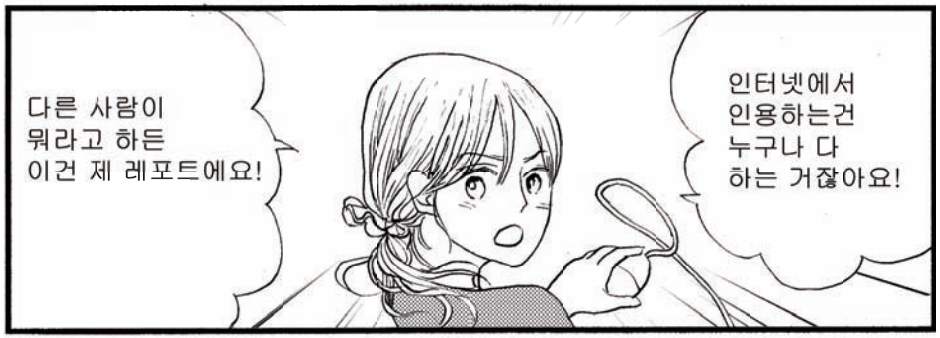
Web에서 붙여 넣기 한 레포트는 NG【후편】

편을 읽은 후, 다음과 같이 해봅시다.

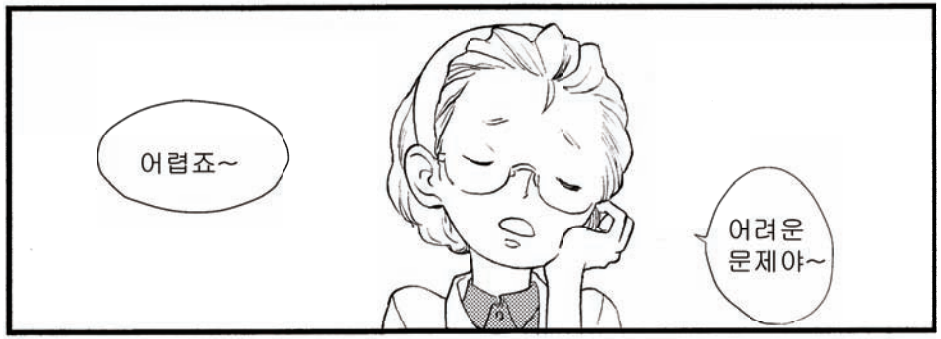
- 저작권 법 상의 인용으로 간주하기 위한 조건을 작성한다.
- 일반적인 문헌의 인용과 웹상의 자료의 인용에서는 무엇이 다를까?
- 인용 부분과 자신의 문장과의 구별을 명확하게 하려면 구체적으로 어떻게 하면 좋을까?
- 인용에 관한 판례를 확인해보자.

*판례: 패러디사건: 사건번호 쇼와51 (재 923)



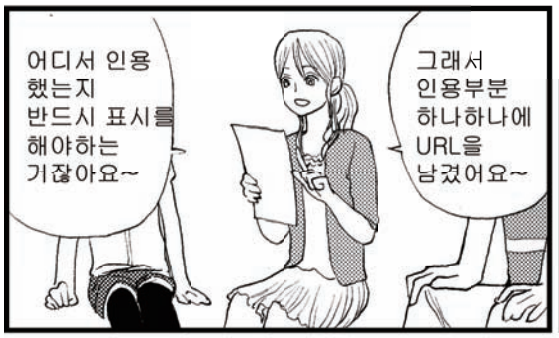

다른 사람이
뭐라고 하든
이건 제 레포트에요!
인터넷에서
인용하는건
누구나 다
하는 거잖아요!


....
르 시!
이것에 대해
어떻게
생각하세요?

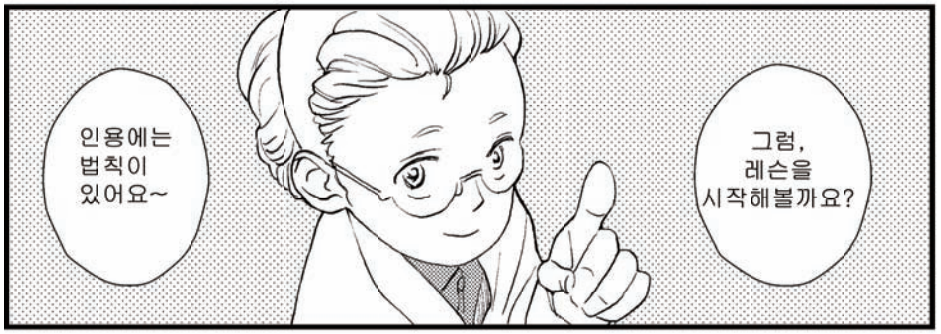

어렵죠~
어려운
문제야~


자~ 그럼
여기서
아이짱에게
질문!

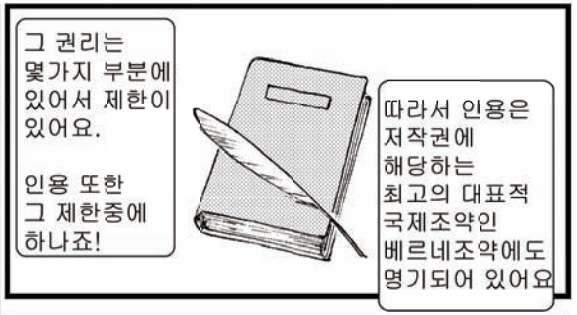

인용이라걸
확인하기 위해선
조건이 있다는
것은 알고 있죠?
물론이에요!


어디서 인용
했는지
반드시 표시를
해야하는
거잖아요~
그래서
인용부분
하나하나에
URL을
남겼어요~


응..
그건
그런데..
그것만으로
충분할까요?

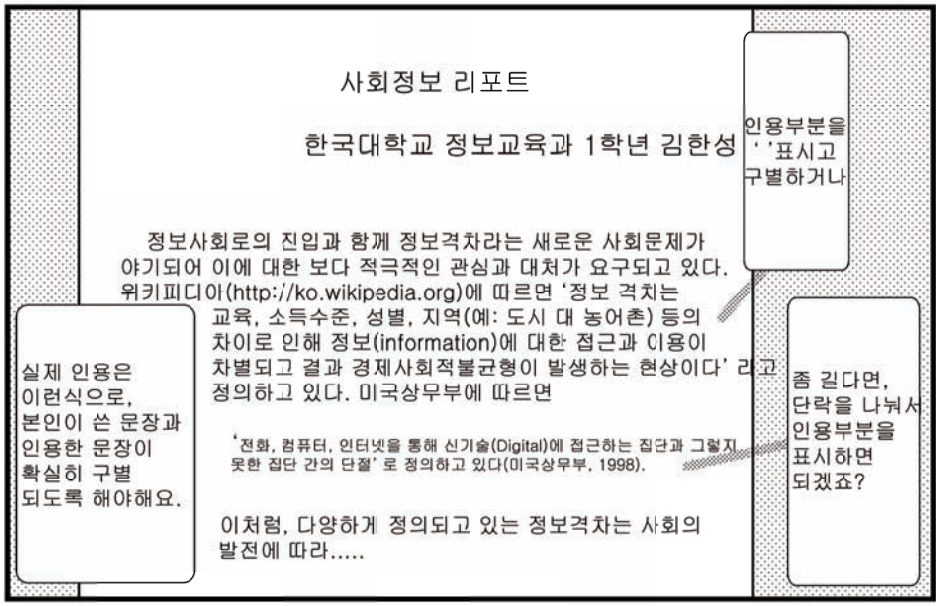

인용에는
법칙이
있어요~
그럼,
레슨을
시작해볼까요?


먼저, 인용을
설명하기
위해서
기초적인
것부터
생각해
봅시다!
저작권
여러분도
저작자에게
자작권이라는
권리가
있다는걸
알고있죠?

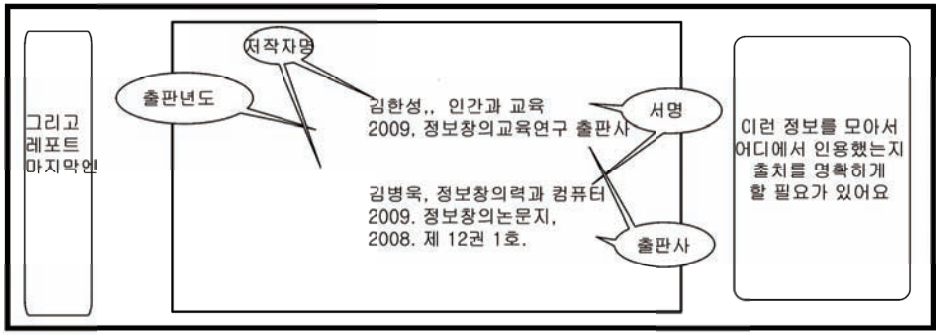

그 권리는
몇가지 부분에
있어서 제한이
있어요.
인용 또한
그 제한중에
하나죠!
따라서 인용은
저작권에
해당하는
최고의 대표적
국제조약인
베르네조약에도
명기되어 있어요

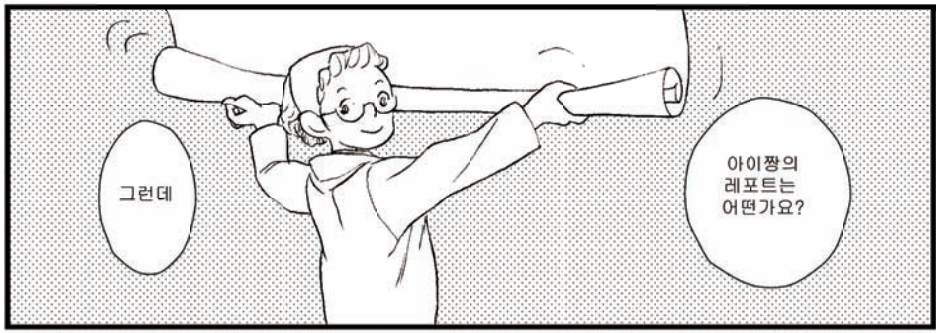

그건 인용이 문화적인
재산을 정당하게
보호해주고, 발전시키기
위해 기본적으로
불가피한 요소라고
생각하기 때문이에요.
먼저,
이점을
이해하고
정당히
인용을
하는 방법을
생각해 봅시다

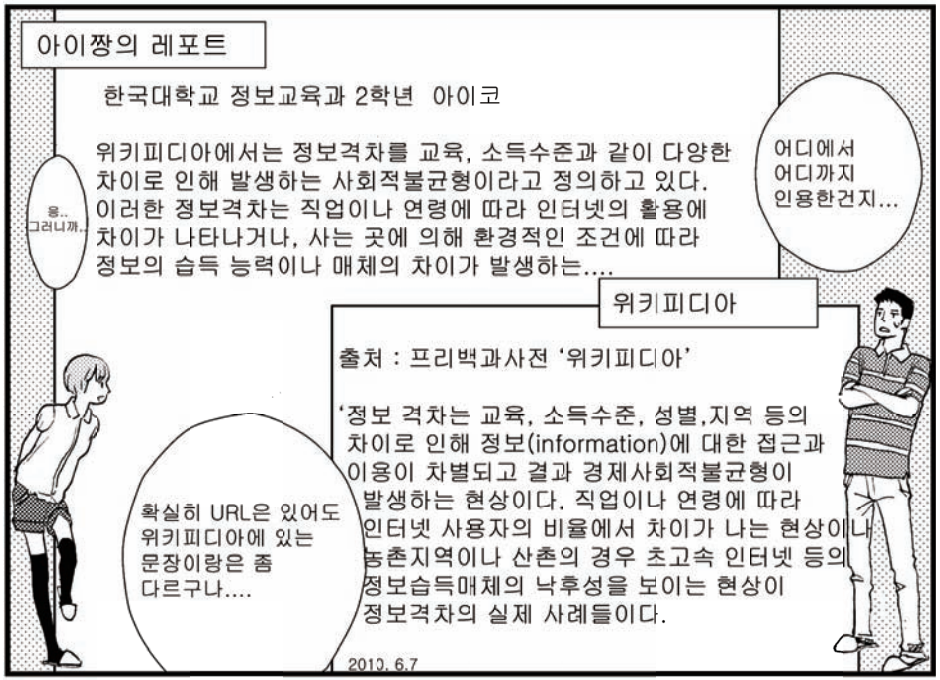

먼저,
인용하려는
것은
이미 공표된
저작물에
한정되는
것으로
신간
비평
연구
등에
사용할
수
있어요.

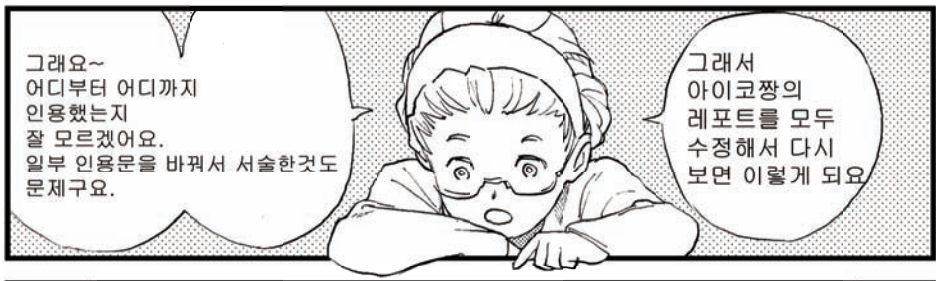

사회정보 리포트
한국대학교 정보교육과 1학년 김한성
인용부분을
' '표시고
구별하거나
정보사회로의 진입과 함께 정보격차라는 새로운 사회문제가
야기되어 이에 대한 보다 적극적인 관심과 대처가 요구되고 있다.
위키피디아(http://ko.wikipedia.org)에 따르면 '정보 격차는
교육, 소득수준, 성별, 지역(예: 도시 대 농어촌) 등의
차이로 인해 정보(information)에 대한 접근과 이용이
차별되고 결과 경제사회적불균형이 발생하는 현상이다' 라고
정의하고 있다. 미국상무부에 따르면
실제 인용은
이런식으로,
본인이 쓴 문장과
인용한 문장이
확실히 구별
되도록 해야해요.
'전화, 컴퓨터, 인터넷을 통해 신기술(Digital)에 접근하는 집단과 그렇지
못한 집단 간의 단절' 로 정의하고 있다(미국상무부, 1998).
이처럼, 다양하게 정의되고 있는 정보격차는 사회의
발전에 따라.....
좀 길다면,
단락을 나눠서
인용부분을
표시하면
되겠죠?

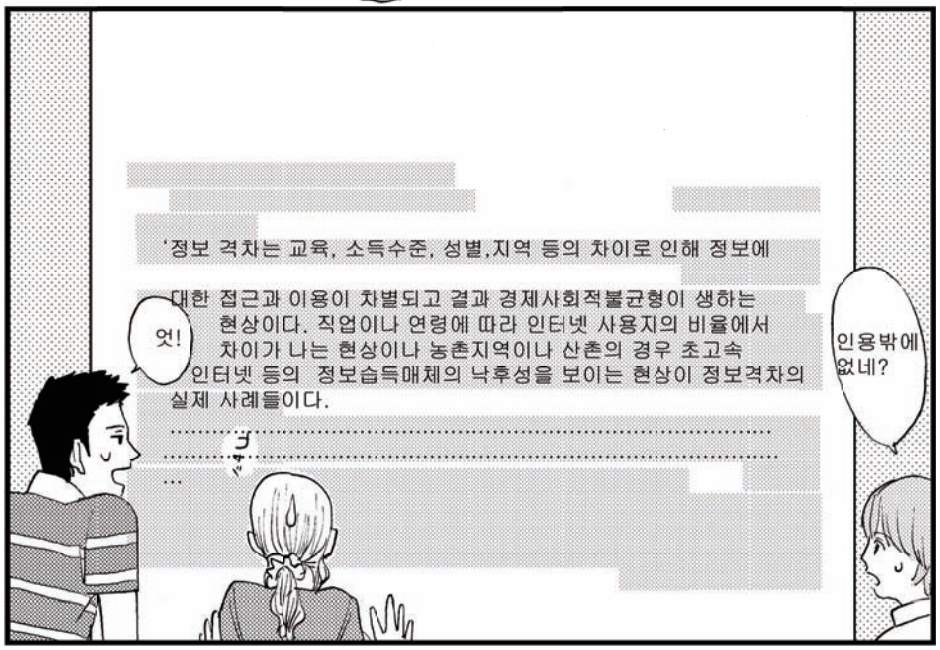

다음으로,
인용을하면
반드시
원문을 그대로
사용해야해요.
이부분을
알기쉽게
쓰려면....
자의대로
원문을
변경하여서
인용하면
안 됩니다.

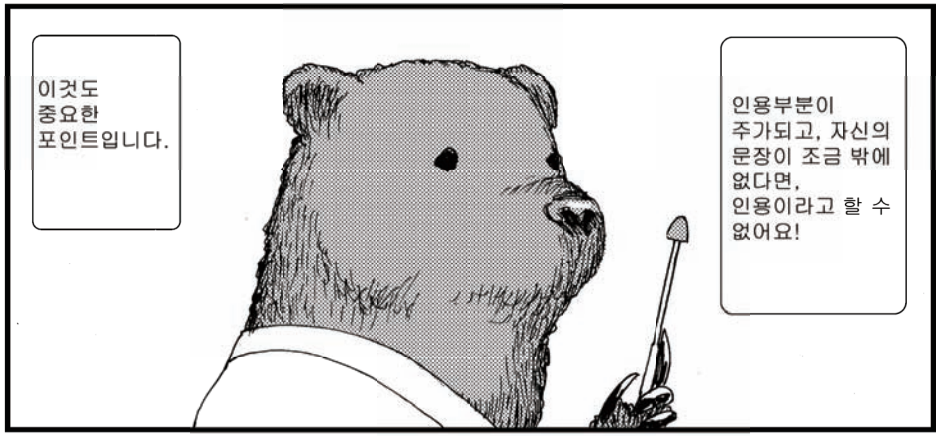

그리고
레포트
마지막엔
저작자명
출판년도
김한성,, 인간과 교육
2009. 정보창의교육연구 출판사
김병욱, 정보창의력과 컴퓨터
2009. 정보창의논문지,
2008. 제 12권 1호.
서명
출판사
이런 정보를 모아서
어디에서 인용했는지
출처를 명확히게
할 필요가 있어요


그런데
아이짱의
레포트는
어떤가요?


아이짱의 레포트
한국대학교 정보교육과 2학년 아이코
위키피디아에서는 정보격차를 교육, 소득수준과 같이 다양한
차이로 인해 발생하는 사회적불균형이라고 정의하고 있다.
이러한 정보격차는 직업이나 연령에 따라 인터넷의 활용에
차이가 나타나거나, 사는 곳에 의해 환경적인 조건에 따라
정보의 습득 능력이나 매체의 차이가 발생하는....
응..
그러니까..
어디에서
어디까지
인용한건지...
위키피디아
출처 : 프리백과사전 '위키피디아'
'정보 격차는 교육, 소득수준, 성별,지역 등의
차이로 인해 정보(information)에 대한 접근과
이용이 차별되고 결과 경제사회적불균형이
발생하는 현상이다. 직업이나 연령에 따라
인터넷 사용자의 비율에서 차이가 나는 현상이나
농촌지역이나 산촌의 경우 초고속 인터넷 등의
정보습득매체의 낙후성을 보이는 현상이
정보격차의 실제 사례들이다.
확실히 URL은 있어도
위키피디아에 있는
문장이랑은 좀
다르구나....
2010. 6.7


그래요~
어디부터 어디까지
인용했는지
잘 모르겠어요.
일부 인용문을 바꿔서 서술한것도
문제구요.
그래서
아이코짱의
레포트를 모두
수정해서 다시
보면 이렇게 되요


'정보 격차는 교육, 소득수준, 성별,지역 등의 차이로 인해 정보에
대한 접근과 이용이 차별되고 결과 경제사회적불균형이 생하는
현상이다. 직업이나 연령에 따라 인터넷 사용지의 비율에서
차이가 나는 현상이나 농촌지역이나 산촌의 경우 초고속
인터넷 등의 정보습득매체의 낙후성을 보이는 현상이 정보격차의
실제 사례들이다.
……
……
…
엇!
인용밖에
없네?


이것도
중요한
포인트입니다.
인용부분이
주가되고, 자신의
문장이 조금 밖에
없다면,
인용이라고 할 수
없어요!

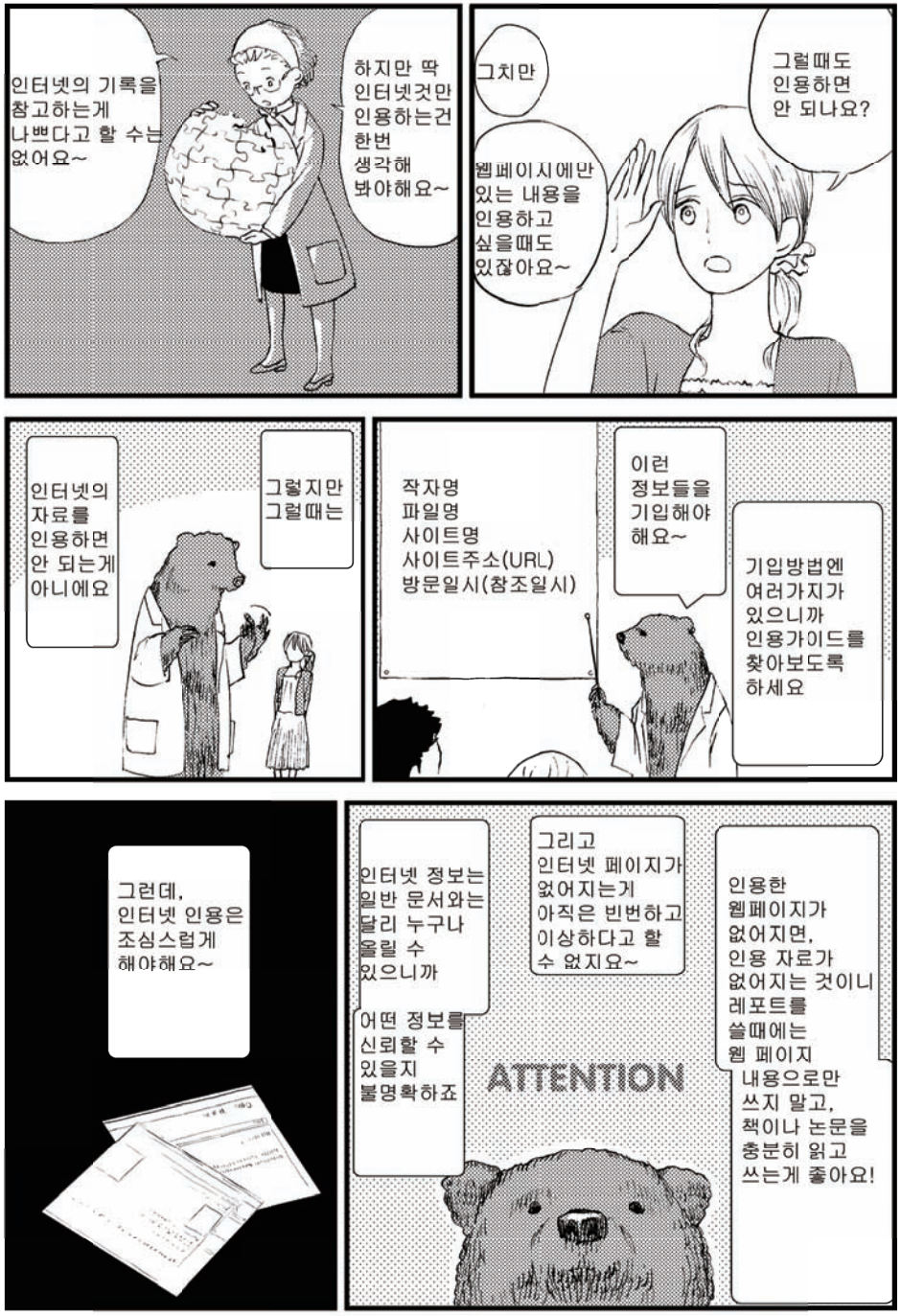

알겠습니다
조금
인용을
줄이라는
말이죠?
헉!
잠깐만요
아이짱~
그것뿐만이
아니에요~
하나더
근본적인
문제가
있어요~

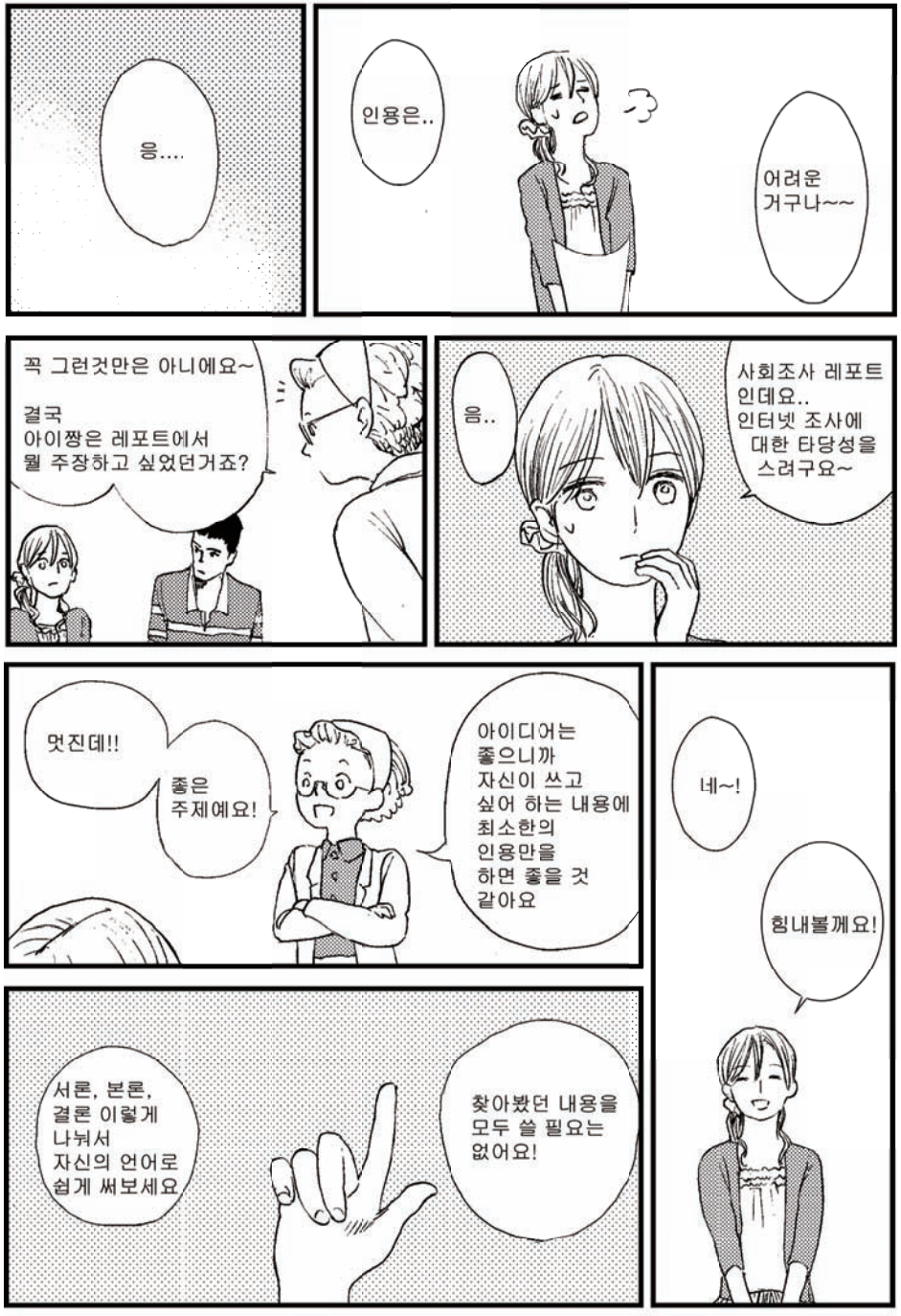

아이짱의
인용은
비평이나
연구를 위해
사용한거죠?
이것은
단순한
카피 인용과는
달라요~
네?


그럼
이 레포트는
안 된다는거
예요?
열심히
썼는데
~~
!


그리고
루시!
인용문에
인터넷 URL만
쓰는건
잘 못된거
아닌가요?


좋은
지적!!
여러가지가
신경쓰일 수
있어요~
봐, 인터넷 내용이
바뀌는 경우도 있고
언제적 내용인지
확실치도 않고,


인터넷의 기록을 참고하는게 나쁘다고 할 수는 없어요~
하지만 딱 인터넷것만 인용하는건 한번 생각해 봐야해요~
그치만 웹페이시에만 있는 내용을 인용하고 싶을때도 있잖아요~
그럴때도 인용하면 안 되나요?
인터넷의 자료를 인용하면 안 되는게 아니에요
그렇지만 그럴때는
작자명
파일명
사이트명
사이트주소(URL)
방문일시(참조일시)
이런 정보들을 기입해야 해요~
기입방법엔 여러가지가 있으니까 인용가이드를 찾아보도록 하세요
그런데, 인터넷 인용은 조심스럽게 해야해요~
인터넷 정보는 일반 문서와는 달리 누구나 올릴 수 있으니까
어떤 정보를 신뢰할 수 있을지 불명확하죠
그리고 인터넷 페이지가 없어지는게 아직은 빈번하고 이상하다고 할 수 없지요~
ATTENTION
인용한 웹페이지가 없어지면, 인용 자료가 없어지는 것이니 레포트를 쓸때에는 웹 페이지 내용으로만 쓰지 말고, 책이나 논문을 충분히 읽고 쓰는게 좋아요!


응....
인용은..
어려운 거구나~~
꼭 그런것만은 아니에요~
결국 아이짱은 레포트에서 뭘 주장하고 싶었던거죠?
음..
사회조사 레포트 인데요.. 인터넷 조사에 대한 타당성을 스려구요~
멋진데!!
좋은 주제예요!
아이디어는 좋으니까 자신이 쓰고 싶어 하는 내용에 최소한의 인용만을 하면 좋을 것 같아요
네~!
힘내볼께요!
서론, 본론, 결론 이렇게 나눠서 자신의 언어로 쉽게 써보세요
찾아봤던 내용을 모두 쓸 필요는 없어요!

【자료】위키피디아 등의 Web상의 기사로부터의 인용

학년 때, 위키피디아로부터의「인용」은 선생님이 안 된다고 말하셨는데, 실제로는 어떤 상황이야?

그것은, 선생님마다 다른거 같아. 그래도, 아오야마(青山)군과 같이 , 위키피디아로부터의「인용」을 허가하지 않고 있을 경우가 많을 거라 생각해. 확실하게 선생님의 지시를 따르는 게 좋겠지.
그럼, 위키피디아의 인용에 대해서 생각해 봅시다.

조금 전에, 저작권법상의 인용을 위한 조건의 하나로서, 출소의 명시(저작권법 제48조)을 올렸습니다. 즉, 어디에서 인용했는지를 정확히 가리키는 것이 필요하게 됩니다. 그 때, 평소 때에는 저자명을 들 필요가 있습니다만, 위키피디아의 경우는, 누가 저자가 됩니까?

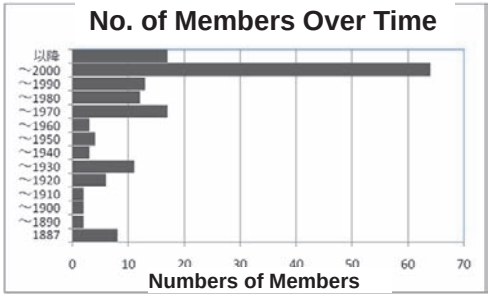
저자 없이,「위키피디아 일본어판」으로 기재하면 되는 거 아닙니까? 위키피디아는 기사수가 압도적으로 많고, 여러 가지 참고가 되어요.

그렇죠. 자신의 의견을 구축하기 위해서 참고로 하는 것은 좋을지도 모르겠습니다.
그러나, 위키피디아는, 저자가 누구인지 모르겠습니다. 또, 수시로 고쳐지고, 내용이 바뀝니다. 리포트를 썼을 때와 리포트의 제출 후에 인용된 내용이 다르게 되면, 인용의 의미가 없겠지요. 이것은, 위키피디아에 제한되지 않고, Web상의 모든 저작물에 공통되는 문제입니다. 서적의 소개와 같이, 원본이 서적으로서 있는 경우는 그것을 인용하면 좋습니다만, Web상에서만 공개되고 있는 저작물도 있습니다. Web상에서만 공개되고 있는 저작물을 인용해서는 안 된다는 것이지 않습니다.
불특정 한 사람이 쓰고, 수시로 바뀌는 Web상의 기사는, 신뢰성이 일반적으로 높지 않고, 그것을 연구 대상으로 할 경우를 제외하고, 그러한 기사를 참고로 한 리포트의 신뢰성도 의심되게 됩니다.

베른조약

저작물은 나라를 넘어서 보호 할 필요가 있고, 여러 가지 조약이나 협정이 국제적으로 맺어져 있습니다. 저작권에 관해서 가장 대표적인 국제 조약이 베른 조약입니다.
베른 조약은 1886년에 유럽 제국을 중심으로 창설되어, 일본은, 1899년에 체결했습니다. 베른 조약은, 그 후 몇 번인가 개정 되어, 1971년의 파리 개정 조약이 가장 최근입니다. 2012년3월15일 현재, 가맹국은 165개국으로, 체결국수의 추이는 아래의 그림과 같습니다. 미국이 체결한 것은 1989년으로 최근입니다.

그림은 WIPO(세계지적소유권기관 (http://www. wipo. int/portal/index. html. en)의 데이터를 바탕으로 작성



베른 조약의 특징은, 무방식 주의(권리를 얻기 위한 수속 필요 없음), 내국민대우, 법률 효력을 들 수 있습니다만, 거기에 더해, 제10조에서의 인용(Quotations)의 기술을 주목해 주십시오.
「동맹국의 법령이 유효한 곳」이라는 유보 조건 없이, 인용이 공정한 관행과 일치하여, 동시에, 그 목적상 정당한 범위 내에서 행하여지는 것을 조건으로 정당한 법으로 인정되고 있습니다. 이것은, 창작 활동은 기본적으로 선인의 지식을 전제로 한 것이며, 지금까지의 성과를 인용이란 형태로 정당한 범위 내에서 활용할 수 있는 것이, 문화의 발전을 위해서는 필수적인 사항이라고 생각됩니다.
왼쪽으로 WIPO의 페이지에 게재되고 있는 베른 조약의 제10조를 일부 발췌합니다.

Article 10
Certain Free Uses of Works:
1. Quotations; 2. Illustrations for teaching; 3. Indication of source and author
(1) It shall be permissible to make quotations from a work which has already been lawfully made available to the public, provided that their making is compatible with fair practice, and their extent does not exceed that justified by the purpose, including quotations from newspaper articles and periodicals in the form of press summaries.
(http://www.wipo.int/export/sites/www/treaties/en/ip/berne/pdf/trtdocs_wo001.pdf)

인용에 관한 대법원판례
패러디 사건:사건번호 쇼와(昭和)51(【오】) 923

사건명 (손해 배상)　재판일 쇼와(昭和)55년3월28일
법정명 대법원제3소법정
결과 파기 환송　판례집 제34권 3호 244페이지
원심재판소명:도쿄(東京) 고등법원　재판일 쇼와(昭和)51년5월19일

판시사항
1 구 저작권법(메이지(明治)32년 법률 제39호) 30조 1항 2호에서 말하는 인용의 의의
2 남이 저작한 사진을 변조하여 이용하는 것에 의해 몽타쥬 사진을 작성해서 발행했을 경우와 저작자인격권의 침해
3 몽타쥬 사진의 작성 발행이 저작자인격권의 침해에 해당된다고 여겨진 사례
재판 요지
1 구 저작권법(메이지(明治)32년 법률 제39호) 30조 1항 2호에서 말하는 인용이란 소개, 참조, 논평 등의 목적으로 자기의 저작물 중에 남의 저작물의 원칙으로서 일부를 채록하는 것 뿐 만 아니라, 인용을 포함한 저작물의 표현 형식상, 인용해서 이용 하는 쪽의 저작물과, 인용되어 이용되어지는 측의 저작물을 명료하게 구별해서 인식할 수 있고, 동시에, 양쪽 저작물간에 전자가 주인, 후자가 종속된 관계임을 요한다.
2 남이 저작한 사진을 변조하여 이용함으로써 몽타쥬 사진을 작성하여 발행했을 경우, 몽타쥬 사진으로부터 남의 사진에 있는 본질적인 특징자체를 직관적으로 느낄 수 있을 때는, 몽타쥬 사진을 한 개의 저작물이라고 볼 수 있다고 하지만 그 작성 발행은, 남의 동의가 없는 한, 그 저작자인격권을 침해하는 것이다.
. 눈의 사면을 스노타이어(snow tire)의 흔적과 같은 슈프르를 그리며 활강해 온 6명의 스키어를 촬영해서 제작한 판례와 같은 산악풍경 컬러사진 중 일부를 제외하고, 슈프르를 타이어의 흔적으로 바꾸어 그 기점에 있는 눈의 사면에 거대한 스노타이어(snow tire)의 사진을 합성해서 작성한 판례와 같은 흑백의 몽타쥬 사진을 발행하는 것은, 기존 산악풍경사진의 저작자의 동의가 없는 한, 그 저작자인격권을 침해하는 것이다.
참조법조
구 저작권법(메이지(明治)32년 법률 제39호)18조, 구 저작권법(메이지(明治)32년 법률 제39호) 30조 1항 2호, 구 저작권법(메이지(明治)32년 법률 제39호) 36조【노】2

出所：裁判所判例検索システム　(2009.3.13現在)
http://www.courts.go.jp/search/jhsp0030?action_id=dspDetail&hanreiSrchKbn=01&hanreiNo=26442&hanreiKbn=06

블로그에 메일의 내용을 소개하면 안되는건가?

【 목표와 포인트】

1. 저작권은 저작 인격권과 재산권으로서의 저작권이 있음을 이해한다.

   ○ 저작 인격권에 대해 설명할 수 있다.
   ○ 저작권법의 저작자의 권리에 대해 이해한다.

2. 저작물의 "공표"는 어떤 행위를 말하는지 이해한다. 또한 "공중"의 저작권 법 상 해석을 이해한다.

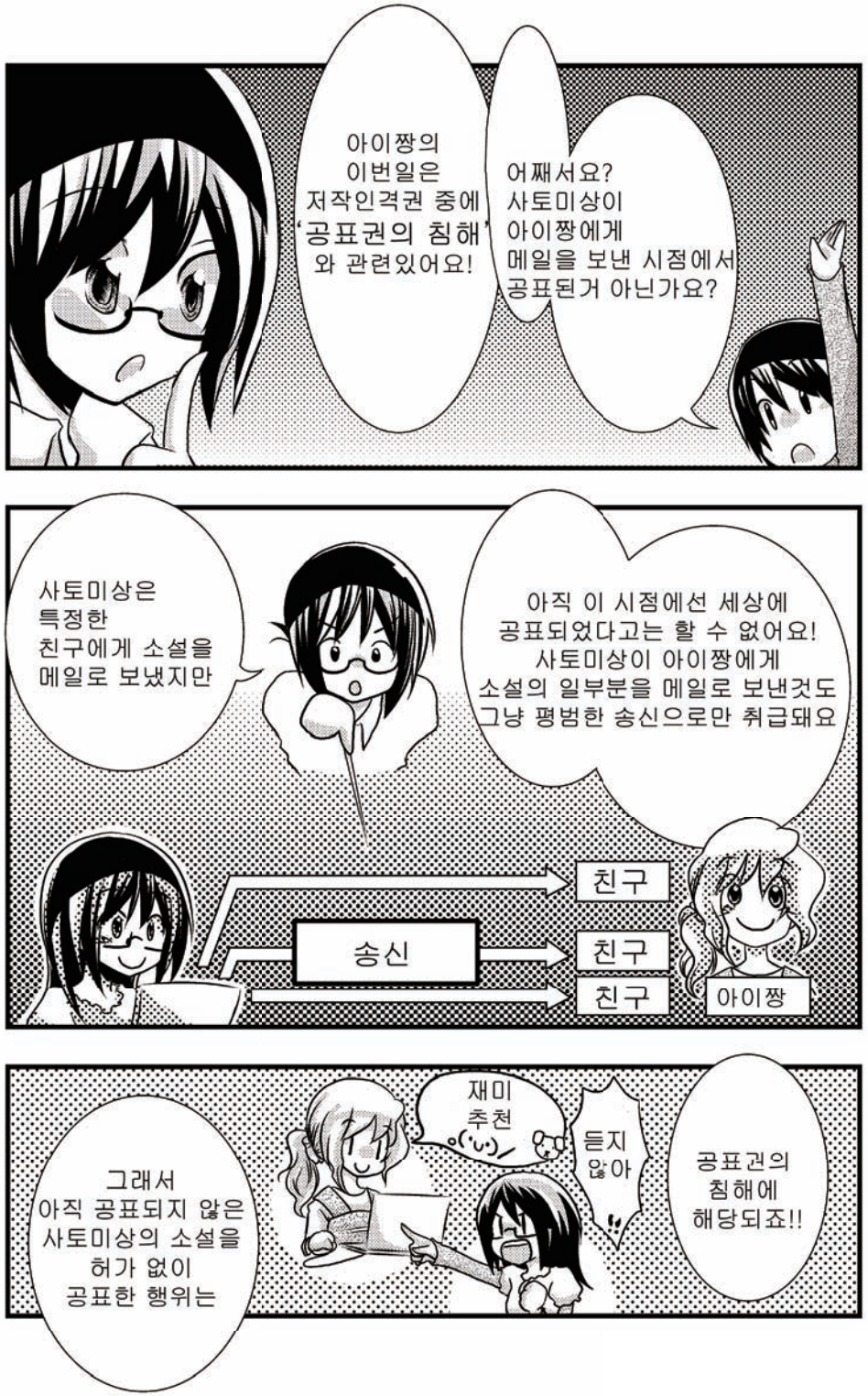

어느정도되면 다시 아이짱에게 메일 보낼테니까 또 의견줘~
응!!
완전 기대!! 기대!!
어!?
사토미상 ~~~~?
읽었어! 읽었어!
이야~ 설마 그런 재능이 있는지 몰랐었네~
무.. 슨.. 말..?
?
소설말야~ [꽃보다 여자] !!
아직 10화만 읽어봤지만
완전~ 최고야! 벌써 다음이 궁금해졌어!!
1화부터 전부 읽어볼수는 없을까?
아오야마군.. 내 소설은 어디서 읽었어..?

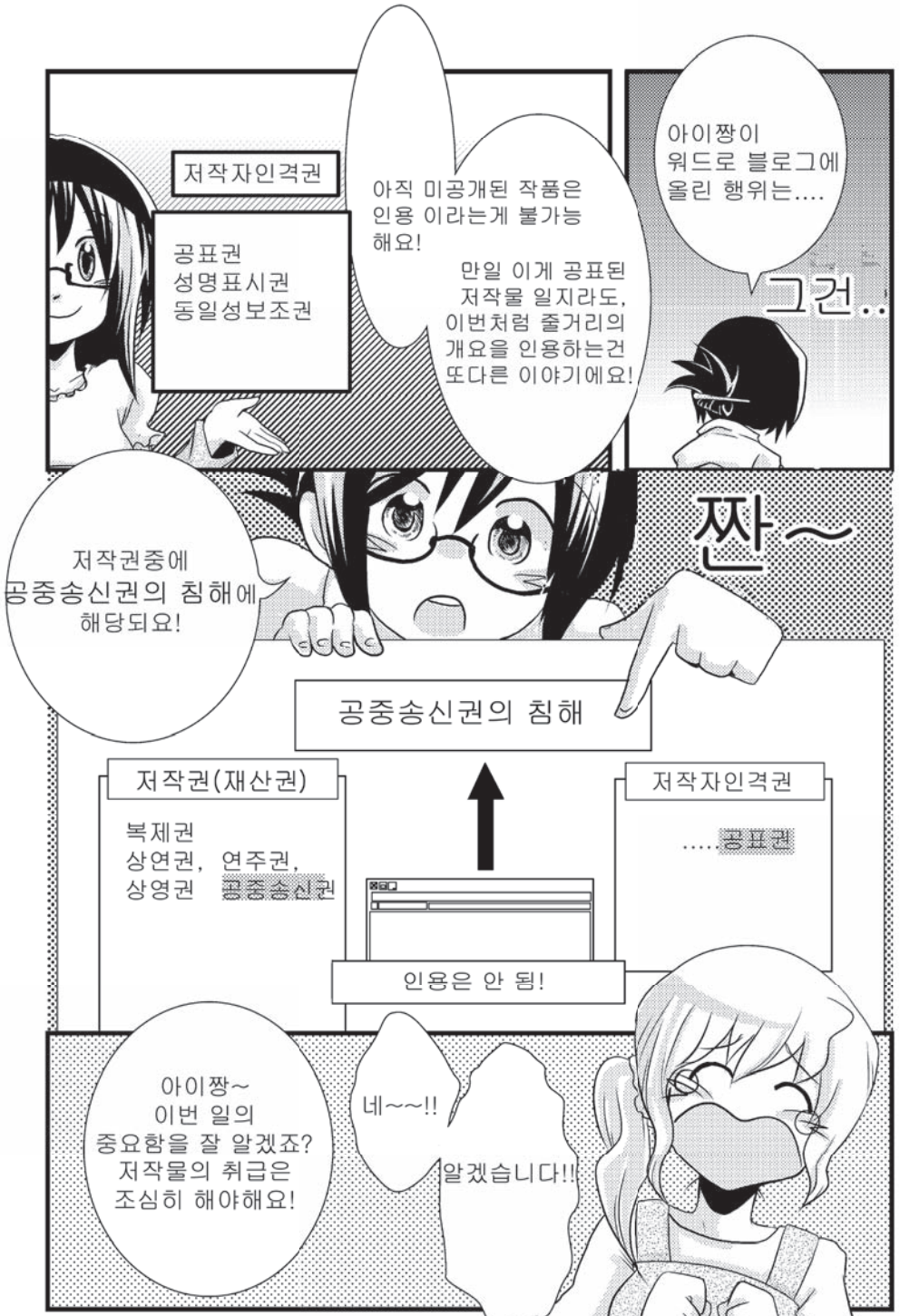

응? 아이짱 블로그에서 봤지?
아이짱..?
난... 소설책의 일부분만 살짝 말했을 뿐인데...
아이짱의 블로그에 올라왔다니..
그런 말씀 마세요~~!
그렇게 재미있으니까 괜찮지 뭐~
일부 사람만 볼 수있으면 아깝잖아~~
그런.. 문제가 아니잖아!!!
잠깐만 아이짱! 뭐좀 묻자!
도대체 어떻게 된거야?
으..
응..?

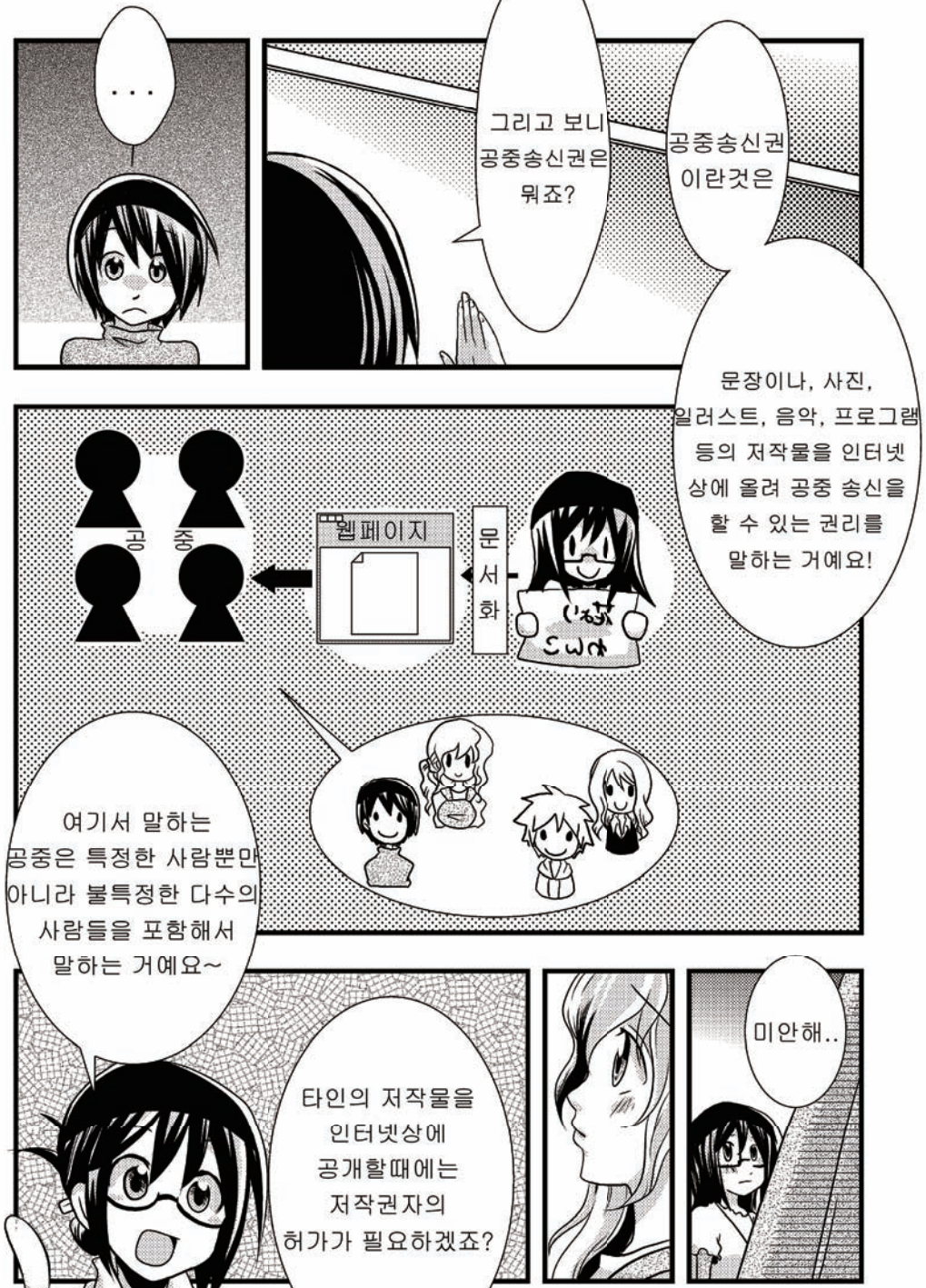

!
흑시 사토미짱 그 일 말야?
블로그 말이야 블로그!
아이짱이 왜! 내 소설을 블로그에 맘대로 공개하고 있는지 물어보는거야!
아~~~! 그거 말야~
응~ 그랬지~ 꽤 평도 좋아!!
코멘트도 많고 뭐 벌써 사토미짱이 대 인기 작가가 된것 같아~
호.. 평.. 이라니!
좀 심하지 않아?!
아무말도 없이말야!
일부 사람에게만 읽게 했고 아직 60%밖에 쓰지 않았다고! 그렇게 말했는데...
아.. 창피하게 시리..


그래도..
그냥..
난 완전 감동해서
사토미상의 소설을 다른 사람에게 알려주고 싶었던 것 뿐야..
그러니까!!
뭔가..
잘못된거야?
자~자~ 아이짱은 이야길 그냥 워드로 만들어서 올린것 뿐이잖아!
제 10화의 개요를 인용했다는 것 정도가 될까?
사토미짱의 작품이라고 표시도 했고!
그 쵸? 루 시!!
그건! 위험하죠!
이건 아이짱의 범죄행위가 될 수 있어요!
범죄요?


자! 들어 봐요!
아이짱
저작자 인격권 이라고 알아요?
네!
그.. 저작권에 대해서 말하는거죠?
저작자는 저작자인격권과 재산권 그리고 저작권을 가지고 있어요!
이런 권리들은 아래에 있는 것처럼 되어 있어요! 봅시다!
저작권(재산권)
복제권
상영권, 연주권,
상영권, 공중송신권 등
저작자인격권
공표권
성명표시권
동일성보존권


아이짱의 이번일은 저작인격권 중에 '공표권의 침해' 와 관련있어요!
어째서요? 사토미상이 아이짱에게 메일을 보낸 시점에서 공표된거 아닌가요?
사토미상은 특정한 친구에게 소설을 메일로 보냈지만
아직 이 시점에선 세상에 공표되었다고는 할 수 없어요! 사토미상이 아이짱에게 소설의 일부분을 메일로 보낸것도 그냥 평범한 송신으로만 취급돼요
송신
친구
친구
친구
아이짱
그래서 아직 공표되지 않은 사토미상의 소설을 허가 없이 공표한 행위는
재미 추천
들지 않아
공표권의 침해에 해당되죠!!


저작자인격권
공표권
성명표시권
동일성보조권
아직 미공개된 작품은 인용 이라는게 불가능 해요!
만일 이게 공표된 저작물 일지라도, 이번처럼 줄거리의 개요을 인용하는건 또다른 이야기에요!
아이짱이 워드로 블로그에 올린 행위는....
그건..
짠~
저작권중에 공중송신권의 침해에 해당되요!
공중송신권의 침해
저작권(재산권)
복제권
상연권, 연주권,
상영권 공중송신권
저작자인격권
.....공표권
인용은 안 됨!
아이짱~ 이번 일의 중요함을 잘 알겠죠? 저작물의 취급은 조심히 해야해요!
네~~!!
알겠습니다!!


...
그리고 보니 공중송신권은 뭐죠?
공중송신권 이란것은
문장이나, 사진, 일러스트, 음악, 프로그램 등의 저작물을 인터넷상에 올려 공중 송신을 할 수 있는 권리를 말하는 거예요!
공중
웹페이지
문서화
여기서 말하는 공중은 특정한 사람뿐만 아니라 불특정한 다수의 사람들을 포함해서 말하는 거예요~
타인의 저작물을 인터넷상에 공개할때에는 저작권자의 허가가 필요하겠죠?
미안해..

용어

【자료】

블로그

개인적인 일기 풍의 기사가 씌어진 웹 사이트. 인터넷 백서 2011에 의하면, 소셜 미디어의 이용률은, 블로그가 49.6%로 가장 높았지만, 작년도보다 5.1%줄었다. 한편, 이용률이 크게 오른 것은, SNS나 Twitter등의 마이크로블로그, Q&A커뮤니티다. SNS는 32.1% (작년보다 10.8% 증가), 마이크로블로그는 16.2% (작년보다 6.4% 증가), Q&A커뮤니티는 25.8% (작년보다 7.3%증가)이다. (참고 문헌:인터넷 백서 2011, 재단법인 인터넷 협회감수).

저작자인격권

저작권법에 있어서의 저작자의 권리는 크게 둘로 나눌 수 있다. 하나는 저작자인격권이며, 또 하나가 저작권(재산권)이다. 재산권으로서의 저작권은, 양도 가능하지만, 저작자인격권은 양도할 수 없는 저작자 고유의 인격적인 권리다. 예를 들면, 본고에 있는 저작물을 공개하는 권리(공표권), 성명을 표시할 것인가 아닌가 ,또한, 어떤 이름으로 표시할지를 결정되는 권리(성명표시권), 무단으로 변경되지 않는 권리(동일성유지권)로부터 구성된다.

2차적 저작물

전의 항목에서 말한 것과 같이, 저작물을 변경하기 위해서는, 저작자의 허락이 필요하다. 한편, 번역, 편곡, 변형, 각색 등의 번안을 한 결과, 새롭게 생긴 저작물을 2차적 저작물이라고 부른다. 2차적 저작물은, 원래의 저작물과는 달리 보호된다. 그 때, 원저작자는, 2차적 저작물의 저작자와 같은 권리를 가지기 때문에, 2차적 저작물의 복제나 배포 등도 원저작자의 허가가 필요가 된다. 2차적 저작물의 창작·이용에 관한 권리는 저작권(재산권)의 하나다.

공중송신

「공중」에 의해, 직접 수신되는 것을 목적으로 송신을 하는 것. 여기서 「공중」이란 불특정한 사람, 또는 특정다수의 사람인 것을 말한다. 따라서, 불특정한 사람에게 수신 가능하면, 가령 그것이 한 사람이어도 공중송신이다. 본고에 있듯이, 저작권자 이외의 사람이 공중송신을 하면, 공중 송신권의 침해가 된다. 한편, 특정다수라는 것은, 일반적으로는 50명을 뛰어넘으면 틀림없는 다수로 여겨지지만, 그렇지 않아도 다수로 간주될 수 있으므로 주의할 것.

저작권법의 구성

현재의 저작권법은, 쇼와(昭和)45년에 제정된 것이지만, 최근에는 몇 년에 1번은, 일부 개정이 행해지고 있다. 자세한 것은 법령검색 등으로 확인할 수 있다. 필요에 따라, 새로운 정보를 확인하면 좋다. 여기에서는, 저작권법의 구성에 대해서 말하겠다.

저작권과 저작인접권

우리나라의 저작권법에 지시된 권리는, 저작자의 권리와 저작인접권으로 크게 둘로 나눌 수 있다. 또, 그 각각이 인격적인 권리와 재산적인 권리로 구성되어 있다. 저작자의 권리는 저작물의 창작자의 권리, 저작인접권은 전달자의 권리다. 이하에서는, 양자의 차이에 대해서 비교해 보겠다.

저작인접권에는, 본고에서 문제가 된 저작자인격권의 공표권에 대한 권리는 없다. 이는 저작인접권은 처음부터 전달자의 권리이며, 공표를 전제라고 하고 있기 때문이다. 또, 재산권에 관해서는, 저작자의 권리는, 모두 허락권인 것에 대응하여 저작인접권에서는, 보수청구권이 있다. 허락권은 다른 사람에게 무단으로 사용되지 않는 권리이지만, 보수청구권은, 사용되는 것이 전제이며, 사용될 때에, 보수를 청구할 수 있는 권리다.

	저작자의 권리 (창작자의 권리)	저작인접권 (전달자의 권리)
인격적 권리	저작인격권 ・공표권 ・저자명 표시권 ・동일성보유권	실연가인격권 ・저자명 표시권 ・동일성보유권
재산적인 권리	저작권(재산 권) -복제권 -상해권,연주권,상영권.공중송신권 -공공의 전달권. 구술권.전시권 -부여권.수여권.대여권	저작 인접권(재산 권) -녹음.녹화권 -방송권.유선방송권 -송신가능화권 -수여권, 댕권

웹 카메라로 초상권을 침해?

【 목표와 포인트】

1. 초상권과 개인 정보에 대한 이해.

   ○ 법규에서 규정의 유무나 대표적인 판례를 이해한다.

   ○ 초상권 및 도촬 행위, 도난 방지 행위에 대해 생각한다.

   ○ 초상화 일러스트, 캐릭터의 초상권에 대해 조사한다.

2. 일반인의 초상권과 유명인의 초상권의 차이를 확인하고 이해한다.


카즈야군이..
왜 아직
동아리방에
있지?
오늘 5시
부터
아르바이트
라고
했는데?
어떻게.
이거 뭐야!
왜 연극부가
화면에
나오는거야?
몰랐어?
카즈야군이
아오야마상이랑
웹카메라로
연극부 상황을
웹으로 보여
준다고했어
교내에
서만..
뭐??
못들었어!
언제부터!?
지난주
부터였나?
지난주?!!!
그러면..
나도 모르게..
촬영되고
있었다는
거네…?;;
다..
다…
다….
근데
~
응?
아오야마
선배!!!
아!
아이짱!


저..기..요!
전 아무것도
못 들었는
걸요!!
뭘??
웹카메라
말이에요!
초상권
침해에요!
그런건!
다른사람
에게
말로
안하고
카메라로
찍는거요
저
질
…
최악!
저질!
신경쓰지마!
아오야마상!
우린 부원 모집을
위해서
교내여러사람에게
보여주려고했던것
뿐이잖아!
최악!저질!
최악!저질!
최악!저질!
악…!!
아이짱은
부원도 아니고
들어올지도
몰랐잖아!
깜짝!
힛


어쩔 수 없는건 아니잖아 카즈야군
아이짱은 누가 보는지도 모르게 찍힌게 기분이 나쁘다는거야~
큰 문제야!
맞아! 바로 그거야!

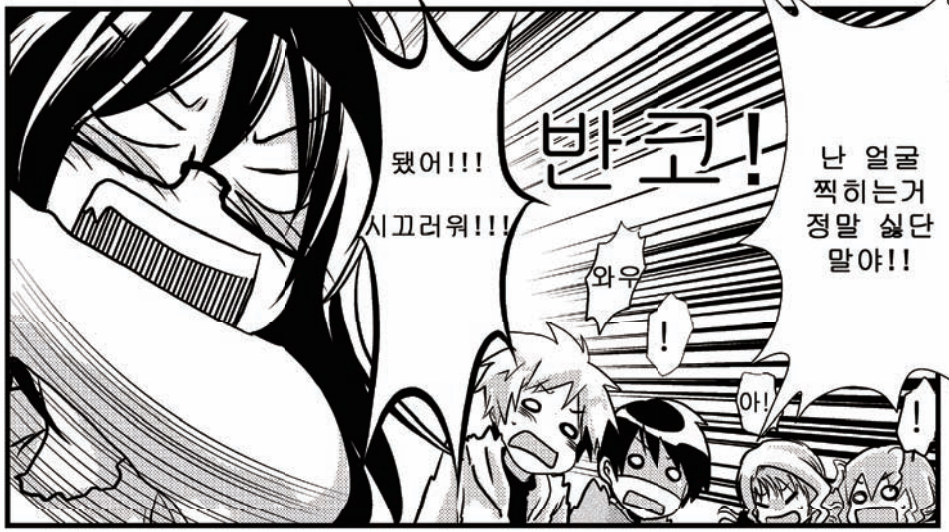

그리고 카즈야 오늘 아르바이트라고 하지 않았어? 내일 필요한 재료를 리카 혼자서 만들게 한 건 너무 한 거 아니야?
진짜 너무해 내시간 돌려내!!


그게 아냐 아이짱 오늘은 무대 소도구를 사러 가려고 쉰다고 말했던 거야!


그럼 정직하게 말하면 좋잖아!
그래 리카와 재료 만드는걸 미룬건 내가 잘못했어
그치만 부원획득을 위해 웹카메라로 우리 행동을 보여준게 저질인건 아니잖아!


그거야 말로 프라이버시 침해라고 생각하는데!!
적반하장도 유분수지!!
있을수없어!


뭐야…
너네..
아무튼 여긴편하게 지낼수가 없다니까
진짜 최악!


돼어!!!
시끄러워!!!
반코!
난 얼굴 찍히는거 정말 싫단 말야!!
와우
!
아!
!

판례에 따라 권리가 확인되어 있다

초상권에 대한 대표적인 판례는 1969년의 교토부학연 사건에관한 판결이에요.

이 판례에는 개인 사생활의 자유 중 하나로 무단 촬영을 당하지 않을 자유가 있다고 적혀있어요

이건 헌법에서 보장하는 생명, 자유, 행복 추구에 대한 권리를 근거로 하고 있어요

초 상 권

누구든지 무단 촬영 되지 않을 자유

헌법 13조

생명, 자유, 행복추구에 대한 국민의 권리

판례 1

교도부학연사건(1969년)

즉, 초상권이 헌법 수준에서 생각할 수 있는 것이라고 하는 판례입니다.

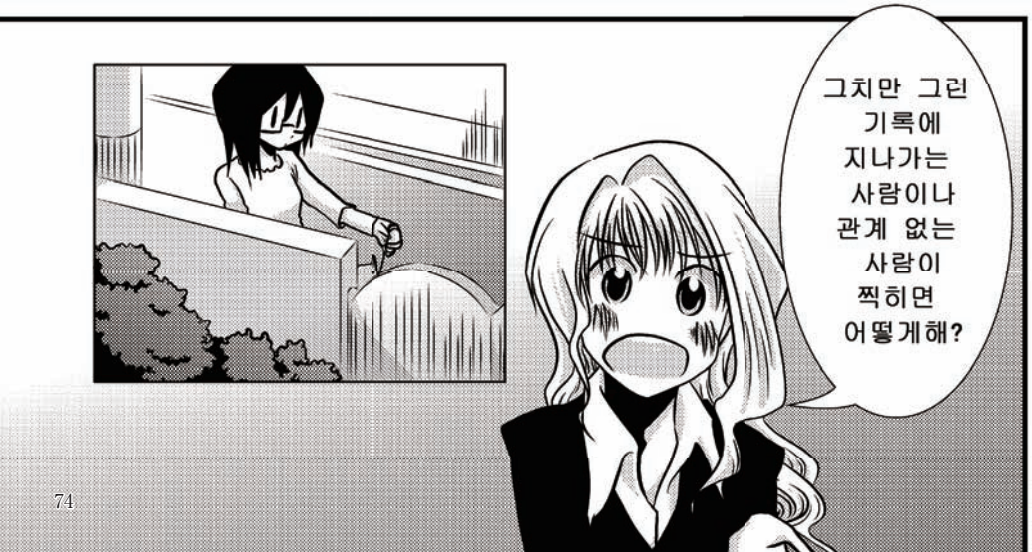

음.. 그치만 사소하게 나마 사람이 찍혔다면 풍경사진도 잘못된 일이 되어 버리잖아요..
일반 상식이랑 조금 다른가..?
초상권
그렇지 풍경사진을 찍어서 공개하거나 하는 것은 표현의 자유라고도 볼 수 있
표현의 자유와 초상권을 어떻게 조화시킬 수 있을까 하는 것도 생각해 볼 필요가 있는 것 같네요~
초상권이 어떠한 상황에서든 인정되는 것은 아니에요.
사회생활을 하다 보면 의도치 않게 무단 촬영을 당하게 되는 상황들이 있으니깐 말이에요.
판례 제 2!
법정 내의 도촬 사건(최고재판 2005년 11월)
무단촬용이 위법인지 아닌지는 찍힌 사람의 사회적 지위, 촬영 목적, 필요성 등을 고려해서 인격적 이익의 위협이 사회생활상 임무수행 한도를 넘어선 일인지를 판단해서 정한다.


촬영 당하는 사람이 어느정도 불이익이 생기는지, 촬영해서 공개할 필요성이 있는지를 잘 살펴봐야만 해
그 말은 촬영할 필요성이 있고 촬영당한 사람에게 불이익이 없다면 무단 촬영도 허용되는 경우가 있다는 거야?
그래도 조심해야 해~ 촬영할 필요성이 있어도 마음대로 생각해서는 안 돼!
어디까지나 대립하는 권리나 자유가 있을 경우에는 균형의 문제가 있어서 간단하게 말할 수는 없어
그러니까 촬영방법 예를 들면, 몰래 촬영하는 상황에서 찍힌 상황은 결국 허용되지 않는 거죠!
이건 촬영한 필요가 있어서~
초상권 침해야!
대립하는 자유, 권리
초 상 권
촬영의 필요성 : 제멋대로 생각해서는 안 됨!


도촬말인가?
핸드폰으로
찍어도
때때로
초상권 문제가
된다는 거네요..
맞아!맞아!
그러니까
웹카메라는
더욱
반대!
그런 건 도촬이야!!
그래..
그래..


그치만,
웹카메라는
도촬이 아니라
도난 방지
목적으로
사용되기도
하잖아~
그건
어떻게
되는거지?

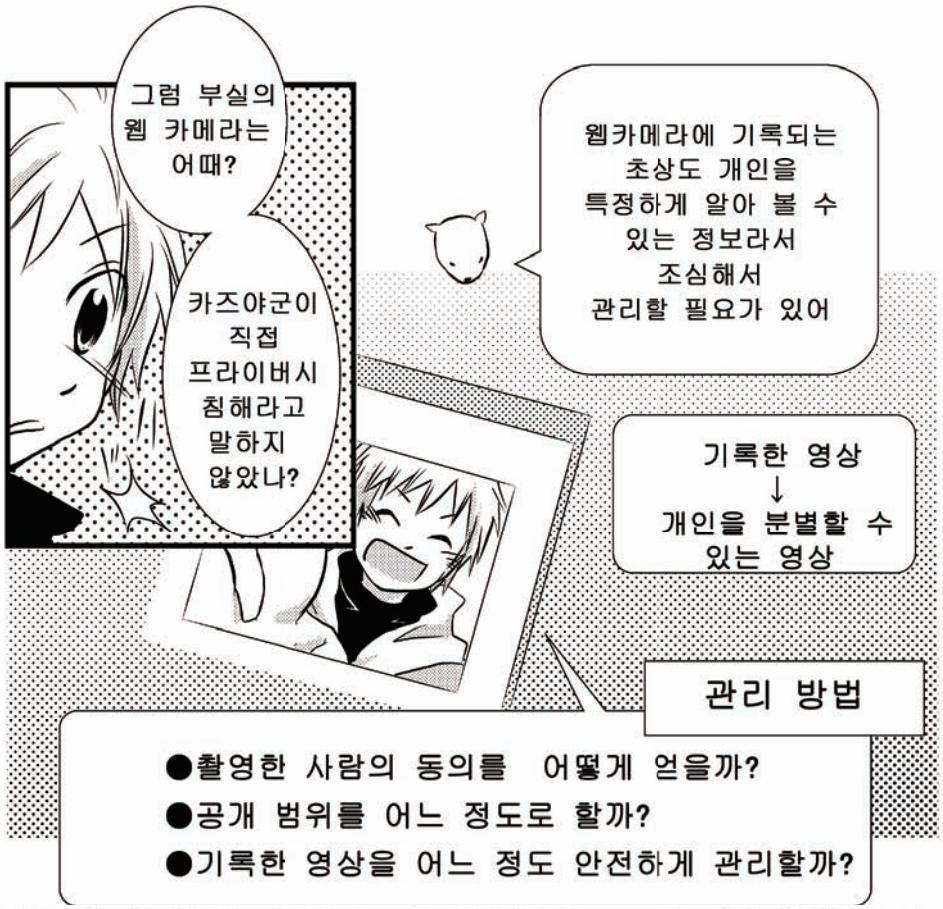

괜찮지 않을까?
집에 도둑이
드는걸 카메라에
기록한다고 해서
아무도 탓할
사람은 없잖아~


그치만 그런
기록에
지나가는
사람이나
관계 없는
사람이
찍히면
어떻게해?

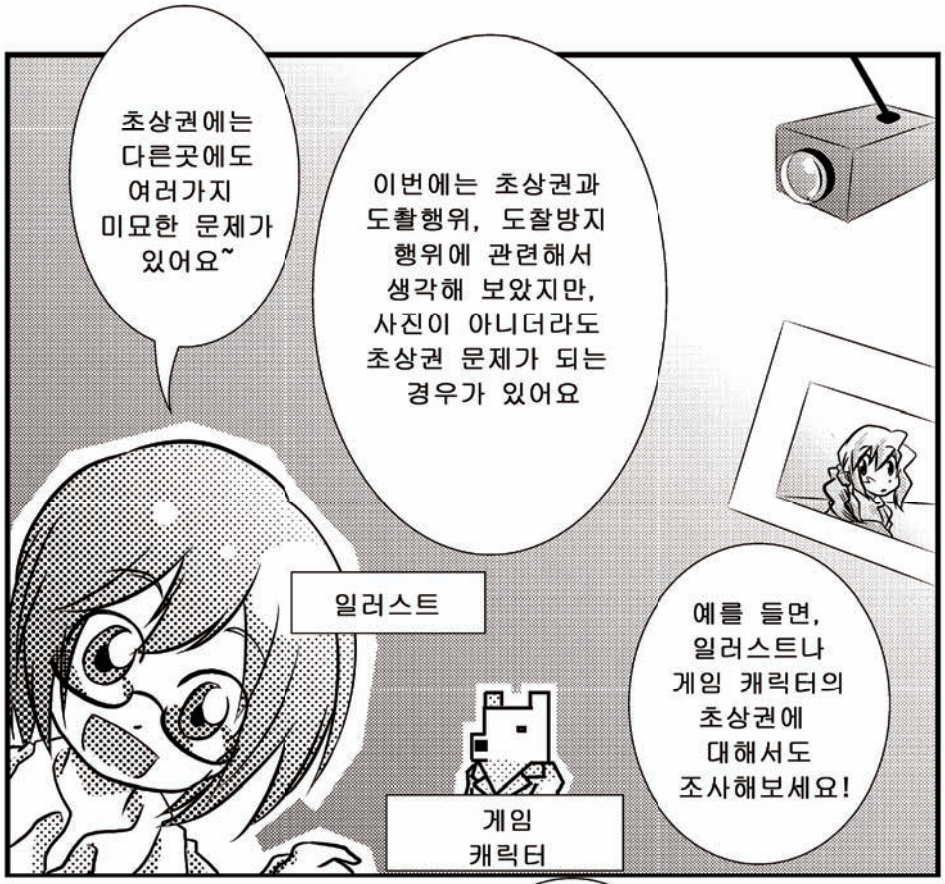

웹카메라나
방법 카메라는
영상 그 자체 뿐만
아니라
기록된 영상의
관리에 대해서도
문제가 되는거 아냐?


맞아!
은행에 가면
[방법카메라 작동 중]이라는
종이가 있어도
그걸
[프라이버시 침해]라고
생각하는 사람은
거의 없잖아~
그건 방범이라는
목적이 확실히 있는
거라 그렇기도
하지만 관리도
관리도
확실하게 하지
않은면 안되는거야~


방법 카메라에
초상이 유출되면
카즈야군이 언제
은행에
갔는지 정보들이
누출되고.. 그러면
곤란하지 않겠어?
그건 곤란하죠~
완전 당연 한 거라고
생각해요!


그럼 부실의 웹 카메라는 어때?
카즈야군이 직접 프라이버시 침해라고 말하지 않았나?
웹카메라에 기록되는 초상도 개인을 특정하게 알아 볼 수 있는 정보라서 조심해서 관리할 필요가 있어
기록한 영상
↓
개인을 분별할 수 있는 영상
관리 방법
●촬영한 사람의 동의를 어떻게 얻을까?
●공개 범위를 어느 정도로 할까?
●기록한 영상을 어느 정도 안전하게 관리할까?


특히, 촬영당한 사람의 동의를 어떻게 얻을까? 공개범위를 어느정도로 할까? 기록한 영상을 어떻게 안전하게 관리할까 등은 확실히 규칙으로 정해두는게 좋지요!
웹카메라나 방법 카메라는 영상 그 자체 뿐만 아니라 기록된 영상의 관리에 대해서도 문제가 되는거 아냐?


초상권에는 다른곳에도 여러가지 미묘한 문제가 있어요~
이번에는 초상권과 도촬행위, 도찰방지 행위에 관련해서 생각해 보았지만, 사진이 아니더라도 초상권 문제가 되는 경우가 있어요
일러스트
게임 캐릭터
예를 들면, 일러스트나 게임 캐릭터의 초상권에 대해서도 조사해보세요!


대립하는 권리와 자유가 있을 때 어떻게 생각해 보면 좋을까?
여러분들도 촬영하는 쪽, 촬영당하는 쪽, 양쪽의 입장을 여러방면에서 모두 생각해 보세요!

용어

【자료】

초상권

사람의 용모나 자태, 즉 초상에 대한 권리다. 무단으로 초상을 촬영되지 않는 인격적인 권리로 여겨진다. 그러나, 법문상의 규정은 없고, 재판소의 판례에 의해 확인되어 온 권리다. 그 근거는 일본 국헌법 13조의「개인의 존중, 행복추구권, 공공의 복지」로 여겨진다. 또, 배우 등의 초상은, 스스로 쟁취했던 명성 때문에, 대가를 얻으며 이용시킬 수 있는 이익을 소유하는 것이며, 인격적 이익과는 이질적인, 독립된 경제적 이익을 소유 한다로 여겨진다. 이 권리는 퍼블리시티권 등으로 불린다. 2012년2월2일, 대법원제1소법정에서는,「초상 등은, 상품의 판매 등을 촉진하는 고객흡인력을 소유할 경우가 있어, 이러한 고객흡인력을 배타적으로 이용하는 권리」를「퍼블리시티권」이라고 사법으로 처음으로 정의하고,「①초상 등 그것 자체를 독립시켜 감상의 대상이 되는 상품 등으로서 사용, ②상품 등의 차별화를 꾀할 목적에서 초상 등을 상품 등에 첨부, ③초상 등을 상품 등의 광고로서 사용 등」의 경우의 위법성에 언급했다.

프라이버시 (사생활침해)

일본에서는, 사생활침해에 대해서도, 초상권과 동일하게 법문상의 정의는 없고, 판례에 의해 확인되고 있다. 워렌과 브랜다이스는, 사생활을, 1890년,「the right to be let alone」라고 정의하고 있다. 정보화가 나아가는 중에, 자기정보 컨트롤권 (자기의 사생활에 영향을 미치는 정보를 컨트롤 할 수 있는 권리)로서도 생각되어 오고 있다.

개인정보보호법

개인정보보호법은,「개인정보의 유용성에 배려하면서, 개인의 권리이익을 보호하는 것」을 목적으로 해서 제정되고 있다. 개인정보보호법에 있어서의 개인정보란, 생존하는 개인에 관한 정보이며, 성명, 생년월일, 기타의 기술로 특정한 개인을 식별할 수 있는 것이다. 메일 주소 만으로는 개인정보가 안되지만, 다른 정보와 대조하는 것으로 개인을 식별할 수 있는 것이라면, 개인정보가 된다.

표현의 자유

표현의 자유는, 일본국헌법 21조「집회, 결사 및 언론, 출판 기타 일절의 표현의 자유는, 이것을 보장한다. 」로 되어, 보장되고 있다. 본고에서는, 표현의 자유와 초상권과의 균형의 이야기가 나오고 있지만, 대립하는 권리가 있을 때는, 어떻게 해야 할까? 본문에서 나오는 두 개의 판례(교토부(京都府)학연사건, 포커스의 법정 내 몰래 사진 사건)의 의도하는 것을 지금 한번 더, 확인하고자 한다.

초상권에 관한 대법원판례 「포커스」의 법정내의 도촬 사건: 사건번호 헤이세이15(受) 281

사건명 (손해 배상)	재판일 2005년 11월10일
법정명 대법원제1소법정	
결과 기타	판례집 제59권 9호 2428페이지
원심재판소명:오사카(大阪) 고등법원	재판일 헤이세이14년11월21일

판시사항

1. 사람의 용모, 자태를 그 승낙 없이 촬영하는 행위와 불법 행위의 여부
2. 사진주간지의 카메라맨이 형사사건의 법정에 있어서 피의자의 용모, 자태를 촬영한 행위가 불법 행위법상 위법으로 여겨진 사례
3. 사람의 용모, 자태를 묘사한 일러스트 그림을 공표하는 행위와 불법 행위의 여부
4. 형사사건의 법정에 있어서의 피고인의 용모, 자태를 그린 일러스트 그림을 사진주간지에 게재해서 공표한 행위가 불법 행위법상 위법이라고는 말할 수 없다고 여겨진 사례
5. 형사사건의 법정에 있어서 신체의 구속을 받고 있는 상태의 피고인의 용모, 자태를 그린 일러스트 그림을 사진주간지에 게재해서 공표한 행위가 불법 행위법상 위법으로 여겨진 사례

재판 요지

1. 사람은 함부로 자기의 용모, 자태를 촬영되지 않는다는 것에 대해서 법률상 보호되어야 할 인격적 이익을 소유하며, 어떤 사람의 용모, 자태를 승낙 없이 촬영하는 것이 불법 행위법상 위법이 될 것인가 아닌가는, 피 촬영자의 사회적 지위, 촬영된 피 촬영자의 활동 내용, 촬영의 장소, 촬영의 목적, 촬영의 태도, 촬영의 필요성 등을 종합 고려하고, 피 촬영자의 상기 인격적 이익의 침해가 사회 생활상 받아들여야 할 한도를 넘는 것이라고 말할 수 있는 것인가 아닌가를 판단해서 결정해야 한다.
2. 사진주간지의 카메라맨이, 형사사건의 피의자의 동정을 보도할 목적에서, 구류 이유공개 수속이 행해진 법정에서 용모, 자태를 그 승낙 없이 촬영한 행위는, 수갑을 하고, 노끈을 붙여진 상태의 용모, 자태를, 재판소의 허가 없이 몰래 찍은 것 등 판시의 사정 아래 불법 행위법상 위법이다.
3. 사람은 자기의 용모, 자태를 묘사한 일러스트 그림에 대해서 함부로 공표되지 않는 인격적 이익을 소유하지만, 그 일러스트 그림을 공표하는 행위가 사회 생활상 받아들일 수 있는 한도를 넘어서 불법 행위법상 위법으로 평가될 것인가 아닌가의 판단에 있어서는, 일러스트 그림은 그 묘사에 작자의 주관이나 기술을 반영하는 것이며, 공표되었을 경우도, 이것을 전제로 한 받아들여짐을 한 다는 특징이 참작되지 않으면 안 된다.

4. 형사사건의 피고인에 대해서, 법정에 있어서 소송 관계인에게서 자료를 보여져 있는 상태 및 손짓을 섞어가며 이야기하고 있는 상태의 용모, 자태를 그린 일러스트 그림을 사진주간지에 게재해서 공표한 행위는, 불법 행위법상 위법이라고 말할 수 없다.
5. 형사사건의 피고인에 대해서, 법정에 있어서 수갑, 노끈에 의해 신체의 구속을 받고 있는 상태의 용모, 자태를 그린 일러스트 그림을 사진주간지에 게재해서 공표한 행위는, 불법 행위법상 위법이다.

참조법조

(1~5에 대해서) 민법 709조, 민법 710조, 헌법 13조 (2에 대해서) 형소송규칙 215조 이밖에, 아래에서 교토부(京都府)학연사건에 관한 판례를 확인할 수 있다 (2012년3월9일 열람).

사건번호 쇼와(昭和)40(ぁ) 1187

재판 연월일 쇼와(昭和)44년12월24일

사건명 (공무집행 방해, 상해 피고사건)

법정명 대법원대법정재판

종별 판결

결과 기각

판례집 권·호·페이지 제23권 12호 1625페이지

원심재판소명:오사카(大阪) 고등법원

재판소판례검색 시스템

;http://www. courts. go. jp/search/jhsp0010? hanreiSrchKbn=01

교토부(京都府)학 연사건의 판례

;http://www. courts. go. jp/search/jhsp0030? hanreiid=51765&hanreiKbn=02

컴퓨터에 몰래 잠입해 들어오는 스파이웨어

【 목표와 포인트】

1. 스파이웨어 및 허위 안티 바이러스 이해.

   - 바이러스 백신을 가장한 악성 소프트웨어의 존재를 인식한다

   - 스파이웨어에 의한 스팸 메일 문제에 대해 생각한다.

2. 스파이웨어와 키로거 등에 의한 정보 유출에 주의한다.

   - 인터넷 카페 등에서 관리되지 않는 공용 컴퓨터를 사용할 때 위험을 생각한다.


뭐가 문제라도 되는거야?
이거 인스톨한지 일주일밖에 안됐단 말야!
근데 벌써 업데이트 라니!
게다가, 업데이트에 60달러나 든다니..
너무 비싼거 같은데 원래는 얼마 정도야?
이상하지?!
음...
뭘 중어러기고 있어 공 여기 있어!
그래서 리카짱 그 컴퓨터 어떻게 됐어?!
그렇게 온거야?
이것 좀 봐봐~
어~
우아~ 이 화면 좀 이상하네~
응응!
도데체 어떻게 했길래 이렇게 된거야?
사실은 일주일 전에 말야 ….


일주일 전
♪
띵~똥~
이 컴퓨터는 바이러스에 감염되어 있습니다. 지금 바로 백신 소프트웨어를 인스톨해 주세요.
인스톨
앗~ 이색깔 좋네... … 응?
그래서?
그래서.. 생각없이 놀래서 그냥 인스톨해 버렸어..
근데, 오늘 느닷없이 60달러로 업데이트 하세요. 라는 화면이 뜨는거야!
좀 수항하기도 하고 뭔가 끈질기기도 하고 어쩜 좋아~~
꽤 위험한걸 그 백신소프트웨어
바로 삭제하는게 좋을것 같아.
역시.. 삭제할 수 밖에 없는 건가? …. 응?


왜 그래?
어?
아
일단은 언인스톨!! 언인스톨!!
아오야마상 슬슬 가자~
안 될리가 없잖아!
몇번이나 했는데.. 삭제가 잘 안돼....
응..
그런...
미안~ 우리지금 역앞에 있는 PC방 갈꺼니까~
미안~ 열심히해서 삭제해둬~
그리고 공 정리도 좀 해줘~~
자.. 잠깐! .. .. ?!
미안~ 바이바이~
치사해..
삭제.. 라니.. 그게 안 되니까 이러는거 아냐!!!
정..말!! 나도 나중에 갈께!!
힘내~!!


응?
우~아
대량의 스팸메일
!
내 주위에 이 주소를 알고 있는 사람은 아오야마 정도 밖에 없는데..
? !
이 메일주소 블로그 용으로 만든건데
와.. 이거 심한데..
온통 스팸메일 이에요
아오야마 상 이것좀 봐요~
응?
설마 아오야마 상이...
설마..
그게 나 일리 없잖아!


내가 메일 주소를 흘리고 다니진 낳았으니까
그러니까 아오야마상 밖에 없다는건데..
쨍그랑~!
뭐야 그게!
좀 심하지 않아!!
스팸메일이 내 탓 이라는거야? 내가 그런 일을 할 사람으로 보여!
그렇게 나오면 나도 할 얘기가 많다고!!
최근 내 메일에도 스팸이 늘었던데..
저를 의심하는거에요? 아무리 선배라고 해도 그건 좀 아니..죠~
뭐야.. 이 분위기 .. 싸우는 거야?
으~~으~~
계속 생트집 잡는게 누군데..
난 그 이상한 소프트웨어 삭제가 안 되서 힘들어 하고 있는데..
이제 안되겠다! 루시! 도와줘~~!!


Hey, Come down! Cool it!
둘 다 침착해 원인은 다른 곳에 있으니까~
네?
들어봐~ 힌트는 바로 PC방 그 컴퓨터!
이... PC방의 이.. 컴퓨터?
카즈야군과 아오야마군은 여기 PC방 회원이죠?
아! ... 네!
둘 다 이 PC방에서 메일을 보내거나 한 적 없어?
네?
아마도 여기 컴퓨터는 스파이웨어에 감염되어 있을꺼야~
그게 원인으로 너희들의 메일 주소가 스팸메일 발신자에게 알려진거지~
에...?


스파이웨어란,
개인정보 등의
기록을
허가없이
가져가도록
만든
소프트웨어예
요
그러니까,
이런곳의
컴퓨터를
사용할 때는
충분히
주의해야
하는 겁니다!
PC방의
컴퓨터는
불특정 다수의
사람이
사용하죠?
누군가
키보드
해킹소프트웨어를
설치해서
당신이 입력하는
정보를 절치하고
있는 가능서도
있죠~
키보드
해킹
프로그램
...
?!
이럥?
키보드해킹
프로그램이란
어떤 명령어를
키보드로
입력했는지를
전부 기록한
다음에
이력정보를
출력하는
툴이야
기억
합니다.
출력
합니다


원래는
감시목적이나
백업하기
위한
수단으로
이용되었는데
컴퓨터에
몰래
심어 놓고
패스워드나
신용카드 번호
등을
몰래
빼내는
사례가
증가하고
있습니다
통신기능을
가지고
키보드 조작
정보를
외부에 송신하는
것까지
등장했으니까
충분히
조심하지 않으면
안 되요!
너무
해요~
그래~?
그러니까
카드번호 같은
중요한
정보를
입력해서는
절~ 대
안 된다니까~
카즈야군
아오야마군
Understand?
아...
네...


넷!
저 말이죠?
앗싸!
좋아~
그럼 다음은
리카군이네?
백신프로그램
으로
위장한
컴퓨터
바이러스와
같은거죠~
리카군이
인스톨한
백신프로그램인데
그건 실제로 위장
백신프로그램이란거
알고 있어?
위장백신프로그
램은 검색
페이지나
다른 사이트 링크,
메일 등에서
유저를 자신의
웹사이트로
유도해요
그건..
뭔가요??


바이러스!?
그래서
유저 컴퓨터가
바이러스에
감염된 것처럼
보이게 해서
위장
소프트웨어를
인스톨하도록
하는 거에요
거기에는
스파이소프트웨
어가
숨겨져 있는
경우도
있어서, 일단
인스톨 하면
그 소프트웨어의
요금을
지불하도록
표시하죠
발견되었습니다
백신프로그램을
인스톨하세요

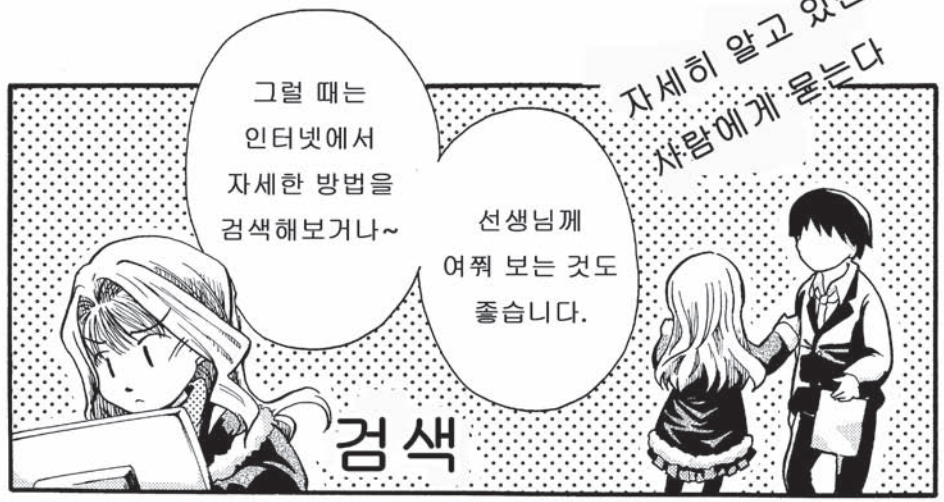

그 표시에 있는
링크를 따라가
결제사이트에서
요금을 내도
잠시 동안
경고표시가
안 나오지만
금방 다시 다른
종류의
경고 표시가
나타나도록
되어 있어요
지불해
주세요
...


우와~ 무서워라
근데 말야
원래 리카군의
컴퓨터에는
백신프로그램은
설치되어 있는거지?
백신프로그램
두 개 설치
한다고해서
성능이 두 배로
좋아지는건
아냐~
갑자기
바이러스에
감염되었다고
해서
깜짝
놀란거라고..


결국 바이러스나
키보드 해킹
프로그램에
주의해야
하는 것도
중요하지만
무심코,
위장 백신
프로그램을
설치하지
않도록 주의하는
것도 필요하단
말씀이죠...
That 's
right .
그렇죠!!


컴퓨터에
새로운
프로그램을
인스톨할 때에는
충분한 주의가
필요해요~
네
옙
저기 있잖아...
새로운 프로그램을
인스톨할 때
주의할 필요가 있는 건
알겠는데...


그 위장
백신프로그램을
지우려면
도대체 어떻게
해야하냐고!!
몇번을
해봐도
삭제가
안 된다
말이에요!!


자세히 알고 있는
사람에게 묻는다
그럴 때는
인터넷에서
자세한 방법을
검색해보거나~
선생님께
여쭤 보는 것도
좋습니다.
검색


또한
피해가
심각한
경우에는
[초기화] 같이
처음 컴퓨터를 샀을
때와
같은 상태로
복구 시키는
힘든 작업이
필요할지도 몰라요
에
...
?!
초
기
화
???
그래도
계속 불편한 것
보단 낫잖아
비싼 수업료
낸 샘치고
힘내렴!!
우...
우...
아~
네....
아...
덧붙여서
공 정리는
안 했어~~
뭐라고!!!

【자료】

용어

스파이 웨어

개인적인 정보나 이용자의 컴퓨터의 움직임 등을 감시하고, 작성원에 보내는 프로그램이다 어떤 소프트웨어의 인스톨 시, 함께 인스톨 될 경우가 많다. 개인적인 정보가 의도치 않게 흘러 나가지는 것 등이 문제가 되고 있다.

위조백신 소프트

문자 그대로, 가짜 바이러스 대책 사이트다. 바이러스에 감염하고 있는 취지의 메시지나 가짜 바이러스 검출 화면을 이용자의 PC 화면에 표시시켜, 이용자에게 대책을 위해서는 유상의 소프트웨어의 인스톨이 필요한 것을 강요한다. 일단, 인스톨해버리면, 원상태로 돌리는 것이 곤란할 경우가 있으며 최악의 경우 하드 디스크의 초기화를 하지 않으면 안될 경우도 있다. 감염 경로는, 메일의 첨부 파일을 열거나, 부정한 프로그램이 장치되어 있는 웹 사이트를 열람하는 것 등이 많다. 백신 소프트를 최신 버전으로 유지하는 것, 스팸 메일 등 의심스러운 메일은 열지 않는 것 등에 주의 하는 것이 좋다.

키로거

키보드로부터의 입력 정보를 감시해서 기록하는 것. 기록한 정보를 외부에 송신하는 것도 있다. 이용자 자신이 적절하게 사용하는 한에 있어서는 도움이 되는 것이지만, 인터넷 카페 등 공용으로 사용하는 PC에서는, 악의를 품고 설치 할 수가 있어, 비밀번호 등이 도난 당할 우려가 있기에 주의가 필요하다. 어떻게 관리되고 있을지 명확하지 않은 PC에서는, 비밀번호나 개인정보를 입력하지 않도록 한다.

공용 PC

대학 PC도 여러분이 공용으로 사용하는 PC지만 인터넷 카페와 같은 익명의 것과는 근본적으로 관리 형태가 다르다. 대학 PC에서는 PC의 상태를 매번 초기화하거나, 바이러스 대책을 최신 버전으로 한 상태에서 PC를 이용한 ID와 이용한 PC의 이용 이력 등을 관리하는 것이 보통이다.

형법등의 개정

2011년, 정보처리의 고도화 등에 대처하기 위해서 형법이 개정되었다. 이 개정으로, 소위 컴퓨터바이러스에 관한 죄가 신설되고 있다.「정당한 이유 없이, 사람의 전자계산기에 있어서 실행의 동시에 발생될 목적으로」, 소위 컴퓨터바이러스를 작성, 제공 등을 했을 경우에는 죄가 된다.

스파이웨어

여기에서는 공용으로 사용하는 컴퓨터가 스파이웨어에 감염한 예를 제시했다. 그러나, 스파이웨어는, 공용의 컴퓨터뿐만 아니라, 여러분의 PC에 잠입할 가능성도 있다. 스파이웨어는 몰래 동작하기에 이용자는 그 존재를 알아차리지 못하는 경우가 많고 모르는 사이에 자신의 정보가 외부에 유출된다. 또, 어떤 정보가 외부에 유출 되었는지는 그 스파이웨어에 따라 다르기 때문에, 그 위험성은 한마디로 표현할 수 없다. 여기에서는 어떻게 감염 되는 것인가 또 어떤 대책이 가능한가에 대해서 검토해 본다.

스파이웨어의 감염 경로

①무료 소프트웨어 등을 인스톨할 때에, 함께 인스톨된다.
②악의 있는 웹 사이트를 열람했을 때에, 자동적으로 인스톨된다.
③메일에 첨부된 파일을 실행하는 것으로 인스톨된다.
④컴퓨터의 보안 취약점을 뚫어서 인스톨된다.

스파이웨어에 관한 대책 예시

①스파이웨어 대책 소프트를 이용한다. 소프트웨어는 최신의 버전으로 갱신한다.
②수상한 사이트나 메일, 화면 표시되는 수상한 메시지 등에 주의한다.
③컴퓨터에 보안 취약점이 없도록, 컴퓨터를 최신 버전으로 유지한다.
④브라우저의 보안 설정을 체크한다.

스파이웨어에 감염했을 경우, 최악의 상황으로 컴퓨터의 초기화가 필요하게 될 경우가 있다. 따라서, 상기와 함께, 필요한 데이터는 적절히 백업을 해 두길 바란다.

위조백신 소프트

리카(梨花)씨는 위조백신 소프트를 인스톨해버린다. 바이러스에 감염되었다는 메시지를 내면서 이용자를 놀라게 하여 부주의하게 소프트웨어를 인스톨시켜버리는 수법이다. 독립 행정법인정보처리추진기구 보안 센터에 의하면 2012년에 들어와서「위조백신 소프트」형의 바이러스가 늘어나고 있다고 한다. 감염 수법은 취약점이 있는 PC에 대하여 웹 사이트 열람 시에 바이러스를 감염시키는 타입이다. 취약점의 해소와 함께 중요한 데이터는 백업을 취하는 것을 유념 해둘 필요가 있다.

원클릭 청구

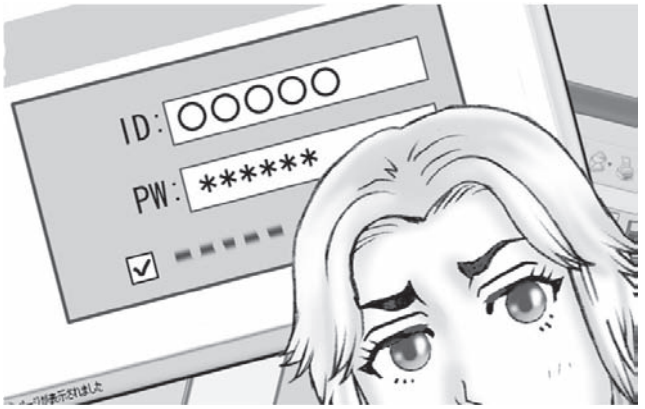
현재, 여러 가지 사기가 횡행하고 있지만, 이 항목에서는 원클릭 청구에 대해서 보충한다. 원클릭 청구는, 메일이나 웹 사이트에 있는 버튼을 클릭함으로써 입회비용이나 열람료 등의 지불 의무가 생긴 것처럼 보여지게 만드는 사기다. 실제로는 입회 등의 의사가 없이 의도에 반하여 단순하게 클릭해버린 것만으로는,「전자소비자계약법 (통칭:주)」의 보호 아래, 지불의 의무는 생기지 않는다. 그러나 최근에서는 다음과 같은 수법이 교묘히 되어가고 있어 주의가 필요하다.

·이용 규약의 화면에서 동의를 시키는 것
·처음에는 무료로 보이게 만들어 안심시키는 것
·악의 있는 프로그램을 실행시켜, 요금청구 화면을 빈번하게 표시하여, 심리적으로 공격하는 것
…등으로, 교묘하게 이용자를 올가미에 빠지게 하는 것이다.

이용 규약화면에서 동의를 얻음으로써, 반드시 위법이라고는 말할 수 없는 수법을 사용하고 있기에 충분히 주의할 것. 독립 행정법인정보처리추진기구 보안 센터에 게재되고 있는 이번 달의 호소 2012년2월은,「스마트 폰이라도 원클릭 청구에 주의! 」라는 주제다. 스마트 폰의 원클릭 청구의 구체적인 예로서, 바이러스에 감염하면 해당 스마트 폰의 전화번호나 메일 주소 등이 원클릭 청구 업자에게 자동 송신되는 것을 예로 들 수 있다, 악질성은 PC에서의 원클릭 청구만큼 올라가고 있다. 부주의하게 어플리케이션을 넣지 말고, 보안 대책을 해 두는 것이 중요하다.

상세한 것은 아래URL을 참조※ (2012년3월9일 열람).
주:「전자소비자계약법」의 정식명칭은,「전자소비자계약 및 전자승낙 통지에 관한 민법의 특례에 관한 법률」이라고 한다.

악의성 웹 페이지



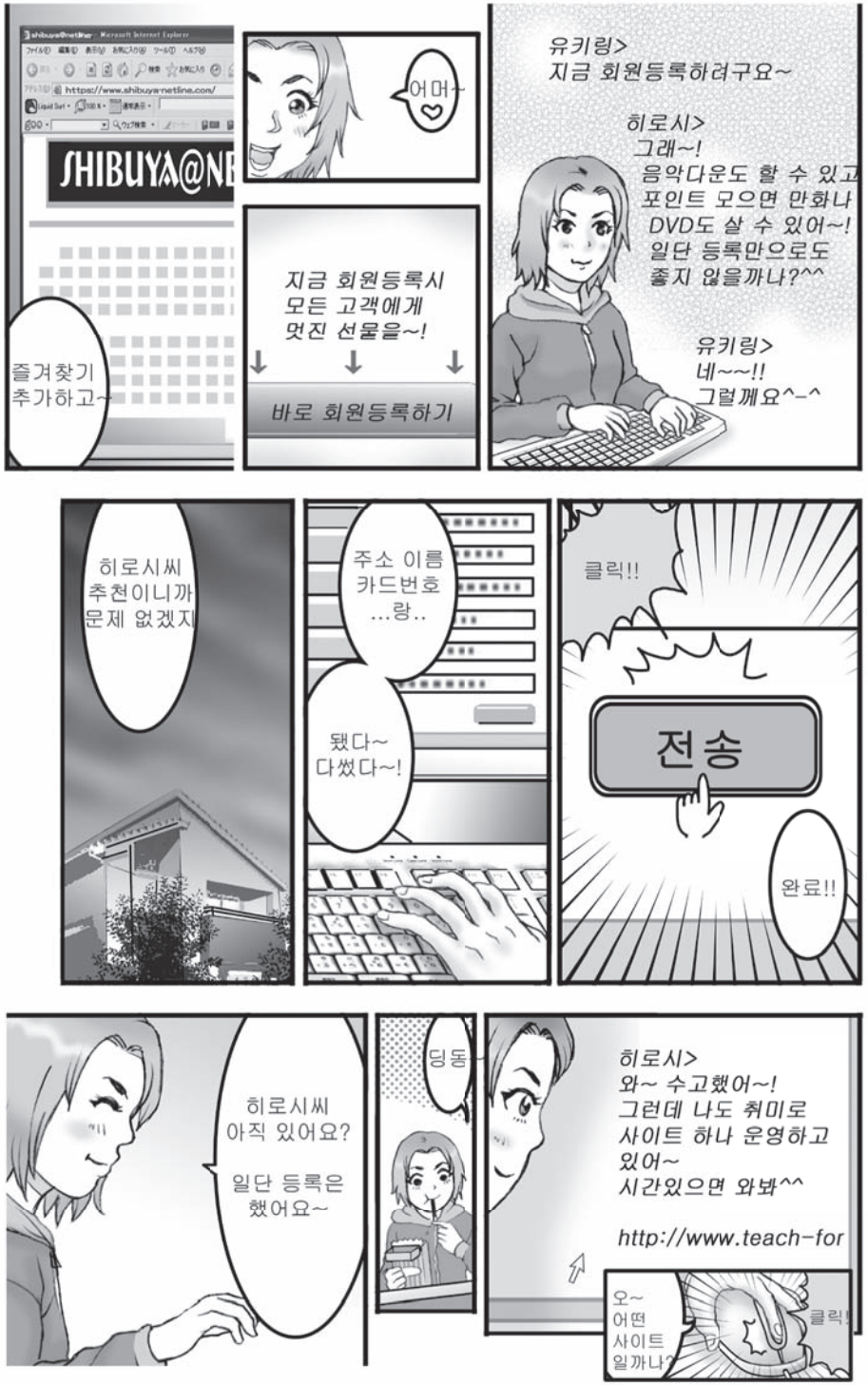
【 목표와 포인트】

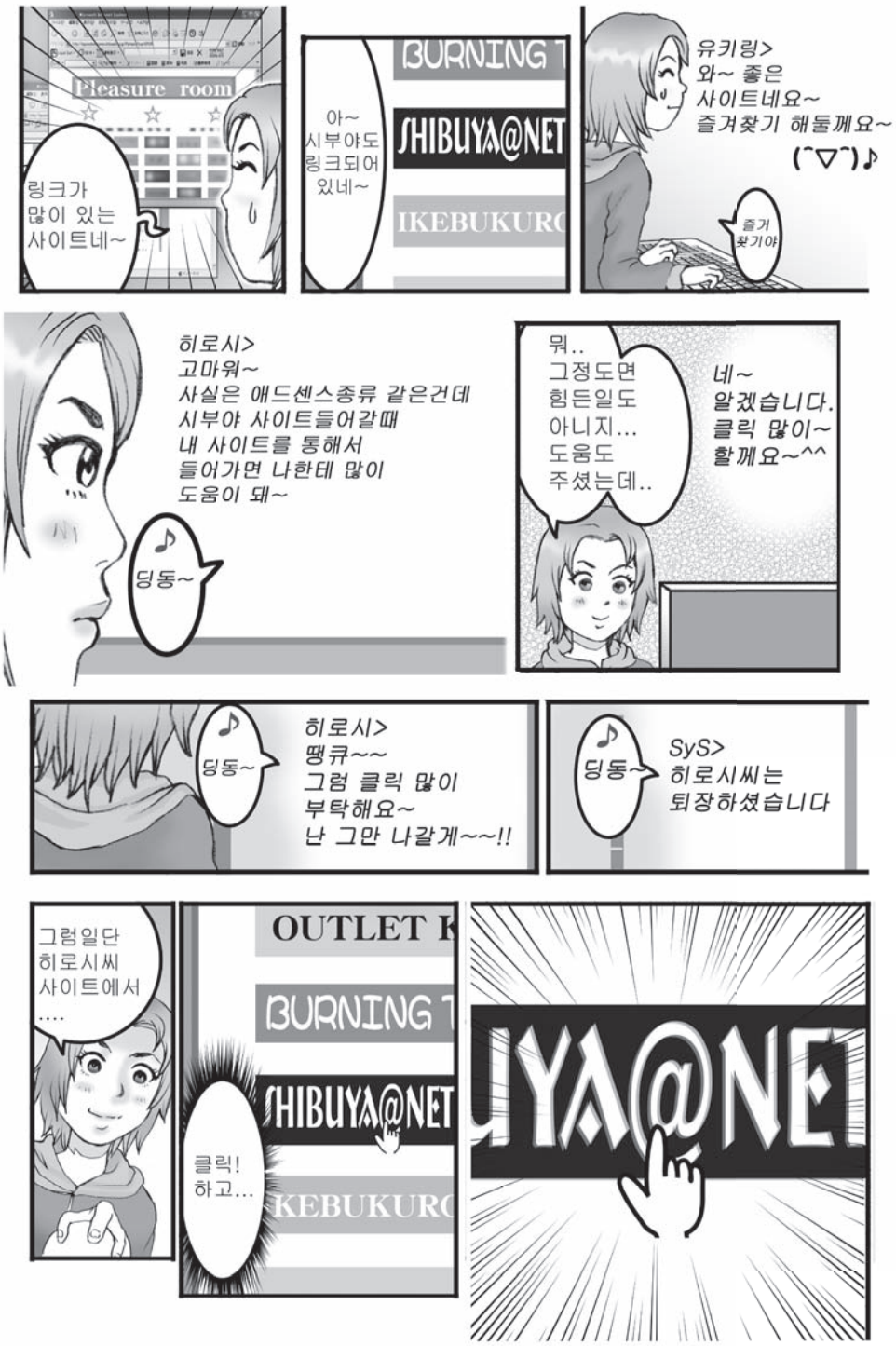
1. 크로스 사이트 스크립팅의 원리와 문제점을 이해한다.

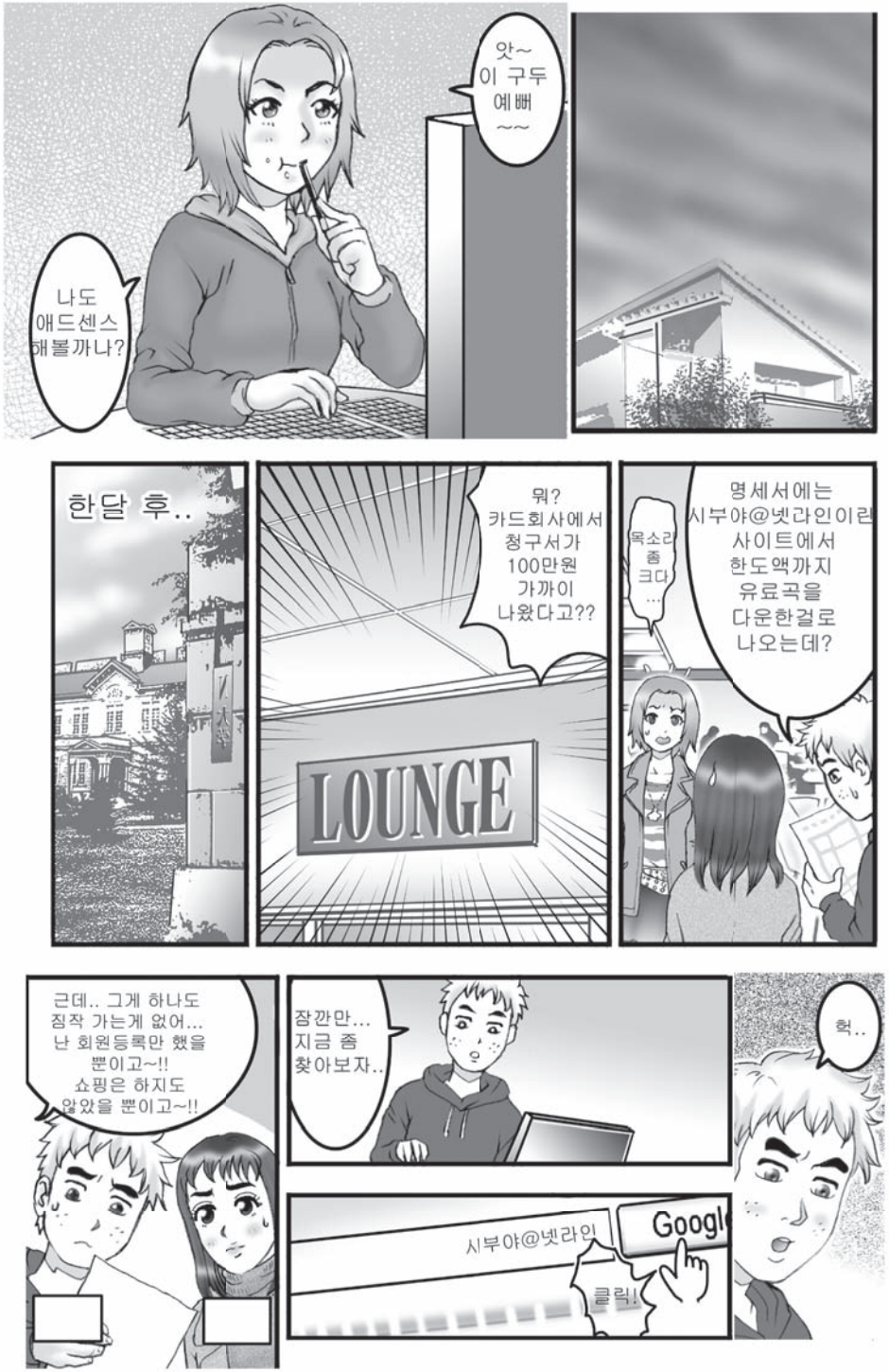
   - 쿠키에 대해 이해한다.
   - 크로스 사이트 스크립팅의 원리를 이해한다.
   - 크로스 사이트 스크립팅의 원리를 이해하여 이 이야기의 다른 어떤 피해를 받을 가능성이 있는지를 인식한다.

2. 크로스 사이트 스크립팅 공격의 피해를 받지 않기 위해, 이용자로 어떤 주의가 필요한지를 이해한다.

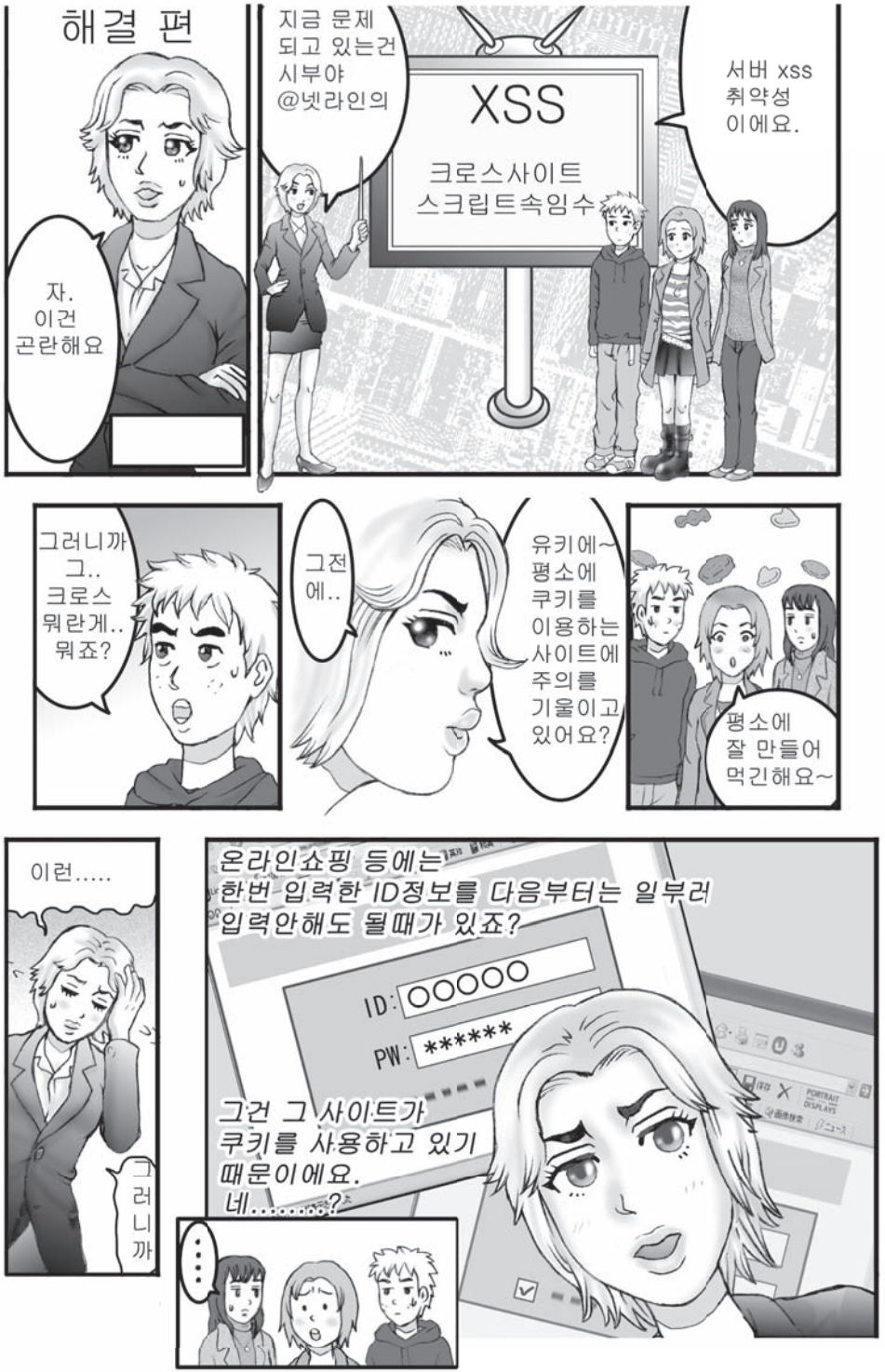
3. 정보 보안과 관련된 다른 문제에 대해서도 조사하여 피해를 당하지 않기 위한 방책을 생각한다.

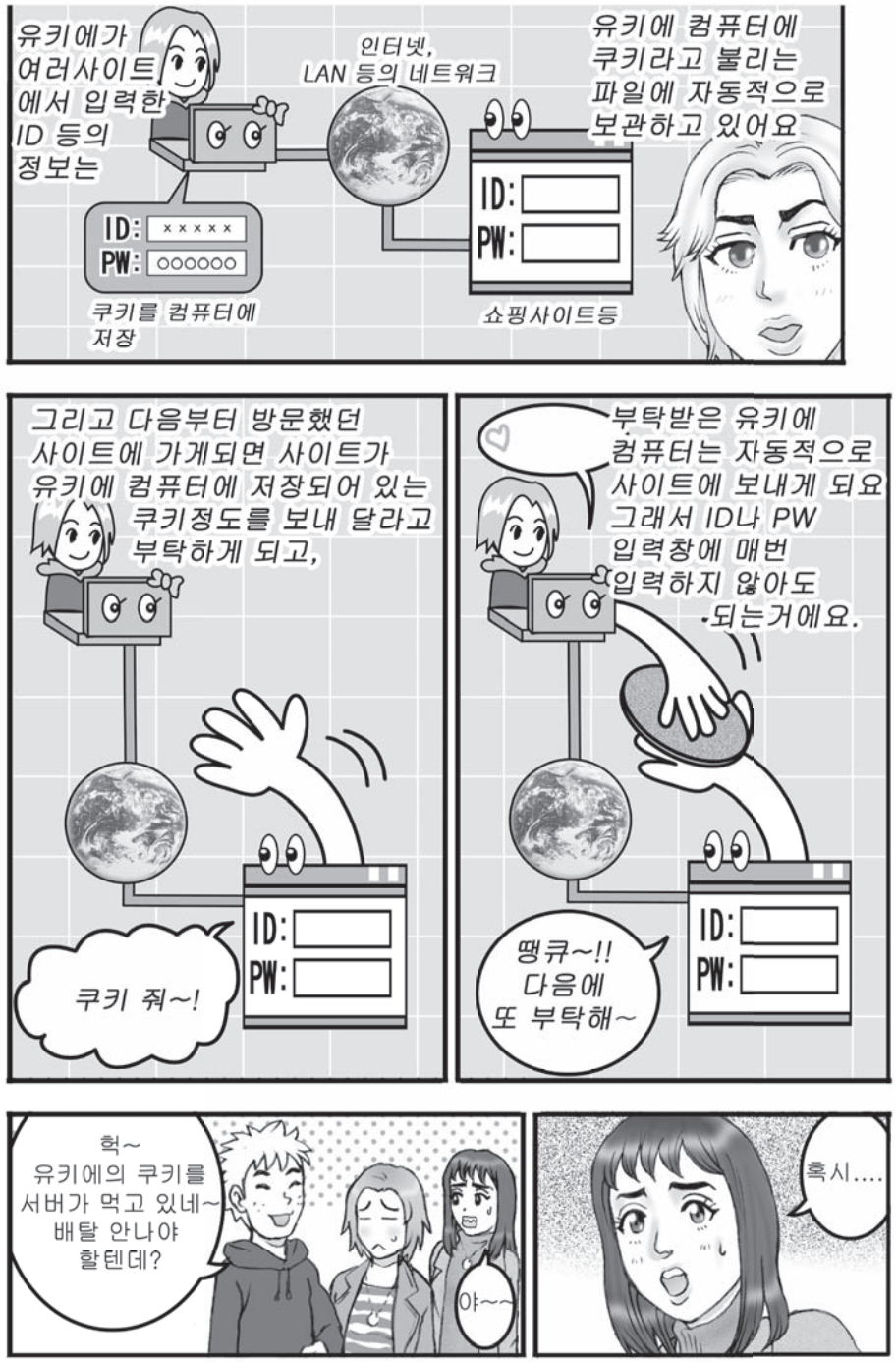

SHIBUYA@NE
즐겨찾기 추가하고~
어머~
지금 회원등록시 모든 고객에게 멋진 선물을~!
바로 회원등록하기
유키링>
지금 회원등록하려구요~
히로시>
그래~!
음악다운도 할 수 있고
포인트 모으면 만화나
DVD도 살 수 있어~!
일단 등록만으로도
좋지 않을까나?^^
유키링>
네~~!!
그럴께요^-^
히로시씨 추천이니까 문제 없겠지
주소 이름 카드번호 ...랑..
됐다~ 다썼다~!
클릭!!
전송
완료!!
히로시씨 아직 있어요?
일단 등록은 했어요~
딩동
히로시>
와~ 수고했어~!
그런데 나도 취미로
사이트 하나 운영하고
있어~
시간있으면 와봐^^
http://www.teach-for
오~ 어떤 사이트 일까나?
클릭!


Pleasure room
링크가 많이 있는 사이트네~
아~ 시부야도 링크되어 있네~
BURNING
SHIBUYA@NET
IKEBUKURO
유키링>
와~ 좋은 사이트네요~
즐겨찾기 해둘께요~
(˘▽˘)♪
즐겨찾기야
히로시>
고마워~
사실은 애드센스종류 같은건데
시부야 사이트들어갈때
내 사이트를 통해서
들어가면 나한테 많이
도움이 돼~
딩동~
뭐..
그정도면
힘든일도
아니지...
도움도
주셨는데..
네~
알겠습니다.
클릭 많이~
할께요~^^
딩동~
히로시>
땡큐~~
그럼 클릭 많이
부탁해요~
난 그만 나갈게~~!!
딩동~
SyS>
히로시씨는
퇴장하셨습니다
그럼일단
히로시씨
사이트에서
....
OUTLET K
BURNING
SHIBUYA@NET
KEBUKURO
클릭!
하고...
YA@NE

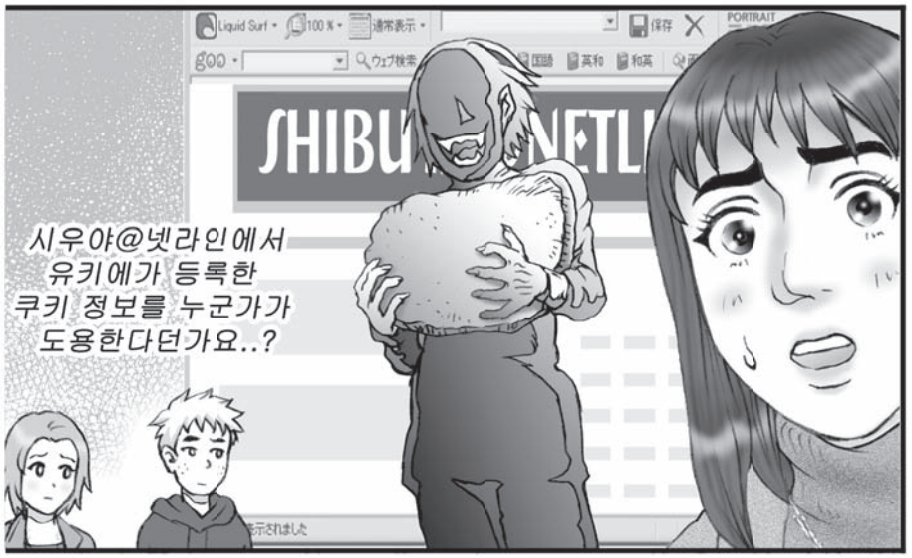

나도 애드센스 해볼까나?
앗~ 이 구두 예뻐~~
한달 후..
LOUNGE
뭐? 카드회사에서 청구서가 100만원 가까이 나왔다고??
목소리 좀 크다...
명세서에는 시부야@넷라인이란 사이트에서 한도액까지 유료곡을 다운한걸로 나오는데?
근데.. 그게 하나도 짐작 가는게 없어... 난 회원등록만 했을 뿐이고~!! 쇼핑은 하지도 않았을 뿐이고~!!
잠깐만... 지금 좀 찾아보자..
시부야@넷라인
Googl
클릭!
헉..


XSS취약성 있는 온라인 넷 쇼핑
아래의 사이트에서 쇼핑할때에는 꼭! 조심하세요!!
아시안e-net : http://....
시부야@넷라인.....
등....
XSS?
음.. 잘은모르겠지만.. 안정성에 문제가 있는 사이트인 것 같아
근데... 왜 이런 사이트에 가입을 해버린거야~!!
그게.. 채팅룸에서 히로시씨가 추천했거든..
저번에 말했던 채팅친구?
그럼, 그 히로시란 사람한테 물어보면 뭔가 알 수 있지 않을까?
응.. 여러가지 가르쳐주기도 하고 너무 친절하고 좋은사람인데..
그게... 요즘 전혀.. 모습이 안 보여서...
채팅방 친구들도 걱정하고 있는데..
뭔가.. 수상한데. 그사람..?
하긴..
아~~ 어떻하면 좋지?
이 돈.... 내가 내야 하는거야??

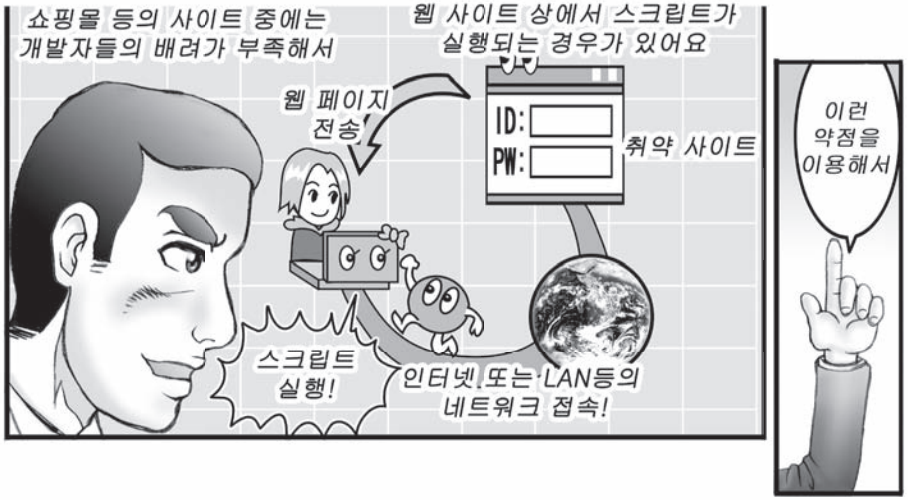

해결 편
자.
이건
곤란해요
지금 문제
되고 있는건
시부야
@넷라인의
XSS
크로스사이트
스크립트속임수
서버 xss
취약성
이에요.
그러니까
그..
크로스
뭐란게..
뭐죠?
그전
에..
유키에~
평소에
쿠키를
이용하는
사이트에
주의를
기울이고
있어요?
평소에
잘 만들어
먹긴해요~
이런.....
그러니
까
온라인쇼핑 등에는
한번 입력한 ID정보를 다음부터는 일부러
입력안해도 될때가 있죠?
ID: OOOOO
PW: ******
그건 그 사이트가
쿠키를 사용하고 있기
때문이에요.
네.....?
....


유키에가
여러사이트
에서 입력한
ID 등의
정보는
인터넷,
LAN 등의 네트워크
유키에 컴퓨터에
쿠키라고 불리는
파일에 자동적으로
보관하고 있어요
ID: xxxxx
PW: OOOOOO
쿠키를 컴퓨터에
저장
ID:
PW:
쇼핑사이트등
그리고 다음부터 방문했던
사이트에 가게되면 사이트가
유키에 컴퓨터에 저장되어 있는
쿠키정도를 보내 달라고
부탁하게 되고,
쿠키 줘~!
부탁받은 유키에
컴퓨터는 자동적으로
사이트에 보내게 되요
그래서 ID나 PW
입력창에 매번
입력하지 않아도
되는거에요.
땡큐~!!
다음에
또 부탁해~
헉~
유키에의 쿠키를
서버가 먹고 있네~
배탈 안나야
할텐데?
야~~
흑시....


안전에 문제가 있는 서버에 ID나 PW를 입력하면..
어딘가 외부에서 그 정보를 훔쳐갈 수도 있는건가요?
예를 들면 …


시우야@넷라인에서 유키에가 등록한 쿠키 정보를 누군가가 도용한다던가요..?


안타깝지만
가능할 수 있어요.
그럼 그건 죠~ 선생님께 물어 볼까요?
조 선생님!
자~ 설명해드리죠!!

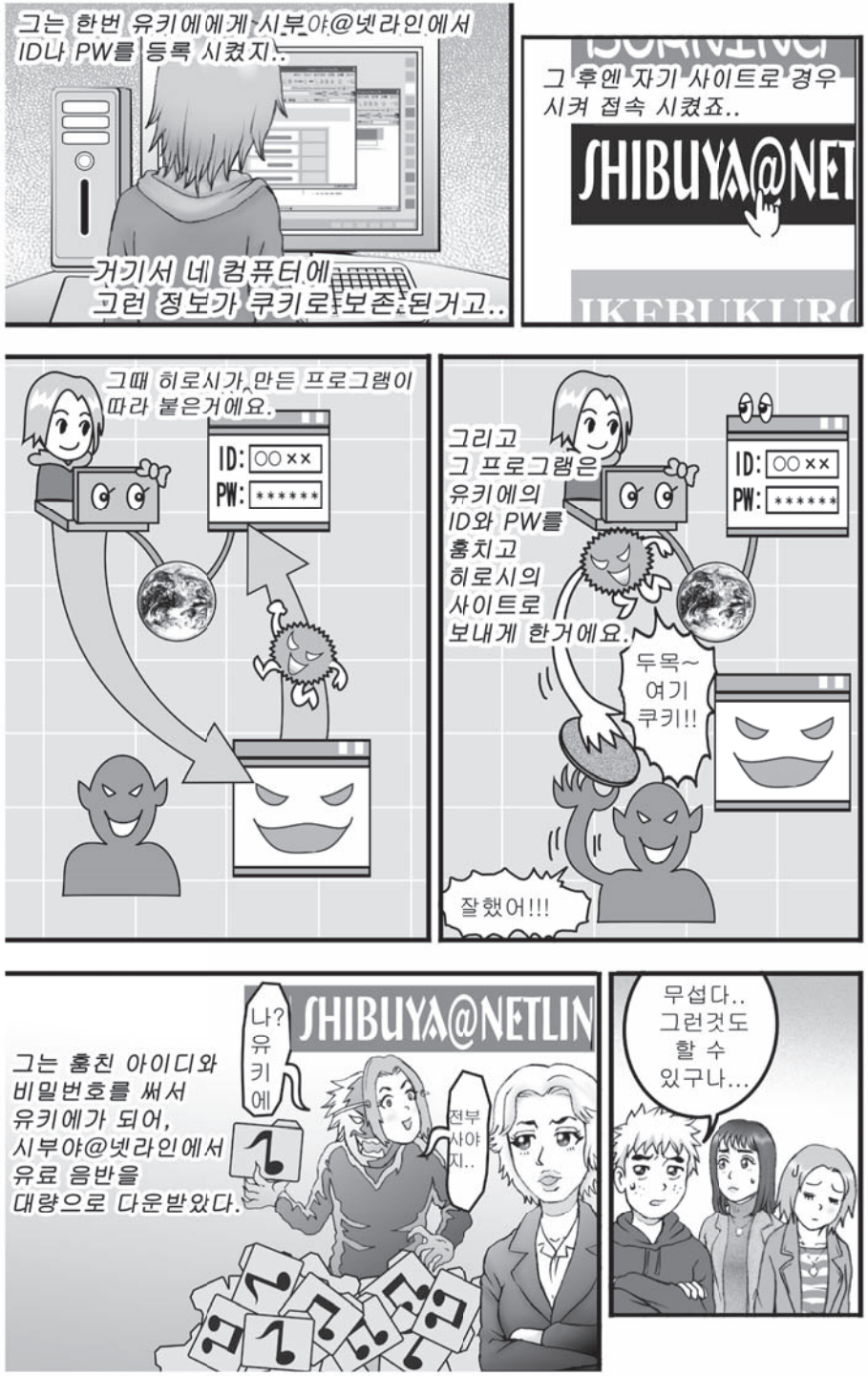

쇼핑몰 등의 사이트 중에는 개발자들의 배려가 부족해서
웹 사이트 상에서 스크립트가 실행되는 경우가 있어요
웹 페이지 전송
ID:
PW:
취약 사이트
스크립트 실행!
인터넷 또는 LAN등의 네트워크 접속!
이런 약점을 이용해서


안 돼!!
사이트에 있는 링크를 클릭한 사람의 쿠키정보를 훔쳐오는
악의성 있는 웹.사이트를 만들 수 있는 거에요.


당사자가 생각하지도 못한 곳에서 정보를 가져간다는 것을 생각하면 일종의 범죄행위라고 볼 수 있죠~!


저기..
결국 제 쿠키를 도용한 것은…


친절하고 착한 착한 친구인 히로시 밖에 없는 거네요….
역시…


그는 한번 유키에에게 시부야@넷라인에서 ID나 PW를 등록 시켰지..
거기서 네 컴퓨터에 그런 정보가 쿠키로 보존 된거고..
그 후엔 자기 사이트로 경우 시켜 접속 시켰죠..
SHIBUYA@NET
그때 히로시가 만든 프로그램이 따라 붙은거에요.
ID: ○○××
PW: ******
그리고 그 프로그램은 유키에의 ID와 PW를 훔치고 히로시의 사이트로 보내게 한거에요.
두목~ 여기 쿠키!!
잘했어!!!
그는 훔친 아이디와 비밀번호를 써서 유키에가 되어, 시부야@넷라인에서 유료 음반을 대량으로 다운받았다.
SHIBUYA@NETLIN
나? 유키에
전부 사야지..
무섭다.. 그런것도 할 수 있구나...


시부야@넷라인은 그런 악의적 프로그램이 실행되는 것을 막는 배려가 되어 있지 않았어요..
그런걸..
크로스사이트 스크립트속임수 의 취약성 이 있다고 하는 겁니다.
XSS
즉, 히로시는 시부야@넷라인의 보안적 맹점을 이용한거죠~
어이쿠~
내 컴퓨터엔 보안 맹점 없는데...
시부야@넷라인도 그렇지만 안전인지 모르는 온라인숍을 이용하는 것은 엄청 위험해요
그렇죠, 특히~

【자료】

용어

어필리에이트

웹 등에 붙여진 기업의 웹 사이트로의 링크를 경유하여 그 기업의 상품의 구입 등이 행해지면, 그 기업에서 링크 건 사람에게 포인트나 보수가 지불된다 라고 하는 구조의 광고 수법의 하나. 인터넷 백서 2011(ISBN9784844330493)에 의하면, 어필리에이트 광고의 시청률은 PC로 약40%, 휴대전화로 약10%, 스마트 폰으로 약20% 정도이다.

보안 홀

보안 취약점 시스템의 보안상의 불량. 홀은 구멍(hole)으로,「안전성의 구멍」이라는 의미. 홀은 큰방(hall)이란 뜻이 아니다. 새롭게 보안 취약점을 찾으면, 바로 바이러스 등의 악의 있는 프로그램이 작성되어 퍼지는 것이 있어 OS 및 웹 브라우저의 업데이트나 바이러스 백신 등의 보안 대책을 꼼꼼히 자주 해 줘야 한다.

쿠키

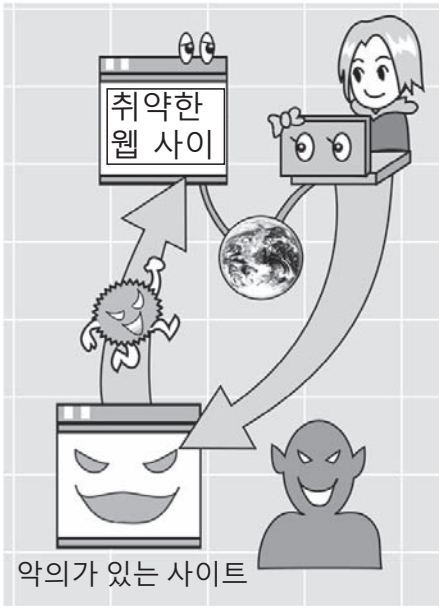
웹 사이트가 열람되었을 때, 웹 브라우저를 통해서 그 웹 사이트의 방문자의 컴퓨터 상에 방문자의 정보나 방문 일시 등을 전용의 작은 파일에 기록해서 보존하는 구조 또는 파일. 이것에 의해, 웹 사이트를 방문했을 때 ID나 신용카드 번호를 매회 입력하지 않아도 되거나, 열람한 페이지에 관계되는 웹 사이트를 소개 주는 등 편리하지만 취약하거나 악의가 있는 웹 사이트에 가게 되면 ID등이 도난 당할 위험성이 있다. 악의가 없을지라도 자신의 기호 등이 알려진다던가 멋대로 판단 되는 경우가 있으므로 주의해야 할 필요가 있다. 필요 없으면 쿠키를 삭제하길 바란다.

크로스 사이트·스크립팅

사이트를 거쳐(크로스하여), 스크립트를 실행하는 공격 수법에 따라 이 이름이 붙여졌다. 자세한 내용은 본 자료를 참조하길 바람. 웹 사이트에 이러한 취약성이 있을 경우 이용자 측 에서 피해를 피하는 것은 어렵다. ID등의 개인정보를 넣는 웹 사이트에는 잘 모르는 웹 사이트의 링크를 경유하지 않고 직접 액세스하도록 만든다. ID등의 개인정보를 넣을 때는 정말로 넣을 필요가 있는 것인가 침착하게 판단하길 바란다.

크로스 사이트·스크립팅의 위력과 피해

본 내용에서는「시부야@넷라인」과 같은 쇼핑 사이트에 크로스 사이트·스크립팅의 취약 성이 있었기 때문에 유키에(由紀恵)씨의 쿠키 정보가 도둑 맞아 피해를 받았습니다. 그러나 크로스 사이트·스크립팅에 의한 피해는 그 외에도 많습니다. 조금 정리해 봅시다.
크로스 사이트·스크립팅에 의해 생길 수 있는 피해에는 다음의 것 같습니다.

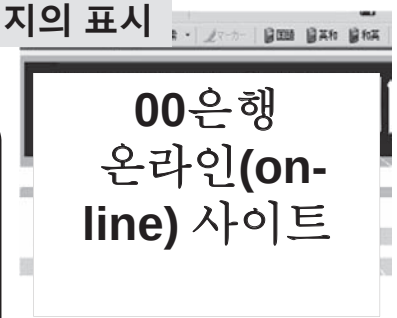


계기는, 악의가 있는 사이트를 열람하고, 악의가 있는 링크 등을 클릭하는 것 (유키에(由紀恵)씨의 예), 또는 그러한 장치의 링크를 포함하는 메일을 받고 그 링크를 클릭하는 것입니다. 그 때, 악의가 있는 사람이 작성한 스크립트가 취약한 웹 사이트로 보내집니다.

쿠키 정보의 취득

쿠키 정보누설

위조페이지의 표시

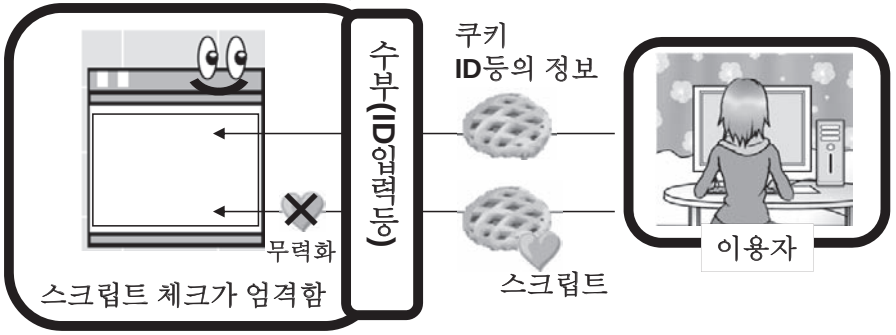


생길 수 있는 피해
·피싱 사기
·쿠키 정보누설 (본인행세, 개인정보의 누설 등. 쿠키와 스크립트에 의함)
・・・・

안심되는 사이트•위험한 사이트에서의 스크립트 처리의 차이

웹 사이트에서는 로그인 화면, 회원등록, 블로그나 게시판 등의 코멘트의 반영 등, 이용자의 입력 내용에 따른 처리가 발생합니다. 악의가 있는 사람이 작성한 스크립트가 웹 사이트에서 어떻게 처리될지 정리해 봅시다.

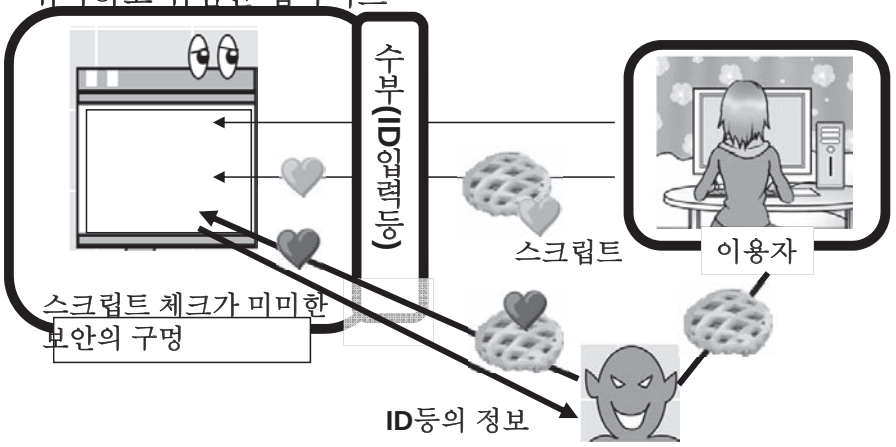
견고하고 안전한 웹사이트



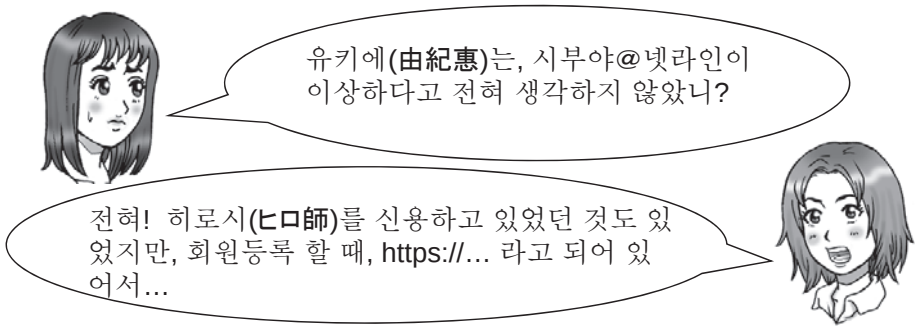
안심되는 온라인(on-line) 사이트에서는, 스크립트의 체크가 엄격하게, 가령 악의 있는 스크립트가 혼입하고 있어도 무력화되어 아무 일도 없습니다.

한편, 취약한 사이트에서는 스크립트의 체크가 미미하여 거기가 보안홀(보안 취약점)이 되어 악의가 있는 스크립트가 실행되어버립니다.

취약하고 위험한 웹사이트



통신의 암호화와 크로스 사이트·스크립팅



https로부터 시작되는 웹 사이트는, 네트워크 상의 통신을 암호화하고 있음을 나타내고 있습니다. 비밀번호 등을 보낼 때 그것이 그대로 네트워크상에 흐르면 도중에 도난 당할 가능성이 있어 위험하므로 암호화해서 통신하는 것입니다. https로부터 시작되는 웹 사이트에서는 브라우저에 열쇠 마크가 붙고 있어 그 열쇠 마크를 클릭하는 것으로 그 웹 사이트의 증명서를 확인할 수 있습니다. 그런 의미에서 유키에(由紀恵)씨가 웹 사이트의 URL을 확인하고 https인 것을 체크한 것은 옳았네요.

그러나, 크로스 사이트·스크립팅의 취약성이 있는 웹 사이트가 비록 https에서 통신을 암호화하고 있어도 악의가 있는 프로그램(스크립트)은 들어가게 됩니다. https에서 통신의 암호화와 크로스사이트 스크립팅의 취약성은 별개의 이야기입니다.

어쨌던 신용카드 번호 등 중요한 정보를 입력할 때는 그것이 정말로 필요인가를 냉정히 생각합시다. 또 입력할 때는 다른 사이트의 링크를 경유할 일 없고 또한 상대편이 신뢰할 수 있는 사이트인 것을 확인한 뒤에 입력해야 합니다. 웹 사이트의 https의 증명서는 그 웹 사이트와의 암호통신의 신뢰성의 증명이며 그 웹 사이트 자체를 신뢰할 수 있다고 하는 증명은 아닙니다. 주의해 주십시오.

크로스 사이트•스크립팅의 취약성

독립 행정법인정보처리추진 기구의「취약성에 관한 신고서 상황 (http://www. ipa. go. jp/security/vuln/report/press. html)」에서는, 3개월 마다 (각 해의 제1사분기 (1Q)로부터 4사분기 (4Q)까지)에 소프트웨어 등의 취약성 관련 정보에 관한 신고 상황이 취합되고 있다.
2004년의 3사분기로부터 공표되고 있는 웹 사이트의 취약성에 관한 신고서는 2011년의 4사분기에 누계6025건이 되고 있으며 그 중에서 크로스 사이트·스크립팅의 신고 비율이 가장 높다. 크로스 사이트·스크립팅의 취약성의 원리는 널리 알려져 있지만 2011년도에는 급증하고 있어 전체의 91%을 차지하고 있다. 브라우저로부터 직접 문자열을 입력할 수 있는 칸에 취약성이 있는 것 이외로 숨김 요소 등 얼핏 보기에는 표시되지 않고 직접 입력할 수 없는 부분에 취약점이 있을 경우가 3분의 1을 차지하고 있는 것을 나타났다. 2011년도 4사분기까지의 상세한 결과는 다음 신고서 상황을 참조.

또한 소프트웨어의 취약성 관련 정보에서는 종류로서 웹 브라우저가 가장 많고 그 다음은 웹 어플리케이션 소프트, 라우터가 있다. 임의의 파일로의 액세스나 스크립트의 실행, 정보의 누설 등의 신고가 많고 또한 스마트폰 관계의 제품에 있어서의 신고가 증가하고 있다.

취약성에 관한 신고 상황
http://www. ipa. go. jp/security/vuln/report/documents/vuln2011q4.pdf

최근 공표된 크로스 사이트•스크립팅의 취약성

취약성 대책정보 포털 사이트 JVN(Japan Vulnerability Notes http://jvn. jp/)에서는, 신고가 있었던 취약성에 관한 정보가 공표되고 있습니다.

최근의 크로스 사이트·스크립팅의 취약성의 보고에 대해 아래에 일부 발췌해서 소개하고자 합니다.

Redmine 에 있어서의 크로스사이트스크립팅의 취약성
（2012/03/14 JJVNVU#428075）

Redmine 은 프로젝트 관리 소프트웨어입니다. Redmine 에는 크로스사이트스크립팅의 취약성이 존재합니다. (생각되는 영향: 사용자가 웹 브라우저상에서 임의의 스크립트를 실행될 가능성이 있습니다.)

SquirrelMail 용 플러그인 Autocomplete에 있어서의 크로스사이트스크립팅의 취약성 (2012/03/09 JVN#56653852)

Autocomplete 은, SquirrelMail 용의 플러그인입니다. Autocomplete 에는 크로스사이트스크립팅의 취약성이 존재합니다. (생각되는 영향은 위와 같다.)

Movable Type 에 있어서의 크로스사이트스크립팅의 취약성 (2012/02/23 JVN#49836527)

mt-wizard. cgi 및 Movable Type 에 동봉되어 있는 템플릿에는 크로스사이트스크립팅의 취약성이 존재합니다. (생각되는 영향은 위와 같음)

EProject Open 에 있어서의 크로스사이트스크립팅의 취약성 (2012/02/06 JVNVU#732115)

Project Open 에는, 입력 미터의 처리에 문제가 있어 크로스사이트스크립팅의 취약성이 존재합니다. (생각되는 영향은 위와 같음)

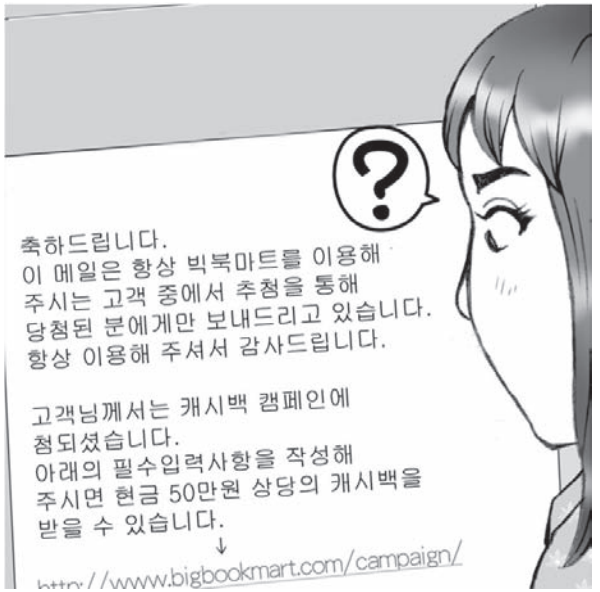
Oracle WebLogic Server 에 있어서의 크로스사이트스크립팅의 취약성（2012/01/20 JVN#54779201）

Oracle WebLogic Server 의 관리 콘솔에는 크로스사이트스크립팅의 취약성이 존재합니다. (생각되는 영향: 해당제품의 관리 콘솔에 로그인하고 있는 사용자의 웹브라우저 상에서, 임의의 스크립트를 실행될 가능성이 있습니다.)

WordPress 일본어판에 있어서의 크로스 사이트•스크립팅의 취약성
（2011/12/26 JVN#44439553）

WordPress. Org 이 제공하는 WordPress 은 웹로그시스템입니다.
WordPress 일본어판에는, 크로스사이트스크립팅의 취약성이 존재합니다.
(생각되는 영향: 사용자의 웹 브라우저상에 임의의 스크립트를 실행될 가능성이 있습니다.)

피싱



【 목표와 포인트】

1) 피싱에 의한 피해와 가해 이해.

   ○ 스푸핑에 의한 피해와 가해의 예제에 대해 생각한다.

2) 피싱의 구체적인 수법을 이해한다.

3) 피싱에 대한 대책에 대하여 생각하고 다음 사항에 주의한다 .

   ○ 메일 발신 주소가 정확하다고는 할 수 없는 것을 이해한다.

   ○ Web에서 ID · 비밀 번호를 보낼 때 그 Web 페이지가 SSL 지원 (https://로 시작하는 URL)임을 확인한다.

   ○ 봇(bot) 같은 바이러스에 감염되지 않도록 바이러스 방지한다.


모야~
잠깐
이 메일
좀 봐봐!
야~
깜짝
놀랬잖아~
축하드립니다.
이 메일은 항상 빅북마트를 이용해
주시는 고객 중에서 추첨을 통해
당첨된 분에게만 보내드리고 있습니다.
항상 이용해 주셔서 감사드립니다.
고객님께서는 캐시백 캠페인에
첨되셨습니다.
아래의 필수입력사항을 작성해
주시면 현금 50만원 상당의 캐시백을
받을 수 있습니다.

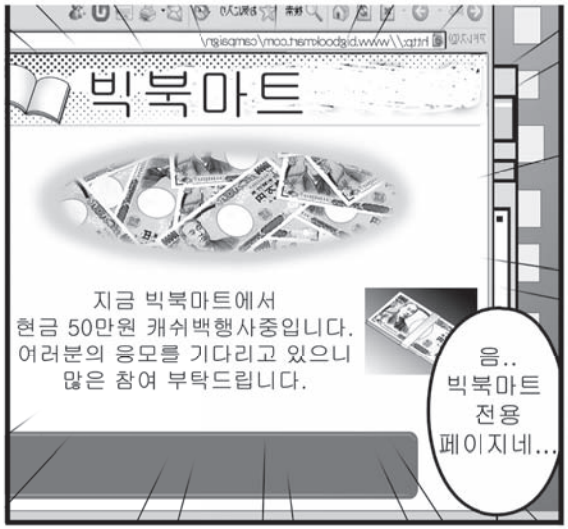

현금 50만원을
준다고!?
굉장한걸?
빅북마트라면
나도 CD를
산적이 있어~!


우와~
굉장한데
평소 행동이
좋아서
그런건가?
좋..겠..다..


50만원
들어으면
초코파르페
사줘~~~
OK!


앗싸!
좋은건
빨리!!
http://www.bigbookmart.com/car

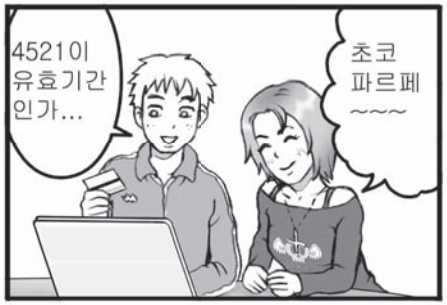

http://www.bigbookm
클릭!!


빅북마트
지금 빅북마트에서
현금 50만원 캐쉬백행사중입니다.
여러분의 응모를 기다리고 있으니
많은 참여 부탁드립니다.
음..
빅북마트
전용
페이지네...


하긴...
빅북마트가
확실하긴
하네..


빅북마트
앗싸~!
이거 다 입력하고
전송만하면,
50만원을 준데~
앗싸~~~~

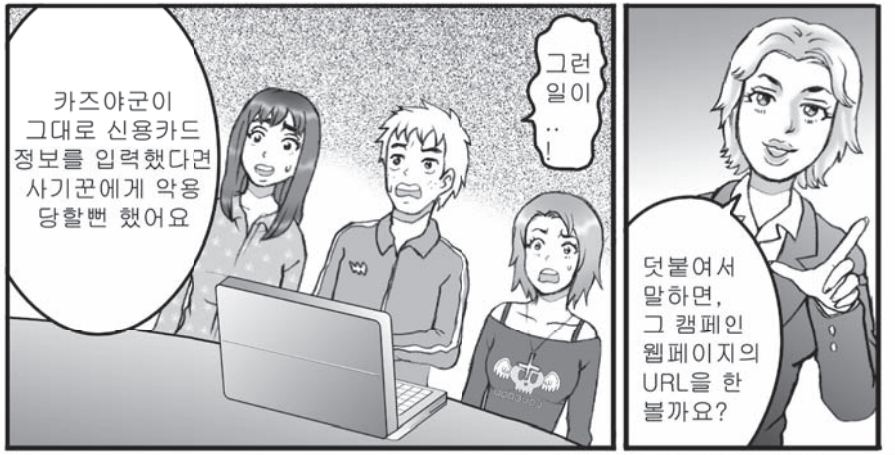

그럼..
카드
번호가...


4521이
유효기간
인가...
초코
파르페
~~~


근데..
잠까만
카즈야..
??
~~~


뭐야~
마사미도
초코파르페
사줄께~~~
안심해!!
그게
아니라...
카즈야..
온라인으로
물건 구입할때
항상
원클릭으로
구입하지
않았어?
응 맞아...
요즘 다른
사이트들도
일일이 매번
입력하는
경우는 없지...
그러면..
왜 일부러
여기서 또
개인정보를
입력시키지?
음..
그러게..
당첨이라
다른거아냐?
난 뽑힌
사람이니까!!
이럴떤..
가르쳐줘
루시~~
이 캠페인
수상하지
않아요??


해 설 편
피.....싱.....???
카즈야군
이번엔
마사미덕에
무사했네요~
이런
사칭메일과
같은 피생엔
주의가
필요해요
출~ 발~!!
그럼,
조선생님의
피싱강좌~
Phishing
타인을 사칭한 메이이나
위장한 웹페이지로
인한 온라인 사기를
피싱이라고 합니다.
낚시를 뜻하는 fishing과
위장수법의 정교화를
위미하는 sophisticated가
합쳐져서 fhishing이
되었다는 설도 있어요.
인터넷은
얼굴을 확인
할 수 없으니
피싱과같은
사기를 하기
더 쉬운
환경이라고
할 수도 있어요
만약에..

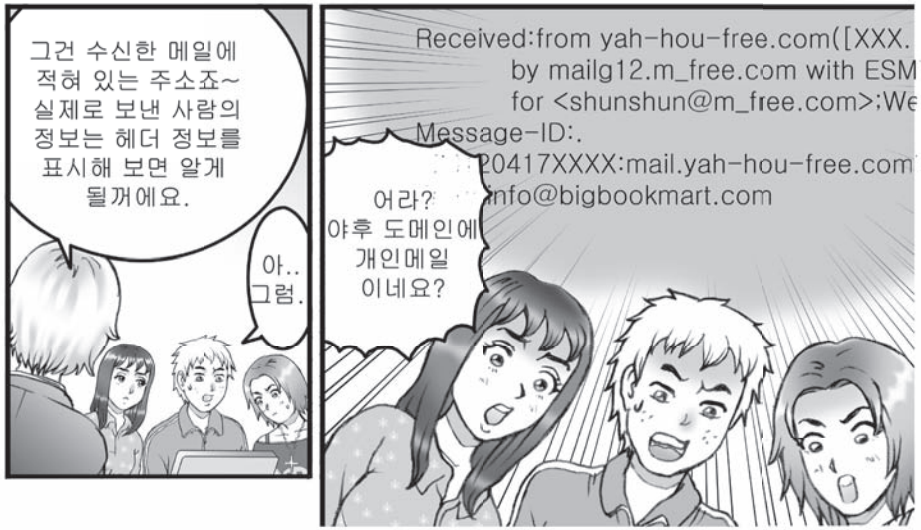

카즈야군이 그대로 신용카드 정보를 입력했다면 사기꾼에게 악용 당할뻔 했어요
그런 일이..!
덧붙여서 말하면, 그 캠페인 웹페이지의 URL을 한 볼까요?


http://www.bigbookmart.com/ca
별로 수상한건 없은것 같은데요?
그럼 다음에 화면에서 오른쪽 마우스를 클릭하고 페이지 속성에서 URL을 확인해봐요


음...
아! 잘보면 www뒤에 점이 없어요!
유형 : .....
연결 : .....
주소(URL) : http://wwwbigbookmart.com/ca


그래, 이상하지? URL을 속여서 표시하거나 디자인을 똑같이 만들어도
원래 기업의 진짜 도메인을 사용하기는 어려워
그래서 진짜 비슷하게 만든 도메인을 쓰고 속이려고 하는 거군요...


그럼, 메일 발신자의 주소는 어떻게 되어 있을까?
음.. 그건..
어라? 발신자 주소는 확실히 빅북이라고 되어 있는데요?
발신자 : info@bigbookmart.com
.....


그건 수신한 메일에 적혀 있는 주소죠~ 실제로 보낸 사람의 정보는 헤더 정보를 표시해 보면 알게 될꺼에요.
아.. 그럼.
Received:from yah-hou-free.com([XXX.
by mailg12.m_free.com with ESM
for <shunshun@m_free.com>;We
Message-ID:.
20417XXXX:mail.yah-hou-free.com
nfo@bigbookmart.com
어라? 야후 도메인에 개인메일 이네요?


알겠지?
수상한 메일이 오면 헤더정보도 꼭 확인해 봐야해요~
피싱수법도 나날이 진화하고 있어서
개인정보를 입력해야할때 이상하다 싶으면 속성을 살펴보고 꼭 주의해야 해요~!!
네!
그것도 그렇지만... 카드정보와 같이 개인정보를 입력하는 등의 소중한 개인정보를 입력하는 페이지에선
송신중에 그 정보를 제 3자에게 보이지 않도록 하기 위해 정보를 암호화 하는 경우가 대부분입니다
그런 암호화 되어있는 페이지는 그림과 같이 브라우저에 열쇠마크가 표시 되어 있으니까 꼭 확인해 주세요!


그밖에도 암호화 되어있는 페이지를 구별하는 방법은 보통 http로 시작하는 URL이 https가 된다는 것입니다
https://www.koreaunive.....
이런경우에는 안전성에 문제가 있다는 경고가 표시 될때도 있습니다.
그런 경우 믿을 수 있는지 확인한 후 접속하고, 불확실하면 접속하지 않는게 좋습니다.
카즈야~ 다행이네요?
네...하하.. 감사합니다
?
근데.. 카즈야
내 덕분에 피싱 사기 당하지 않았으니까 초코 파르페는 잘 먹을께~~~
근데 사기 당할거 생각하면 초코 파르페 사는건 아무일도 아니지 뭐~~
헉. 이것도 큰일인걸...
하하하
친구도 진짜지 가짜지 잘 구별 해야해요

용어

【자료】

피싱

회원대상의 사이트나 금융 기관 등의 사이트로 위장하여 이용자에게 사용자ID와 비밀번호, 암호번호, 신용카드 번호 등을 입력시켜 그것을 훔치는 사기이다. 수법으로는 전자 메일로 가짜 메일 주소를 사용하거나 가짜의 웹 사이트를 그럴 듯하게 나타내는 일 등이 있다. 전자 메일의 송신처를 속이는 것은 어렵지는 않으므로, 정보를 입력하기 전에 그 정보가 정말인가 입력의 필요가 있는 것일지 등을 확인을 하는 것이 중요하다.

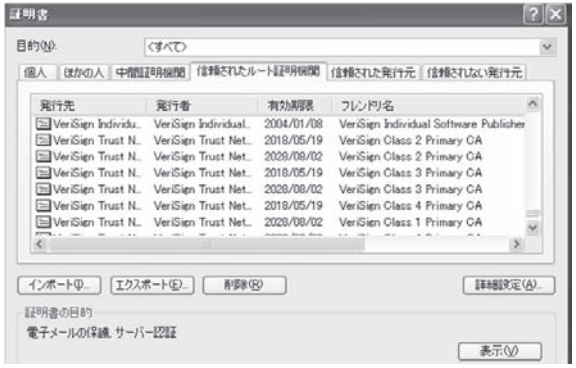
증명서(공개암호증명서)

통신을 암호화하는 웹 사이트(URL이, https://로부터 시작되는 것)에는 화면에 열쇠 마크가 표시되고 있다. 그 열쇠 마크를 클릭 혹은 더블 클릭하는 것으로 증명서를 표시할 수 있다. 증명서로부터는 업데이트의 유무, 증명서의 유효기한, 올바른 URL 등을 볼 수 있다. 각자 한번은 확인해 두면 좋다.

아래의 그림과 같이, 각PC에는「신뢰받은 증명 기관」이라는 기본적인 증명서가 인스톨되어 있다. 이것에 의해 증명서를 신뢰할 수 있는 것인가 아닌가의 판단을 간편하게 실시할 수 있도록 하고 있다.

봇(BOT)

컴퓨터 바이러스의 일종이며 감염시킨 컴퓨터를 네트워크 상에서 조종하는 것을 목적으로 작성된 프로그램. 감염한 컴퓨터가 가짜의 웹 사이트가 되어 알지 못하는 사이에 피싱 사기를 도와주고 있는 경우도 있기에 주의가 필요하다.



피싱의 구체적인 수법 예시

피싱 사기는 우선 정규 기업을 위장한 메일이 보내지는 경우가 많다.

①회원대상의 사이트나 금융기관 등의 사이트로 위장하고 이용자에게 메일을 보낸다. 그 메일에는 계약의 변경, 불량의 갱신, 캠페인이나 서비스의 제공 등의 내용이 쓰여져 있다. 동시에 웹 사이트에의 링크나 첨부 파일 등이 포함되어 있다. 첨부 파일을 사용하는 수법에서는 해당기업의 공식 어플리케이션(application)으로 위장하고 첨부된 실행 파일을실행시키도록 만든다.

예를 들면 은행의 경우에는 인터넷 은행용 어플리케이션(application) 소프트로 가장하거나 뉴스 사이트의 경우에는 기사 리더 어플리케이션(application)으로 가장하거나 한다. 어느 쪽의 경우에도 믿도록 만들기 위해 정규 기업의 로고나 진짜 웹 사이트 혹은 진짜와 아주 닮은 가짜 웹 사이트를 포함하여 표시시키는 등 행해지는 경우가 있다.

この度、あなたがキャッシュバックキャンペーンに当選いたしました。こちらの専用のウェブサイトから必要事項をご記入頂ければ、現金５万円のキャッシュバックが受けられます。
↓
http://www.bigbookmart.com/campaign/

웹 사이트에의 링크 예

②A【웹 사이트로의 링크인 경우】

링크를 클릭하면 ID나 비밀번호, 신용카드 번호와 같은 정보 입력을 요구하는 화면이 표시된다. 속아서 정보를 입력하면 범인에게 정보가 송신된다.

②B【첨부 파일의 경우】

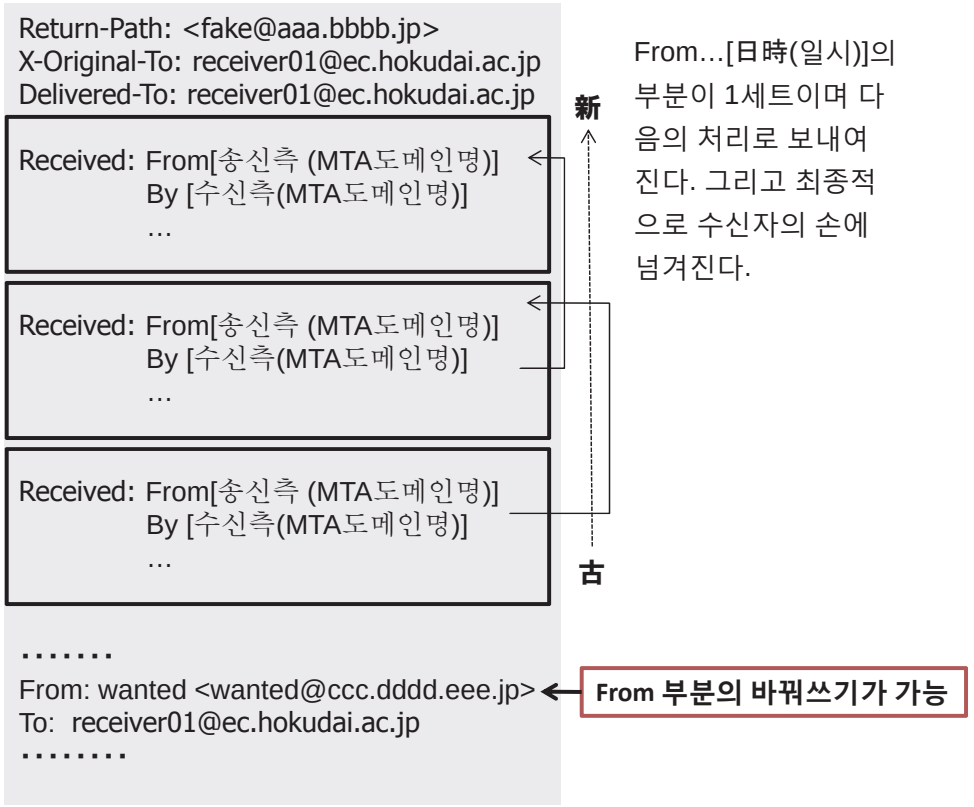
첨부 파일을 실행하면 숨어있는 트로이 목마와 같은 바이러스나 키로거 등이 실행되어 범인에게 수시로 정보를 송부한다.

최근에서는 피싱 사기의 수법도 교묘해지고 있다. 제시한 예시와 상관없이 정보를 입력하거나 신규 소프트웨어를 인스톨 할 때는 정말로 신뢰할 수 있는 것인가를 검토하고 알 수 없을 경우에는 실행하지 않는 등의 주의가 필요하다.

메일 헤더 정보

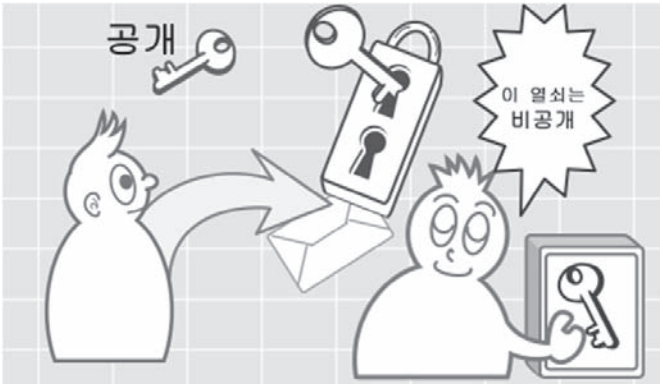
피싱 사기를 만나지 않기 위해서는 평소부터 ID나 비밀번호, 암호번호, 신용카드 번호와 같은 것을 안이하게 입력하지 않고 또한, 부주의하게 안전 한지 모르는 소프트웨어를 인스톨하지 않는 태도가 필요하다. 본고에서는 기타 많은 피싱 사기로 사용되는 메일에 대해서 보충한다. 우선 메일의 표면상 가짜 송신자로 둔갑하는 것은 용이하다. 보다 상세한 정보가 쓰여져 있는 헤더 정보의 개략은 모식적인 예(발췌)로 이하와 같다.

메일의 헤더 정보에서는 아래에서 순서대로 처리되고 있다. 보내져 온 메일의 통신 경로에 의심스러운 것이 없는지를 확인한다.



헤더 정보의 모식 예시

공개 열쇠 암호는 숨은 공로자



【 목표와 포인트】

1) 대칭 암호와 공개 키 암호화의 차이점과 특징에 대해 이해한다.
   - 공개키 암호화는 어떤 암호 시스템인지 이해한다.
   - 공개키와 비밀키가 어떤 장면에서 사용하는 방법을 이해한다.

2) 암호 통신 및 전자 서명의 관계를 이해한다.
   - 인증 기관 (CA : Certificate Authority)의 역할을 이해한다.
   - 공개 키 인증서가 무엇인지 이해한다.
   - SSL (https://) 통신의 처리를 구체적으로 이미지 할 수 있게 된다.
   - 구체적으로 인증 기관의 전자 서명을 확인하고 공개 키 인증서가 수정되지 않았거나 등을 확인된다.

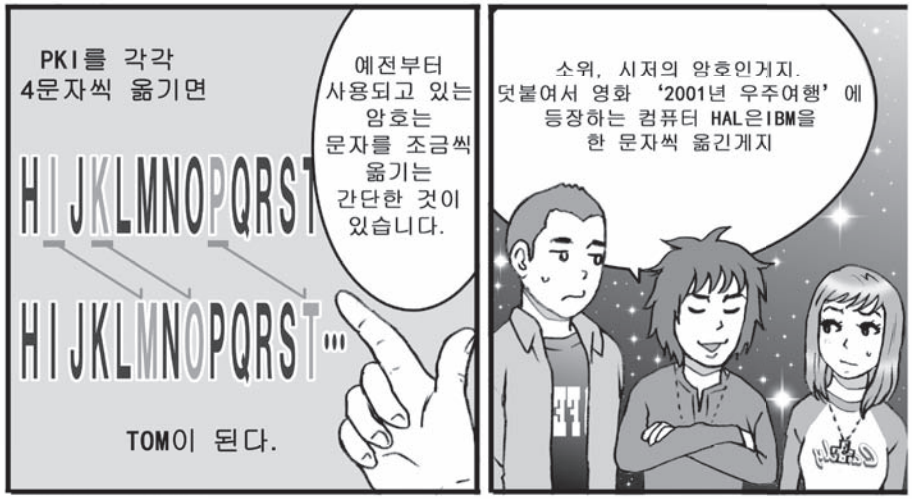
3) RSA 암호의 구조와 안전성에 대해 이해한다.


그건 분명 암호를 사용하는 거라고. 공개키라던가, EMI라고 하는…
예를 들어, 패스워드 같은거 보낼 때, 열쇠마크가 표시되지?
뭐야 그게?? 무슨 소리인지 잘 모르겠는데

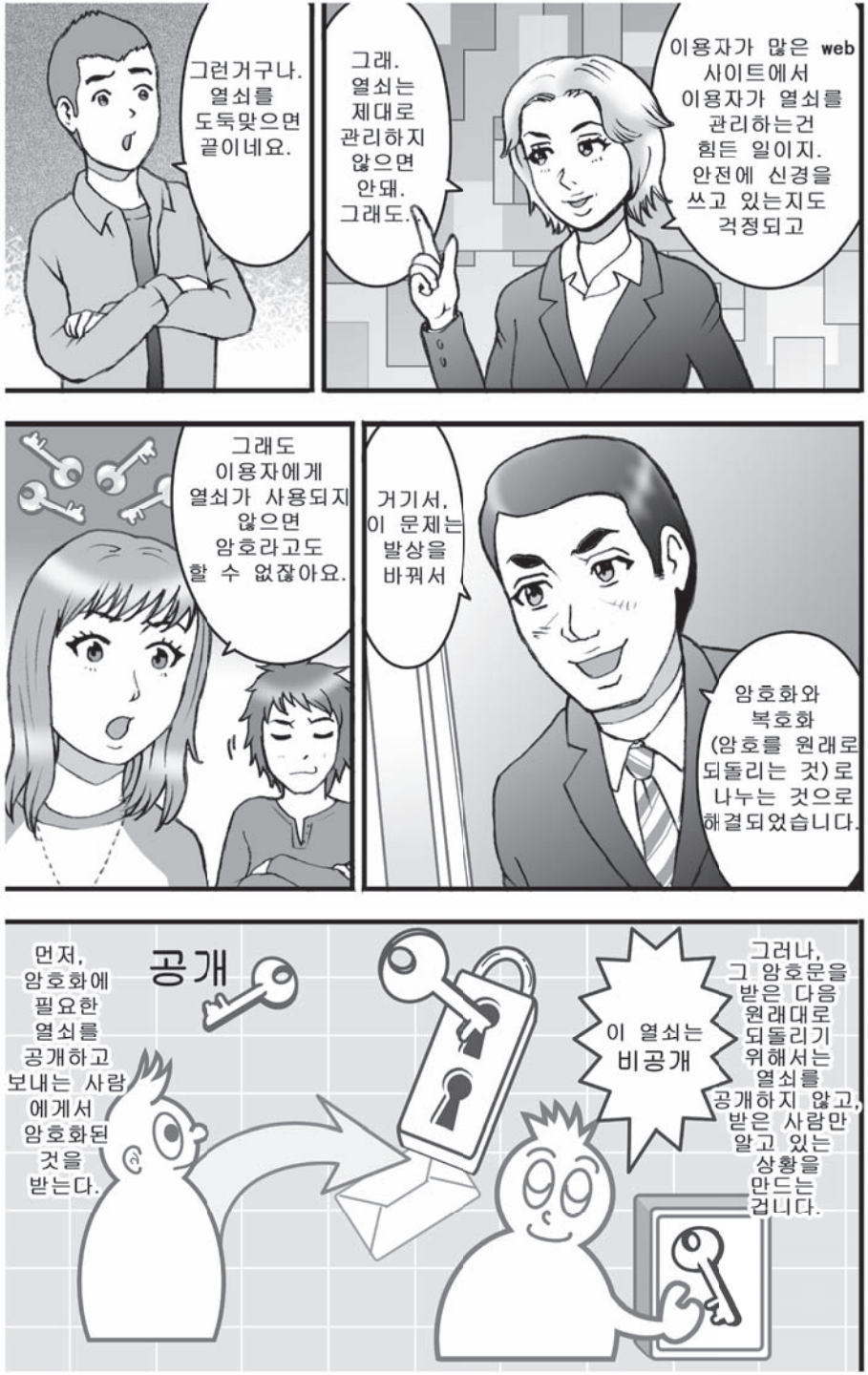

뭔가요? 그 공개키라는게?
그보다 EMI는 레코드 회사 아닌가?
뭐, 어쨌든 국가에서도 암호를 사용해서 전자정부 같은 서비스를 시작할 정도로 암호는 중요한 거야
으… 수업 좀 성실하게 들어뒀어야 했는데…


근데, 공개키는 뭔가요? 자세히 좀 알려주세요.
열쇠를 공개하는 거야? 위험하지 않아?
으악… 깊게 알려고 하고 있다! 루시! 헬프~!!


아오야마군, 작년 착실하게 학점 받았죠? 제대로 하지 않으면…
EMI가 아니고 PKI !!
죄송합니다..
원래 암호란, 특정인에게만 전달되기 위해서 그 이외의 사람이 알 수 없는 방법으로 나타내는 것입니다.

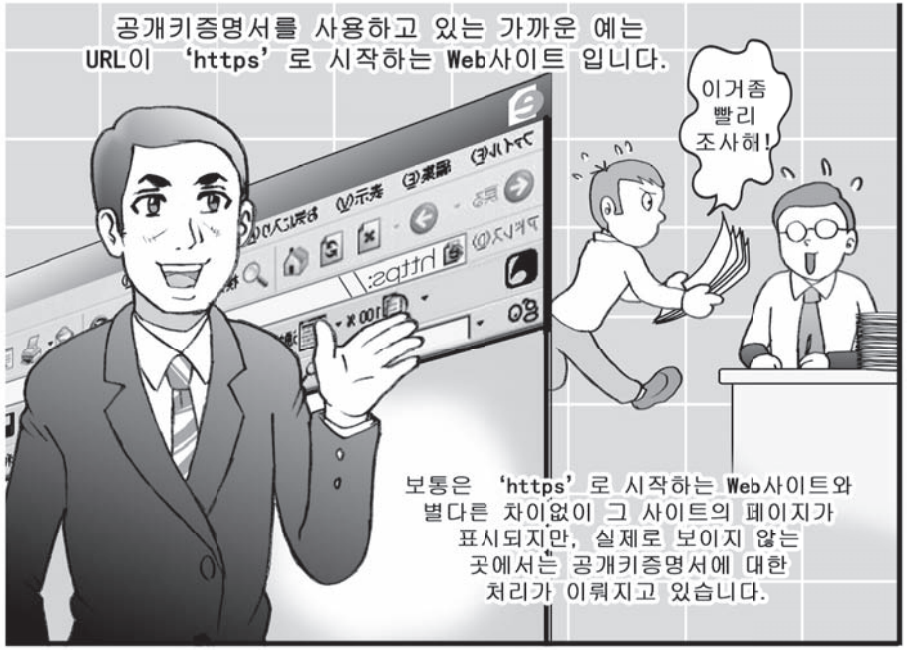

PKI를 각각 4문자씩 옮기면
HIJKLMNOPQRST
HIJKLMNOPQRST‴
TOM이 된다.
예전부터 사용되고 있는 암호는 문자를 조금씩 옮기는 간단한 것이 있습니다.
소위, 시저의 암호인거지. 덧붙여서 영화 '2001년 우주여행'에 등장하는 컴퓨터 HAL은IBM을 한 문자씩 옮긴게지


그랬었지, 더욱 강력한 암호가 여러가지 생각되어 왔지만..
만든방법, 푸는방법을 공유
열쇠로 비밀유지
거기에는 암호를 보내는 사람과 받는 사람이 만드는 방법, 푸는 방법을 공유해서 암호의 열쇠가 되는 것을 비밀유지하는 것이 필요했습니다.


그런거구나. 열쇠를 도둑맞으면 끝이네요.
그래. 열쇠는 제대로 관리하지 않으면 안돼. 그래도..
이용자가 많은 web 사이트에서 이용자가 열쇠를 관리하는건 힘든 일이지. 안전에 신경을 쓰고 있는지도 걱정되고
그래도 이용자에게 열쇠가 사용되지 않으면 암호라고도 할 수 없잖아요.
거기서, 이 문제는 발상을 바꿔서
암호화와 복호화 (암호를 원래로 되돌리는 것)로 나누는 것으로 해결되었습니다.
공개
먼저, 암호화에 필요한 열쇠를 공개하고 보내는 사람에게서 암호화된 것을 받는다.
이 열쇠는 비공개
그러나, 그 암호문을 받은 다음 원래대로 되돌리기 위해서는 열쇠를 공개하지 않고, 받은 사람만 알고 있는 상황을 만드는 겁니다.


그러면, 이용자에게 열쇠를 준비해서 나누어 주는것 하지 않아도 완료될 겁니다.
공개키
비밀키
이러한 암호를 공개키암호 라고 부릅니다.
흠. 흠.
그래도 열쇠가 공개되는건 편리하지만, 가짜 공개키가 간단히 위조되는거 아닌가요?
A가 아닌 사람이 A인척 한다거나…
좋은 질문이에요! 그것을 위해서…
인증국
A의 공개키라는 것을 증명해주는 겁니다.
'인증국' 이라 불리는 국제적인 기관이 있는 겁니다.


인증국에 인증되면,
인증국
< 공개키증명서 >
'공개키 OO은 A의 공개키입니다.' 라는 메세지와 인증국의 전자서명이 붙여집니다. 이것을 공개키인증서 라고 부릅니다. 전자서명에 대해서는 나중에 자세히 설명하겠습니다.
진짜 A의 열쇠인가..
인정!!
어디 보자~


공개키증명서를 사용하고 있는 가까운 예는
URL이 'https'로 시작하는 Web사이트 입니다.
이거좀 빨리 조사해!
보통은 'https'로 시작하는 Web사이트와 별다른 차이없이 그 사이트의 페이지가 표시되지만, 실제로 보이지 않는 곳에서는 공개키증명서에 대한 처리가 이뤄지고 있습니다.


'https' 로 시작하는 Web사이트에 접속하면
https
여기 두개
공개키 증명서
Web 사이트
처음에 그 사이트로부터 공개키 증명서와 공개키가 보내져 옵니다.
그렇다고해도, 공개키와 상대의 Web사이트로부터 자동적으로 보내집니다.


웹브라우저가 처리를 해주지만 사용자는 의식할 필요가 없습니다.
인증국의 공개키는 이전에 브라우저에 설치되어 있기 때문이지.
그렇군요.


웹브라우저는 먼저 공개키 증명서의 인증국이 신뢰할 수 있는 기관인지를 확인합니다.
으흐흐흐
인증국
수상해!
그 다음, 전자서명을 조사하여 공개키가 고쳐진 곳이 있는지, 공개키증명서가 유효한지, 그리고 웹사이트의 URL이 올바른지 등을 확인한다.
흠...

문제가 없을때는 그 웹사이트의 페이지를 보여줍니다만…

만약 문제가 있으면

(IE 7)

이러한 표시가 나옵니다.

그럼, 그러한 경고가 나오지 않으면 안심할 수 있는거에요?

NO!!

Web 브라우저에서 그러한 경고가 나오지 않도록 하는 방법도 있어.

그러니깐, 인터넷카페 (PC방) 같은 곳에서 경고문이 나오지 않는다고 해서 안심하면 안됩니다.

위험하다고 생각될때는 공개키증명서의 내용을 확인하세요.

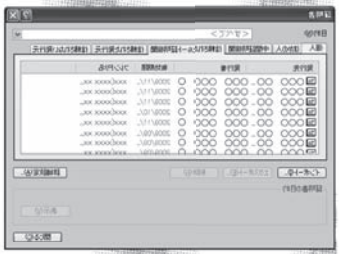
확인하다니 어떻게 하죠?

'https' 로 시작하는 web 사이트의 web 페이지에는 '키마크' 라는 것이 표시됩니다.

키마크

보통, 윈도우 우하단이나 툴바등에 표시됩니다.

그 키마크를 클릭하거나 더블클릭하면, 증명서 발행기관이나 유효기관 등 공개키증명서에 대한 정보가 표시됩니다.



의심스러울때는, 'https' 라고 해도 신용하면 안됩니다.

네!

그럼, 다음은 아까 죠 선생님이 말씀하셨던 '전자서명' 에 대해 아오야마군이 설명할 수 있겠어요?

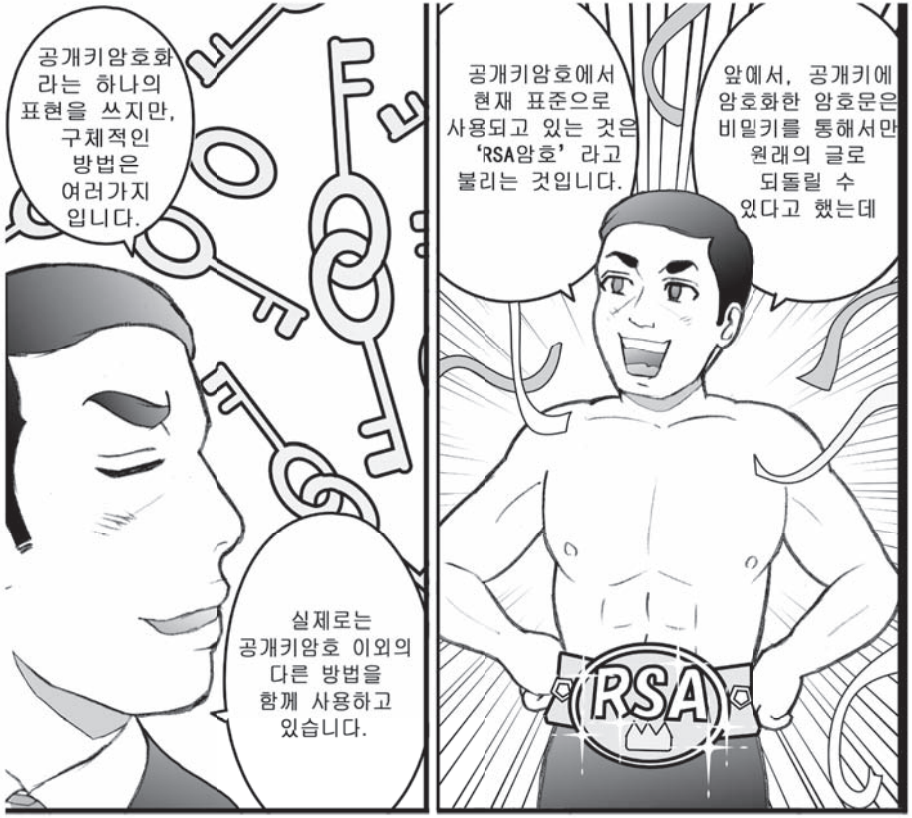
두근

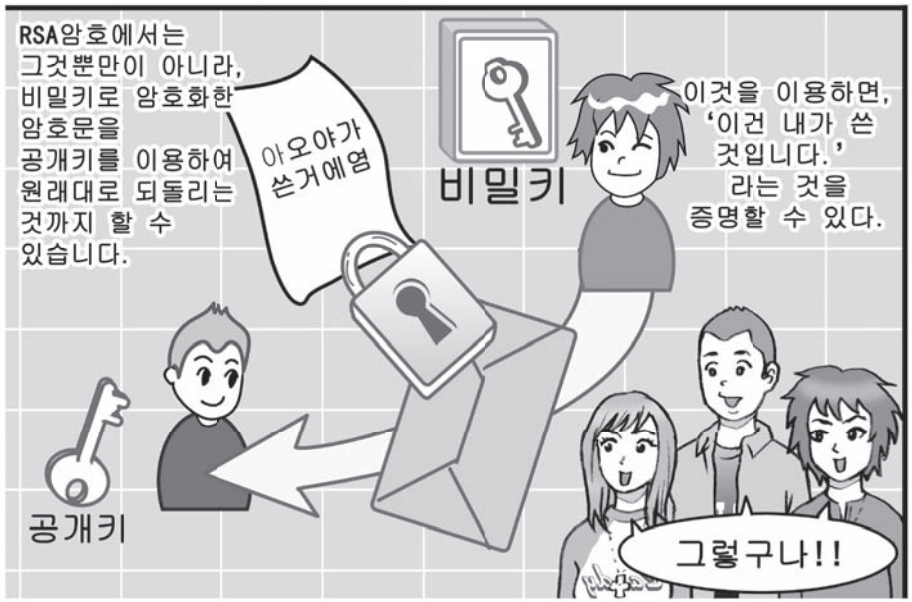
옛?

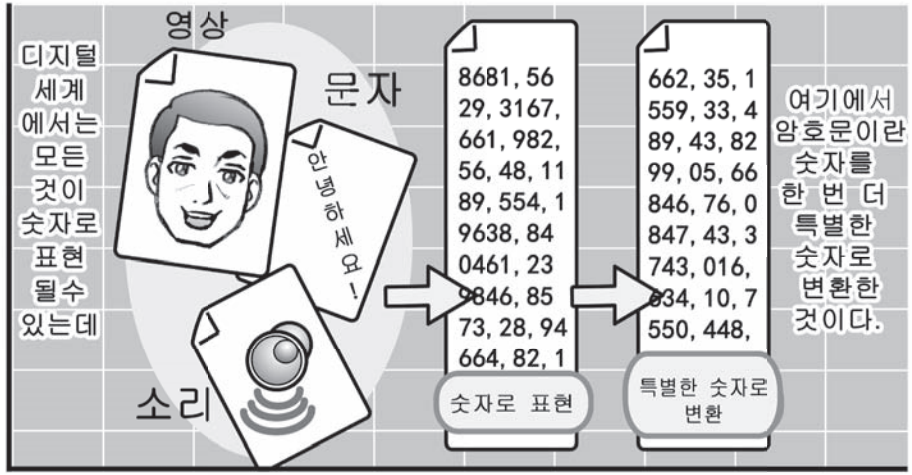
부..분명히 공개키 암호와 관계가 있는것 같은데…

Yes!

먼저, 공개키 암호의 구조를 이해해야 하죠.

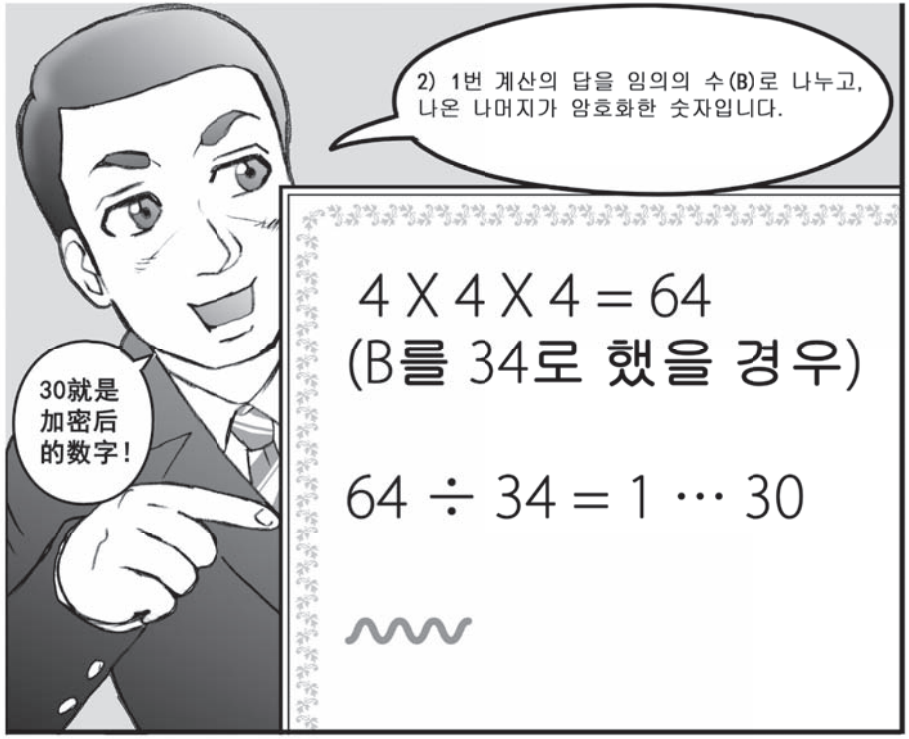

공개키암호화라는 하나의 표현을 쓰지만, 구체적인 방법은 여러가지 입니다.
실제로는 공개키암호 이외의 다른 방법을 함께 사용하고 있습니다.
공개키암호에서 현재 표준으로 사용되고 있는 것은 'RSA암호' 라고 불리는 것입니다.
앞에서, 공개키에 암호화한 암호문은 비밀키를 통해서만 원래의 글로 되돌릴 수 있다고 했는데
RSA

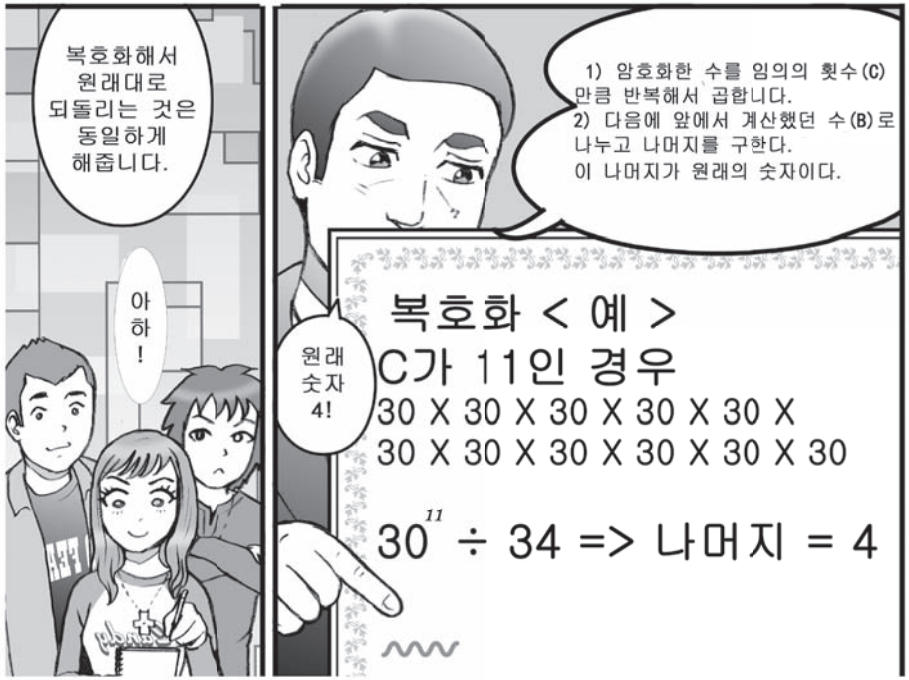

RSA암호에서는 그것뿐만이 아니라, 비밀키로 암호화한 암호문을 공개키를 이용하여 원래대로 되돌리는 것까지 할 수 있습니다.
아오야가 쓴거에염
비밀키
이것을 이용하면, '이건 내가 쓴 것입니다.' 라는 것을 증명할 수 있다.
공개키
그렇구나!!


디지털 세계에서는 모든 것이 숫자로 표현 될수 있는데
영상
문자
소리
안녕하세요!
8681, 56 29, 3167, 661, 982, 56, 48, 11 89, 554, 1 9638, 84 0461, 23 9846, 85 73, 28, 94 664, 82, 1
숫자로 표현
662, 35, 1 559, 33, 4 89, 43, 82 99, 05, 66 846, 76, 0 847, 43, 3 743, 016, 034, 10, 7 550, 448,
특별한 숫자로 변환
여기에서 암호문이란 숫자를 한 번 더 특별한 숫자로 변환한 것이다.


RSA암호는 다음과 같은 순서로 암호화가 됩니다.
Let's study!!

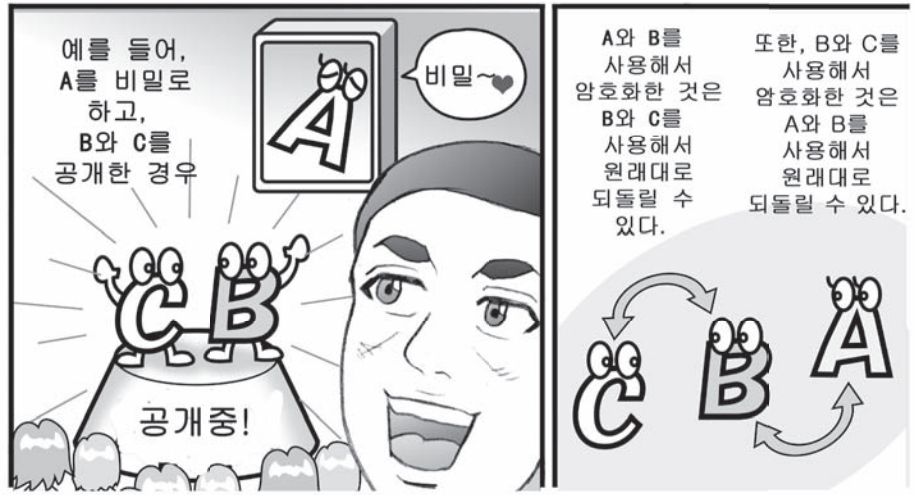

1) 먼저 기준이 되는 숫자를 임의 수(A)만큼 반복해서 곱합니다.
< 예 >
4 X 4 X 4 의 경우
3번 곱했기 때문에
A = 3


2) 1번 계산의 답을 임의의 수(B)로 나누고, 나온 나머지가 암호화한 숫자입니다.
4 X 4 X 4 = 64
(B를 34로 했을 경우)
64 ÷ 34 = 1 … 30
30就是加密后的数字!

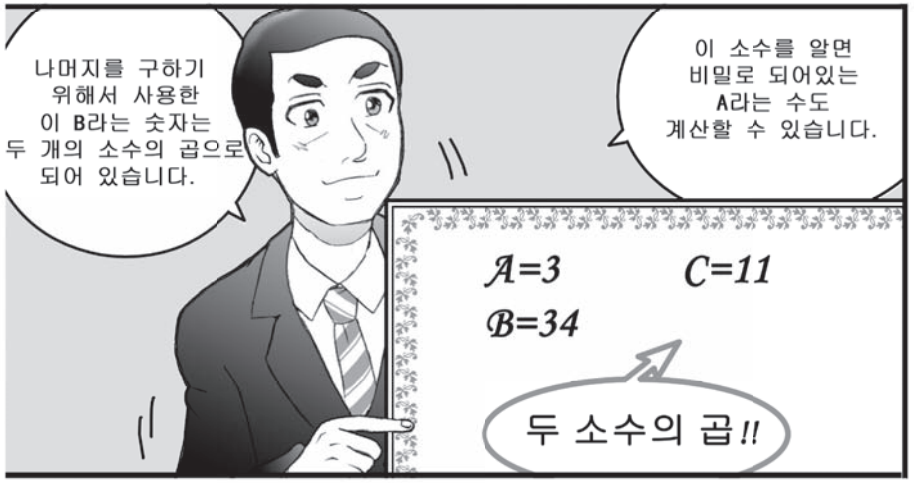

복호화해서 원래대로 되돌리는 것은 동일하게 해줍니다.
아하!
1) 암호화한 수를 임의의 횟수(C)만큼 반복해서 곱합니다.
2) 다음에 앞에서 계산했던 수(B)로 나누고 나머지를 구한다.
이 나머지가 원래의 숫자이다.
원래 숫자 4!
복호화 < 예 >
C가 11인 경우
30 X 30 X 30 X 30 X 30 X
30 X 30 X 30 X 30 X 30 X 30
30^11 ÷ 34 => 나머지 = 4

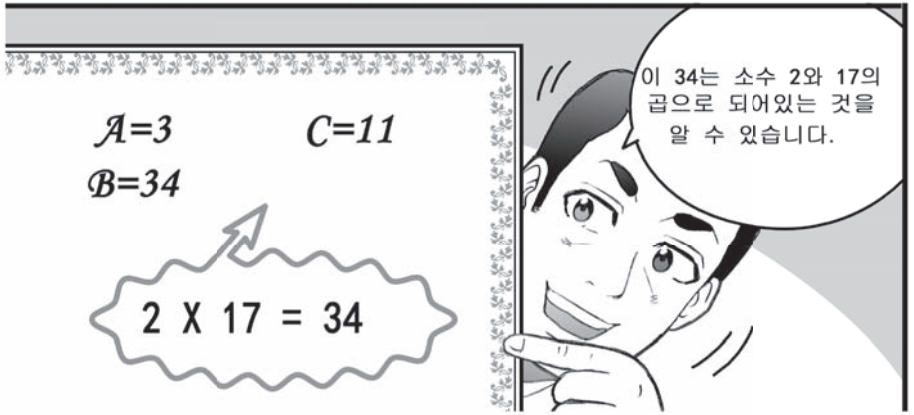

암호로 만드는 순서도 원래로 되돌리는 순서도 모두 정해져 있는 거네요.
Yes!
예전에는, 보내는 사람과 받는 사람이 암호를 만드는 방법, 푸는 방법이나, 암호의 열쇠를 비밀로 공유해야 했지만

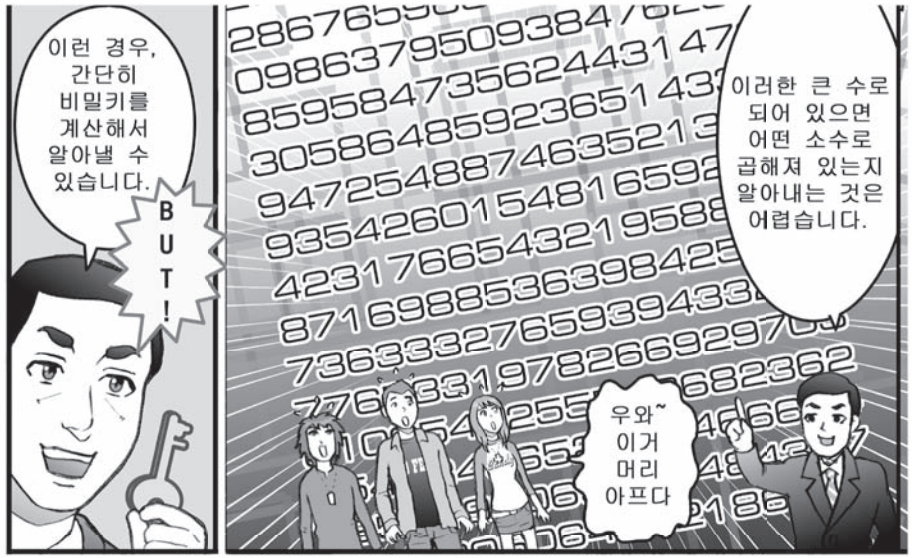

비밀키를 안전하게 공유하는게 어렵기 때문에
공개키암호라면 순서도 공유키도 공개해서, 비밀키만 안전하게 관리하면 되니까 안심이 되지요.
C B A
RSA암호에서는 A, B, C 쪽이 암호의 열쇠가 되는 겁니다.


예를 들어, A를 비밀로 하고, B와 C를 공개한 경우
A
비밀~
C B
공개중!
A와 B를 사용해서 암호화한 것은 B와 C를 사용해서 원래대로 되돌릴 수 있다.
또한, B와 C를 사용해서 암호화한 것은 A와 B를 사용해서 원래대로 되돌릴 수 있다.
C B A


B는 암호를 만들때도, 원래대로 되돌릴 때도 쓰는거군요.
B
맞아요. 실은 이 B가 이 암호의 강력한 점 입니다.
A, B, C의 숫자는 어떤 수를 넣어도 되는 것이 아닙니다.
RSA암호의 개발자는 어떤 수를 넣어야 수식이 성립하는지를 나타내었다.

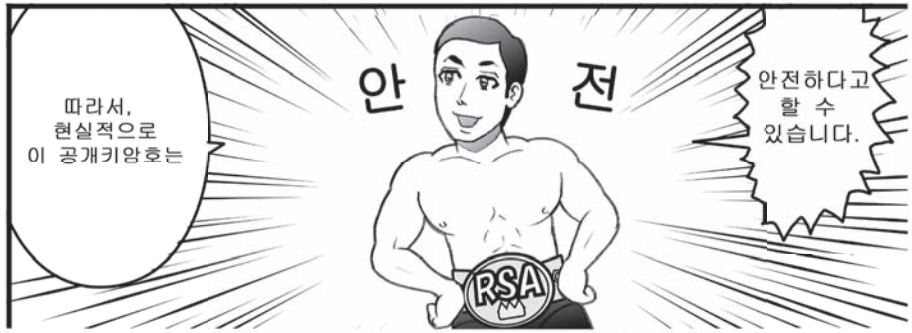

나머지를 구하기 위해서 사용한 이 B라는 숫자는 두 개의 소수의 곱으로 되어 있습니다.
이 소수를 알면 비밀로 되어있는 A라는 수도 계산할 수 있습니다.
A=3
C=11
B=34
두 소수의 곱!!

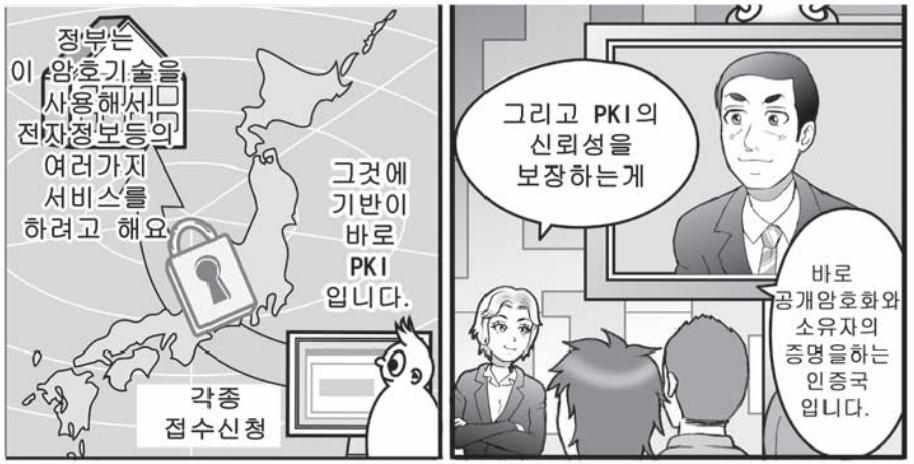

A=3
C=11
B=34
2 X 17 = 34
이 34는 소수 2와 17의 곱으로 되어있는 것을 알 수 있습니다.


이런 경우, 간단히 비밀키를 계산해서 알아낼 수 있습니다.
B U T !
이러한 큰 수로 되어 있으면 어떤 소수로 곱해져 있는지 알아내는 것은 어렵습니다.
우와~ 이거 머리 아프다


이러한 수가 어떤 소수의 곱으로 되어 있는지를 발견하기 위해서는
알려져 있는 소수들 중에서 하나씩 하나씩 대입해 보는 수 밖에 없습니다.


세계에서 가장 빠른 컴퓨터를 사용해서 1초에 천조번 계산할 수 있어도 엄청난 시간이 걸립니다.


따라서, 현실적으로 이 공개키암호는
안 전
안전하다고 할 수 있습니다.
RSA



漫画：門倉つりっツ書浩

用語集

【자료】

공개키번호

공개키번호에서는 암호화와 디코딩에 다른 키를 사용한다. 이들 키는 하나의 짝으로 되어있어 그 속의 한쪽 키를 공개한다. 메시지를 상대로부터 보내지는 경우를 생각해 본다. 상대가 암호화 할 때에 사용하는 키를 공개해 두고 그것을 사용하여 암호화되어 송부 받게 한다. 그것을 디코딩 할 때에 사용하는 키는 자신만이 가지고 있으면 메시지는 안전하게 받을 수 있다. 공개하는 키를 공개키, 비밀로 하는 열쇠를 비밀키라고 한다. 공개키번호의 방식은 몇 개나 제안되고 있지만 현재 현실에 사용되고 있는 것은 다음 항에 있는 RSA 암호다. 예를 들면 SSL에서의 (https로부터 시작되는 URL에 있어서의) 통신은 일상적으로 사용되고 있다.

RSA암호

리베스토, 샤미아, 에델먼에 의해 1976년에 개발된 공개키번호를 3명의 머리 문자를 따서 RSA암호라고 부른다. 암호화 및 디코딩은, 정수완 인수 계산을 사용한다. 해독에는 소인수분해가 필요하여 최고성능의 컴퓨터를 구사해도 소인수분해가 현실적으로 불가능한 큰 정수를 사용하는 것으로 보안 강도를 보증한다.

인증국

공개키번호를 시스템으로서 성립되게 하기 위해서는, 열쇠의 소유자가 특별히 지정되어 안전하게 관리되지 않으면 안 된다. 이것을 짊어지고 있는 것이 인증국이다. 인증국은 국제적 기관으로 정보 보안에 관해 신뢰할 수 있는 기관이 아니면 안 된다.

전자서명

적당한 문장과 그것을 비밀키로 암호화한 암호문을 보내면 수신자는 암호문을 공개키로 디코딩 하고, 그것을 암호화 전의 문장과 비교하여 일치시킴으로써 비밀키의 소유자가 보낸 것임을 확인할 수 있다. 여기에서 이것을 전자서명이라고 부른다. 실제로는 송신한 텍스트를 요약 함수를 사용하여 압축한 문장을 비밀키로 암호화해서 보내면 수신자는 보내진 텍스트를 같은 요약 함수를 사용해서 압축하고 디코딩 한 문장과 비교하는 것이 행해지고 있다.

공개키번호의 장치

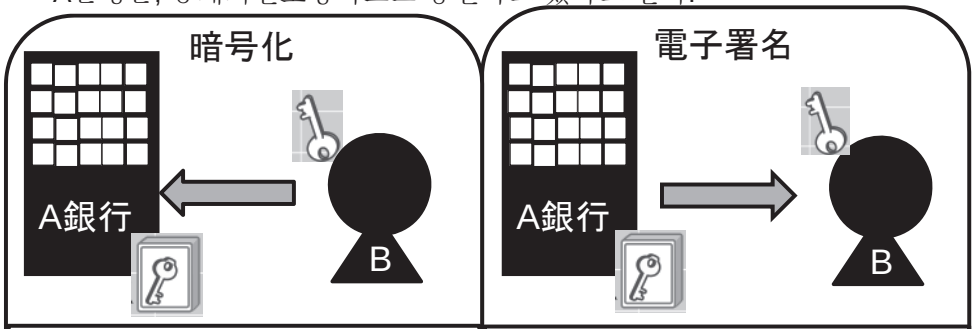
현재의 사회에서는 정보통신 속에서 암호화가 일상적으로 사용되고 있다. 암호는 왜 필요한 것일까? 예를 들면 인터넷쇼핑이나 온라인 은행에 있어서의 정보의 교환에서는 금전의 수수가 행하여진다. 그 때 정보가 외부에 새는 것은 용서되지 않는다. 인터넷을 할 때에는 내용을 제 삼자에게 알리지 않고 상대에게만 확실하게 정보를 전하는 것 (다른 사람에게는 흘리지 않는다)이나, 확실하게 발신자를 특정시킬 수 있어 만약 내용의 개편이 발생하면 그것을 검출 시킬 수 있다. (개편, 위장을 막는 것) 이 필요하다. 여기에서 전자를 위해 암호화가, 후자를 위해서 전자서명이 사용되고 있다.

웹 사이트상의 정보 교환으로 인터넷이 사용된다. 인터넷에서는 정보의 분리(패킷화)로 하여 전하며, 통신 경로에는 각양각색의 중계 기기(라우터)가 존재하고 있다. 통신 내용을 암호화함으로써 도청을 막을 필요가 있다. 또 암호화된 정보의 디코딩은 대단히 어려운 것이 아니면 안 된다.

일반적으로 기업은 다수의 고객을 안고 있다. 암호를 위해서 고객고유의 키를 매회 생성, 배포하는 것은 곤란하다. 이것을 해결하는 것이 공개키번호 방식이다. 공개키번호에서는, 이하의 성질을 가진 공개키와 비밀키의 두 가지 키를 사용한다.

■공개키로 암호화한 메시지는, 비밀키에서 밖에 디코딩 할 수 없다.
■비밀키로 암호화한 메시지는, 공개키로밖에 디코딩 할 수 없다.

A은행은, 공개키번호방식으로 통신하고 있다고 한다.



A은행의 공개키에서 암호화된 정보는 비밀키를 가지고 있는 A은행에서 밖에 디코딩 할 수 없다.(중간 다른 장치 없음). A은행뿐만 디코딩 할 수 있기에 이용자는 같은 공개

A은행의 비밀키로 암호화된 정보는 A은행만 생성할 수 있다. 이용자B로의 통지에서 A은행의 비밀키를 사용하여 생성한 전자서명을 부가함으로써 이용자B는 확실하게 A은

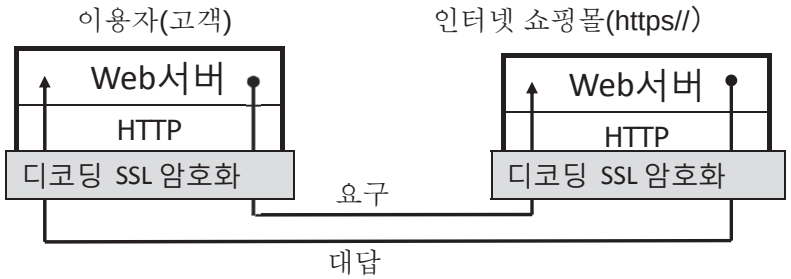
실제의 SSL통신

공개키번호가 제안되기 전에는 암호라고 하면 공통의 열쇠를 이용하여 암호화· 디코딩을 하는 것이었다. (공통키암호). 공통키에서의 큰 문제는, 키를 어떻게 안전하게 보내는 사람과 수신자가 공유할 지다. 인터넷상에서의 교환에서는 열쇠를 직접 상대에게 주고받을 수 없다. 안전하게 열쇠의 수수를 하는 것은 어렵다. 최근에는 공개키번호의 구조가 만들어져 안전하게 메시지의 교환을 할 수 있게 되었지만 공개키번호에서는 공통키암호에 비해 처리 속도가 늦은 것이 난점이다. 이 장점·단점을 비추어 실제로는 다음과 같은 것이 행해지고 있다.

•메시지는 공통키방식으로 암호화하여 통신한다.
•그 공통키는 공개키방식으로 암호화하여 통신한다.

즉, 공개키방식으로 안전하게 공통키의 수수를 하고, 그 후는 그 공통키로 메시지를 교환하는 것이다. 그 예로서, 여기에서는 인터넷상의 쇼핑몰에 접속하여 쇼핑을 하는 것을 예로 들 수 있다.

⓪서버 상에 증명서등록완료의 공개키, 비밀키가 등록되어있다.
①이용자에게서 요구가 있으면, 서버는 공개키를 증명서부착으로 이용자에게 보낸다.
②이용자 측은 공개키가 진짜인 것을 확인하고, 공통키를 발행하여 서버에 보낸다.
③서버상에서 비밀키를 사용하여 공통키를 얻은 후 그 공통키를 이용하여 암호화 통신을 시작한다.



이러한 순서를 거침으로서 암호화된 내용을, 통신 도중에는 다른 곳에 흘리지 않고 보낼 수 있다.

RSA암호에 있어서의 문자열의 암호화•디코딩【발전항목】

여기서는, RSA암호로 어떻게 메시지를 암호화·디코딩 하고 있는지에 대한 개략을 나타낸다.

●RSA암호의 알고리즘

【암호화】

①메시지의 문자열을 정수화시킨다.
②각각의 정수에서 대하여,
암호의 정수= mod (원의 정수^{C}, B)
여기서, C, B는 공개키 (원의 정수< B)
상기의 식으로부터, 암호화된 정수를 추구한다.
한편, mod(x, y)이라고 한 표기는 x 을 y 로 나눈 나머지를 나타낸다.

【디코딩】

①각각이 암호화되고 있는 정수에서 대하여,
원래의 정수= mod(암호의 정수^{A}, B)
여기서 A는 비밀키
상기의 식으로부터, 원래의 정수를 추구한다.
②추구된 정수를 문자열화시킨다..

●공개키로 이용하는 열쇠A, B, C의 생성 방법
① 다른 소수p 및 q를 적당히 선택한다. B = p × q
② j 은, 최소 공배수(p-1, q-1)로 한다.
③ j 과 서로 근본이 되는 C를 적당히 선택한다. (최대공약수(j ,C)=1)
④ mod(C × A, j)=1 되는 A를 요구한다.

여기에서, B와 C가 공개키로 A가 비밀키이다. 해독되지 않기 위해, 큰 숫자를 사용한다. B는 2개의 소수의 적분이 되고 있다. 즉, B를 2개의 소수의 적분(소인수분해)할 수 있으면, RSA암호의 알고리즘은 위에서 말한 바와 같이 미리 결정되어 있으므로 비밀키를 계산할 수 있게 된다. 따라서 이 암호의 강도는 B가 얼마나 큰 숫자인지에 의존하게 된다. 소인수분해는 대상의 정수가 크면 클수록 급격하게 어려워진다. 현재 안전성이 높은 암호가 되기 위해서는 B가 2048비트 (2048자릿수의 0/1의 나열)이상으로 요구되고 있다. 이것은, 미국 국립표준기술연구소가 낸 정부기관에서의 사용에 필요로 되는 요건이며, 2010년까지의 이행을 요구하고 있는 것으로, 암호의 2010년 문제라고 불리고 있다.