서장 인터넷의 기초

0-1 인터넷 리터러시

인터넷은 신문, 라디오, 텔레비전에 이은 새로운 미디어로 탄생했습니다. 다만 이 미디어로 정보를 받아들일 때는 신문, 라디오, 텔레비전에 비해 얻을 수 있는 정보의 신뢰성을 충분히 따져봐야 합니다.

인터넷 상에서는 공공기관이나 기업, 나아가 개인까지 누구나 손쉽게 SNS 에 글을 올리거나 동영상을 게시할 수 있습니다. 따라서 정보의 신뢰성이 반드시 높지 않다는 한계가 있습니다. 인터넷을 통해 얻은 정보에 대해서는 그것이 정확한지 스스로 판단해야 합니다.

1. 미디어 리터러시

정보는 발신자가 의도하는 대로 가공하여 만들어집니다. 예를 들어 일부를 일부러 강조하거나 반복함으로써 정보가 주는 인상을 바꿀 수 있습니다. 따라서 정보 수신자는 원래 의미와 다르게 정보를 받아들일 수 있습니다. 편향된 정보나 허위 정보(유언비어)에 휘둘리지 않으려면 미디어의 특성을 이해하고 판단하는 능력이 필요합니다. 이처럼 수집한 정보를 주체적·비판적으로 분석·평가하는 능력을 '미디어 리터러시'라고 합니다. 특히 다음 4 가지를 고려하여 정보를 판단하는 것이 좋습니다.

・여러 정보원(도서·신문·TV·블로그 등)에서 확인한다.
・이 정보로 이익을 보는 사람은 누구인가. 손해를 보는 사람은 누구인가. 이해득실을 따져가며 퍼지는 정보가 아닌지 따져보는 습관을 기른다.
・데이터 수집 방법과 데이터 표현 방식, 데이터를 제시하는 진짜 목적이 무엇인지 생각한다.
・어떤 정보가 전달되고 있고, 어떤 정보가 빠져 있는지 생각한다.
・어떤 입장의 사람이, 어떤 의도로 보낸 정보인지 생각한다.

2. 정보 윤리

인터넷이 전 세계에 보급되면서 시간과 거리의 제약 없이 소통하고 정보를 교환할 수 있게 되었습니다. 하지만 그 이면에는 부적절한 정보가 의도적으로 퍼지거나, 이전에는 없던 새로운 유형의 범죄가 증가하는 등의 문제도 일어나고 있습니다.

정보 윤리(정보 도덕)란 본래 정보를 다루는 데 있어서 '사람이 지켜야 할 도리'를 의미하며, 네트워크 사회뿐만 아니라 현실 사회에서도 중요한 의미를 지닙니다. 인터넷이 보급되어 누구나 손쉽게 다양한 정보를 주고받을 수 있게 된 현재, 정보 윤리의 중요성이 더욱 커지고 있습니다.

현실 사회와 마찬가지로 네트워크 사회에서도 타인에게 피해를 주거나 범죄에

휘말리지 않기 위해서는 올바른 의식과 구체적인 지식이 필요합니다.
네트워크 사회의 편리함을 누리기 위해서는 네트워크 사회의 일원인 우리 각자가 정보 윤리의 중요성을 나의 일처럼 진지하게 고민해야 합니다.

0-2 사이버 범죄

인터넷을 비롯한 정보통신기술이 보급되면서 일상생활이 편리해졌습니다. 하지만 그 이면에는 각종 문제에 직면할 위험도 있습니다.

총무성의 「(2023 년) 통신 이용 동향 조사」(2024 년 6 월 공표)에 따르면, 국내 인터넷 이용률(개인)은 86.2%입니다. 인터넷 이용자 비율은 13~59 세 각 연령대에서 90%를 넘고 있습니다. 기업이나 단체 외에도 개인을 대상으로 한 교묘한 수법의 사이버 범죄가 늘어나고 있으며, 스마트폰 보급과 함께 다양한 피해가 잇따르고 있습니다.

1. 사이버 범죄의 경향

2023 년(레이와 5 년), 사이버 범죄 검거 건수는 12,479 건으로 2021 년부터 높은 검거 실적을 유지하고 있습니다.

불법접속금지법 위반 사건의 검거 건수는 521 건으로 전년 522 건과 거의 같은 수준입니다. 대학 등의 학술 기관을 노려 정보를 탈취하는 불법 접속이 빈번히 발생하고 있습니다.

악성코드 등 무단 명령 전자기록 관련 범죄 및 컴퓨터·전자 기록 대상 범죄는 1,000 건에 달해 전년(948 건) 대비 증가했습니다. 신용카드 부정 사용과 인터넷 뱅킹 부정 송금이 역대 최다를 기록했습니다.

멀웨어로 인한 피해 중에서도 특히 랜섬웨어를 이용한 공격이 눈에 띄게 늘고 있습니다. 데이터를 암호화하는 패턴뿐만 아니라, 데이터를 암호화하지 않고 탈취한 정보를 공개하겠다고 협박하는 수법도 늘고 있습니다.

0-3 학교 이용 규칙과 예절

1. 원격 수업을 수강한다

코로나 19 감염 확산 방지를 계기로 Zoom 이나 Microsoft Teams 등의 화상 회의 시스템을 활용한 원격 수업과 화상 회의 활용이 크게 늘었습니다. 원격 수업을 수강할 때는 다음 사항에 유의하시기 바랍니다.

・소프트웨어나 앱은 공식 사이트에서 다운로드한다.
・메시지 오전송이나 화면에 비친 내용에 주의한다.
・수업 참가자 외에는 URL 이나 회의 번호를 알려주지 않는다.
・이름은 본명으로 한다(학교의 지시가 있으면 그에 따른다).

※본명이 아닐 경우, 무관한 사람으로 오인되어 결석 처리되거나 원격 수업 접근이 거부될 수 있습니다.

- 단정한 복장을 갖춘다.
- 시간에 늦지 않는다.
- '딴짓'을 하지 않고 수업에 집중한다.
- 수업을 무단으로 촬영·녹화·녹음하지 않는다(허용된 경우에도 적절한 범위 내에서만 이용한다).

0-4 휴대 단말기 이용

1. 본체 관리

스마트폰이나 휴대전화 등의 휴대 단말기를 사용하는 사람들은 그 안에 가족이나 친구·지인의 전화번호나 이메일 주소 등의 개인정보를 저장하고 있습니다. 휴대 단말기의 분실이나 방치는 개인정보 유출로 이어질 수 있습니다. 지인이나 친구의 개인정보를 보호하기 위해서도 자신의 휴대 단말기는 책임감 있게 관리해야 합니다. 주요 관리 사항은 다음과 같습니다.

- 분실이나 도난 시 대책으로 비밀번호를 설정하고 잠금을 걸어둔다.
- 운영 체제(OS)를 최신 버전으로 업데이트한다.
- 스마트폰의 경우 무단 개조(탈옥, 루팅 등)를 하지 않는다.
- 앱은 신뢰할 수 있는 곳(공식 마켓)에서 설치한다.
- 안드로이드 기기에서는 앱 설치 전에 접근 권한(퍼미션) 항목을 확인한다.
- 앱 설치 후에도 정기적으로 사용자 리뷰를 확인한다.
- 평가가 좋지 않거나 개인정보 보호가 우려되는 앱은 삭제하는 것이 좋다.
- 스마트폰에 보안 소프트웨어(백신 앱)를 설치한다.

2. 사용상의 주의사항

스마트폰이나 휴대전화 등의 휴대 단말기를 사용할 때는 다음과 같은 예절을 지켜야 합니다. 또한 주변에 사람이 있을 때는 큰 소리로 통화하지 않는 등 주변 사람에 대한 배려가 중요합니다.

촬영 기능 사용 시 주의사항

휴대 기기의 촬영 기능을 이용해 찍은 사진이나 영상을 공유하는 사람들이 늘고 있습니다. 간편하게 촬영할 수 있어 편리하지만, 반면에 '몰래 촬영'이나 서점 등에서 책을 무단으로 촬영하는 이른바 '디지털 절도' 같은 범죄가 발생하고 있습니다.

아무 생각 없이 찍은 사진이나 영상이라도 당사자의 허락 없이 웹 페이지나 SNS 등에 게재하는 것은 사생활 침해, 초상권 침해, 저작권 침해에 해당할 수 있으니

삼가야 합니다.

걸으면서 스마트폰을 하는 것은 매우 위험합니다

스마트폰을 조작하면서 걷는 것은 매우 위험한 행위입니다. 사람뿐만 아니라 자동차나 자전거와 부딪히는 사고가 발생할 수 있습니다. 역 계단에서 넘어지거나 플랫폼에서 추락하는 사고도 실제로 발생하고 있습니다. 또한 주변에 대한 주의가 소홀해지기 때문에 수상한 사람의 표적이 될 수 있습니다.

자신뿐만 아니라 주변 사람을 위험에 빠뜨릴 수도 있으므로, 걸으면서 스마트폰을 사용하는 것은 위험한 행동임을 인식하고 절대 하지 마십시오.

운전 중에는 사용하지 마십시오

운전 중 휴대전화 사용으로 많은 교통사고가 발생하고 있습니다. 운전 중에는 전원을 끄거나 운전 모드로 설정하고, 안전한 곳에 차를 세운 후 휴대폰을 사용하세요. 운전 중 휴대전화 사용은 도로교통법 위반입니다.

또한 자전거 운전 중 스마트폰 조작 등의 '운전 중 휴대폰 사용'은 도로교통법 제 70 조에 정해진 '안전운전의 의무' 위반에 해당합니다.

이는 자동차든 자전거든 운전 중 스마트폰 등을 사용하면 화면에 주의가 쏠려 주변 상황 인지가 늦어져 사고로 이어지기 때문입니다. 또한 함께 헤드폰 등을 착용하면 주변 상황을 소리로 인지하기도 어려워져 사고를 유발하기 때문입니다.

운전 중 스마트폰 사용 등의 위반 행위를 하지 않도록 하십시오.

제 1 장 사용자 인증과 계정

1-1 비밀번호 설정 및 관리

비밀번호는 중요한 정보이므로 타인에게 알려지지 않도록 철저히 관리해야 합니다. 또한 비밀번호를 설정할 때는 타인이 추측하기 쉬운 문자열로 설정하지 않도록 주의해야 합니다.

학교마다 규정이 다를 수 있으므로 해당 학교의 규정을 따르십시오.

1. 비밀번호 관리 책임

비밀번호는 컴퓨터 사용자가 정당한 사용자 본인임을 확인하는 중요한 정보입니다. 악의적인 제 3 자에게 노출되면 시스템에 불법 접속당하고, 시스템은 물론 네트워크 전체의 보안까지 위협받을 수 있습니다.

단순한 비밀번호 하나라고…… 얕잡아봐서는 안 됩니다. 하나의 비밀번호로 시스템에 침입한 해커는 네트워크상의 다른 시스템까지 침투하여 범죄에 악용할 수도 있습니다. 단 한 사람의 부주의가 시스템 사용자 전체에 피해를 줄 수 있습니다. 비밀번호 관리에 각별히 주의하십시오.

2. 비밀번호를 다룰 때의 주의사항

비밀번호를 다룰 때는 다음 사항을 준수하십시오.

・비밀번호는 가족이나 가까운 친구에게도 알려주지 않는다.
・비밀번호를 눈에 띄는 곳에 메모해 두거나 모니터에 붙여놓지 않는다.
・비밀번호를 공용 컴퓨터에 저장하지 않는다(자동 완성 기능도 사용하지 않는다).
・비밀번호를 소리 내어 말하지 않는다.
・이메일에 비밀번호를 적지 않는다.
・비밀번호를 입력할 때는 손가락 움직임을 다른 사람에게 노출하지 않는다.
・ 비밀번호가 도용되었거나 타인에게 노출된 것으로 의심되면 즉시 비밀번호를 변경한다.

3. 나쁜 비밀번호의 예

아래에 제시된 것은 타인이 추측하기 쉬운, 보안에 취약한 비밀번호입니다. 이러한 비밀번호는 설정하지 않도록 유의하십시오.

・자신이나 가족, 친구, 애완동물의 이름(Masako, Pochi, Tama 등)
・자신의 생일이나 전화번호, 그 외 타인이 쉽게 알아낼 수 있는 개인정보를 사용한 문자열(July04 등)
・사전에 실려 있는 단어
・지명, 인명, 구단명 등의 고유명사(Kyoto 등)
・모두 같은 알파벳(AAAAAAAA 등)
・과거에 사용했던 비밀번호
・키보드에서 인접한 문자열(asdf, qwer 등)
・위 비밀번호의 철자를 뒤집거나 숫자만 덧붙인 것(0toyk77, masako3 등)

4. 좋은 비밀번호의 요령

아래는 안전한 비밀번호 설정을 위해 일반적으로 권장되는 기준입니다.

・대문자, 소문자, 숫자, 특수 기호를 혼합한다.
・자신은 기억하기 쉽고 타인은 추측하기 어려운 문자열
・10 자 이상의 충분한 길이.

5. 더 안전한 비밀번호 설정 요령

다음 방법을 활용하면 더 안전한 비밀번호를 만들 수 있습니다.

문장의 단어의 첫 글자를 사용한다
  자신만 알고 있는 사실을 영문(또는 로마자 표기)으로 만든다.
예문 Our family went to Nikko by train in April.
  단어의 첫 글자를 취한다 → ofwtnbtia
  대문자, 소문자를 섞는다 → OfwtNbtiA
  특수 기호를 섞는다 → OfwtNbtiA#

6. 비밀번호 재사용은 위험합니다
  인터넷 서비스는 대부분 가입할 때 비밀번호를 설정해야 합니다. 새로운 서비스에 가입할 때마다 비밀번호가 늘어나고, 비밀번호가 늘어나면 기억하기가 어렵습니다.
  하지만 그렇다고 해서 모든 서비스에 같은 비밀번호를 사용하는 것은 위험합니다.
어떤 인터넷 서비스에서 비밀번호가 유출되었다고 가정해 보겠습니다. 다른 서비스에도 같은 비밀번호를 설정해 두었다면, 무단 로그인을 당할 수 있습니다. 이를 '계정 탈취'라고 합니다. 쇼핑 사이트나 SNS 에서 비밀번호가 유출된 결과, LINE 계정을 탈취당한 사례가 있습니다.
따라서 여러 서비스에서 비밀번호를 재사용하는 것은 가급적 피해야 합니다.

리스트형 공격(비밀번호 리스트 공격, 리스트형 계정 해킹)
  불법으로 입수한 사용자 ID 와 비밀번호 목록을 이용해 불법 접속을 시도하는 공격입니다. 인터넷 쇼핑 등 다양한 웹사이트에서 동일한 비밀번호를 재사용하는 사용자가 많아 이러한 공격에 의한 피해가 속출하고 있습니다.

서비스별로 설정한 비밀번호를 관리하기 위한 비밀번호 관리 도구도 시중에 출시되어 있습니다.
또한 서비스별로 다른 비밀번호를 만들려면 평소 사용하는 비밀번호에 서비스명 약어를 붙이는 방법도 있습니다.

  다만, "line", "facebook" 등 원래 비밀번호와 서비스 이름의 구분이 쉽게 추측될 수 있는 방식은 적절하지 않습니다. 이러한 방식을 사용하면 어느 한 서비스에서 비밀번호가 유출될 경우 다른 서비스의 비밀번호도 쉽게 추측될 수 있어 위험합니다. 비밀번호에 서비스 이름을 포함할 경우 기호를 섞는 등 방법을 고안해야 합니다. 또한 여기서 사용한 예시를 그대로 사용하는 것도 위험하므로 삼가야 합니다.

Iau1BET# + l!E（LINE） → Iau1BET#**l!E**
Iau1BET# + f!K（facebook） → Iau1BET#**f!K**

1-2 사용자 ID 와 비밀번호의 무단 탈취

악의적으로 타인의 컴퓨터나 네트워크 시스템에 무단 침입하여 데이터를 파괴·변조하거나 엿보는 행위를 크래킹이라고 합니다. 또한 이런 행위를 하는 사람을 크래커라고 합니다.

크래커는 다양한 방법으로 타인의 비밀번호를 알아내 네트워크에 침입합니다. 주요 수법을 아래에 정리합니다.

무차별 대입 공격

가능한 문자 조합을 모두 대입하는 방식으로 비밀번호를 해독하는 방법입니다. 사람이 직접 하기는 어렵지만, 컴퓨터에 맡기면 비밀번호 문자열이 짧은 경우 비교적 짧은 시간에 해독할 수 있습니다.

사전 공격

해커는 비밀번호 해독을 위한 전용 사전(단어 목록)을 사용합니다. 이 사전에 수록된 등록된 모든 단어를 비밀번호로 대입하는 프로그램을 통해 타인의 비밀번호를 해독합니다. 대규모 사전에는 30 만 개 이상의 단어가 수록되어 있으며, 영어 단어는 물론 유명 과학자나 정치인의 이름, 스포츠 선수나 아이돌의 이름 등도 포함되어 있습니다.

소셜 엔지니어링(소셜 크래킹)

네트워크 사용자에게 관리자나 관계자인 척 전화·이메일로 접근하여 비밀번호를 알아내는 수법입니다.

또한 키보드 입력을 엿보거나 휴지통을 뒤지는 행위도 소셜 엔지니어링에 해당합니다.

키로거

키로거(Keylogger)란 사용자의 키보드 입력을 기록하는 소프트웨어로, 원래는 프로그래머가 입력 기록을 디버깅 등에 활용하는 도구였습니다.

그러나 인터넷카페 등 공용 컴퓨터에 키로거가 설치되어 비밀번호가 도난당하는 사건이 발생하고 있습니다. 여러 사람이 공동으로 사용하는 인터넷카페 등의 컴퓨터에 중요한 개인정보(계정이나 신용카드 번호 등)를 입력하는 것은 피하는 것이 안전합니다.

피싱

가짜 사이트로 유인하여 사용자 ID 나 비밀번호를 입력하도록 유도해 이를 훔쳐내는 수법은 '피싱'이라 하며, 불법 접속의 일종에 해당하는 범죄입니다.

비밀번호가 일단 해커의 손에 넘어가면, 사칭당하여 더 많은 정보를 빼앗길 수 있습니다. 결국에는 그 계정을 악용하여 다른 네트워크까지 침입당해 피해가 확대될 위험이 있으므로, 비밀번호 관리가 매우 중요합니다.

통신 감청

인터넷상의 통신은 도청당할 위험이 있습니다. 그러나 후술하는 통신 암호화를 통해 도청되더라도 내용이 해독될 가능성은 크게 낮아집니다. 따라서 ID 나 비밀번호 등 중요한 정보를 입력할 때는 통신이 암호화되어 있는지 확인하십시오.

특히 무료로 사용 가능한 무료 Wi-Fi 에서 비밀번호가 설정되지 않은(암호화되지 않은) 경우, 도청되어 내용이 노출될 위험이 있습니다. 또한 불특정 다수가 이용하는 호텔 등의 공용 컴퓨터를 사용할 때에도 주의해야 합니다.

메모 앱

스마트폰 등의 메모 앱은 클라우드에 데이터가 자동 저장되어 매우 편리하지만, 클라우드 서버에 취약점이 있으면 정보가 유출될 위험이 있습니다. 따라서 메모 앱에 비밀번호 등 민감한 정보를 저장하지 마십시오.

1-3 인증 방식

사용자를 인증하는 방식에는 앞 절에서 살펴본 비밀번호 외에도 다음과 같은 것들이 있습니다.

1. 일회용 비밀번호 인증

부정한 접속에 의한 비밀번호 도용을 방지하는 방법으로 일회용 비밀번호 인증이 있습니다. 일회용 비밀번호는 이름에서 알 수 있듯이 매번 로그인 시 발급되며, 한 번만 사용할 수 있는 일회용입니다. 누군가에게 알려지더라도 해당 비밀번호는 다음 로그인 시 자동으로 무효화됩니다.

2. 생체 인식 인증

생체정보를 이용한 인증 방식을 생체인증(바이오메트릭스 인증)이라고 합니다. 인증에 사용되는 생체정보로는 지문, 얼굴, 음성, 손바닥이나 손가락의 정맥, 눈의 홍채 등이 있으며 각각 전용 장치가 필요합니다.

이 중 가장 널리 보급된 방식은 지문을 이용한 인증입니다. 노트북이나 USB 메모리, 최근에는 스마트폰 등 소형이라 분실·도난 위험이 큰 기기에 지문 인증 센서가 장착되어 판매되고 있습니다.

생체 인증에 사용하는 것은 신체적 특징이기 때문에 분실이나 망각의 우려가

없습니다. 반면, 도입 비용이 높고, 노화나 부상, 질병으로 인해 본인이라도 인증에 실패할 가능성도 있습니다.
초기에는 신체적 특징을 이용하기 때문에 복제가 어려워 비밀번호 인증보다 강력한 보안을 확보할 수 있었습니다. 그러나 최근에는 생체 인증을 뚫는 기술도 진화해 왔기 때문에, 반드시 안전하다고 단언할 수 없게 되었습니다.

3. 다중 요소 인증

IC 카드와 정맥 인증을 결합한 방식을 도입하는 은행도 있습니다. 이를 2 요소 인증이라고 합니다.
그 외에도 비밀번호와 지문 조합 등이 있습니다. 여러 요소를 결합한 인증 방식을 총칭하여 다중 요소 인증(MFA)이라고 합니다. 단일 인증보다 강력한 보안을 확보할 수 있습니다.

4. 2 단계 인증

다중 인증과 마찬가지로 인증 강화를 위해 2 단계 인증이라는 기술도 널리 사용되고 있습니다. 2 단계 인증이란 웹 서비스나 애플리케이션에 로그인할 때 로그인 ID 나 비밀번호로 인증한 후 추가로 별도의 인증 절차를 거치는 보안 대책을 말합니다.
ID 와 비밀번호만으로 인증하는 경우 비밀번호 유출 등이 발생하면 무단 접근을 허용하게 되지만, 2 단계 인증을 사용하면 스마트폰 등을 소지해야 하므로 보안 강도가 한층 높다고 볼 수 있습니다.

제 2 장 인터넷의 기본적인 주의점

2-1 소셜 미디어(SNS)의 이용

1. 소셜 미디어 이용 시 주의사항

소셜 미디어는 인터넷상의 소통 수단으로 폭발적으로 보급되었습니다. 손쉽게 정보를 발신할 수 있는 반면, 배려 없는 경솔한 발언이 타인에게 상처를 주거나 범죄로 이어질 수 있습니다. 글을 올리기 전에 다음 사항에 충분히 유의하십시오.

・타인의 발언을 인용할 때는 정확하게
・비방 중상이나 음란한 발언, 사생활을 침해하는 발언을 하지 않는다
・차별 발언을 하지 않는다
・발언하는 정보의 내용에 주의한다
・사진 게시 시 주의한다
・과격한 행위를 촬영하지 않는다
・고객 테러(손님이 가게에 끼치는 폭언· 행패 등)와 같은 행위는 업무 방해에 해당한다
・개인정보나 사생활 관련 정보를 기재하지 마십시오

・폭발, 살인 등의 범행 예고를 기재하지 마십시오
・불필요한 해시태그는 사용하지 마십시오
・그룹 대화방에서는 개인적인 메시지를 보내지 마십시오
・게시판에 발언할 때는 운영 방침이나 규칙을 확인하고, 게시판 주제와 무관한 글은 자제하십시오
・선거 관련 게시물에 주의하십시오

필터 버블(Filter Bubbles)

인터넷상의 각종 서비스에서는 열람 이력 추적(트래킹)과 취향 맞춤 검색 결과 표시(필터링)를 통해 사용자가 관심을 가질 만한 정보를 선별·제공하는 시스템이 사용되고 있습니다. 이로 인해 웹 페이지 검색 기록 등을 통해 사용자의 취향에 맞는 콘텐츠만 예측·표시되어 접하는 정보가 자신의 취향에 맞는 것으로만 한정되는 현상을 필터 버블이라고 합니다.

이처럼 인터넷에서는 자주 보는 콘텐츠나 선호하는 콘텐츠가 우선 표시되는 구조가 있다는 점을 기억해 두십시오.

에코 챔버(Echo Chamber)

SNS 나 인터넷 게시판 등에서 자신과 비슷한 가치관을 가진 사용자들끼리만 교류하면, 점차 비슷한 의견만 접하게 됩니다.
이 현상을 비슷한 의견만 메아리처럼 되돌아오는 닫힌 공간이라는 의미로 에코 챔버라고 합니다.
닫힌 네트워크 공간에서는 자신과 비슷한 의견에 둘러싸여 자신의 사고방식이 더욱 편향되고 강화되기 쉽다는 점에 주의해야 합니다.

2. 정보의 진위를 가려내다

예를 들어, 웹사이트에 "A 사 주가가 오른다"는 글을 본 것만으로 즉시 그 주식을 구매하는 것은 미디어 리터러시 관점에서 바람직한 행동이라 할 수 없습니다. 웹사이트라는 매체의 익명성 등의 특징을 고려하여 허위 정보가 아닌지 확인할 필요가 있습니다.

가짜 정보·잘못된 정보와 허위 정보의 확산

사실과 다른 거짓 정보나 잘못된 정보를 허위 정보(페이크 뉴스)라고 합니다.
단순히 조회 수를 늘려 주목받으려는 목적이나, 비방과 중상을 목적으로 한 게시물이 있습니다. 그중에는 정치나 선거를 유리하게 이끌기 위해 악용하는 사례도 있습니다.
이러한 거짓 정보에 현혹되지 않도록 적절히 대처하려면 정보의 진위를 판별하는 리터러시가 중요합니다.

또한 지진이 발생한 직후, "동물원에서 동물이 탈출했다", "쇼핑몰에서 화재가 발생했다" 등 혼란을 틈탄 허위 정보가 퍼지기도 합니다.
이러한 정보는 널리 확산될 수 있지만, 사실을 확인하고 근거를 파악한 뒤 신중하게 대응해야 합니다.
2021 년에는 난폭운전 가해자와 무관한 일반 여성을 '피처폰 여자'로 지칭하며 사건과 관련이 있다는 허위 정보를 유포한 유튜버가 고소당했습니다. 허위 정보 유포로 인해 피해 여성에게 대량의 괴롭힘 전화와 비방·중상 게시물이 이어졌습니다. 피해를 입은 여성은 명예를 훼손당했다며 배상 청구를 하고 있습니다.
이러한 허위 정보는 사람을 상처 입히고 몰아붙여 평범한 일상마저 빼앗아 버립니다. 허위 정보 유포자가 되면 법적 책임을 져야 합니다. 따라서 무책임하게 근거 없는 정보를 유포하지 않도록 주의합시다.

딥페이크(Deep Fake)

인공지능 기술을 이용해 만들어지는 가짜 동영상입니다. 고도의 이미지 인식·합성 기술을 활용하기 때문에 진위 여부를 구분하기 어려워지고 있습니다.
예를 들어, 특정 정치인의 영상을 다른 사람의 영상과 합성함으로써 마치 그 정치인이 발언하는 것처럼 보이는 허위 정보에 악용될 수 있습니다.
인공지능 연구 성과 중 하나인 딥러닝(Deep Learning: 심층 학습)이라는 알고리즘이 사용되기 때문에 이렇게 불립니다.

인플루언서(Influencer)

인터넷에서 사용자의 구매 행동에 강한 영향력을 가진 사람을 인플루언서(Influencer)라고 합니다. 특히 SNS 에서 많은 팔로워를 보유한 유명 블로거(Blogger)나 유튜버(YouTuber), 인스타그래머(Instagrammer), 틱톡커(TikToker) 등이 인플루언서에 해당합니다.

인플루언서에게 은밀히 의뢰하고 대가를 지급하여 자사 상품 홍보 활동을 하는 것을 스텔스 마케팅(Stealth Marketing)이라고 합니다. 일반 소비자가 스텔스 마케팅에 부추겨지거나 속아서 상품을 구매하는 경우가 있습니다.
따라서 인플루언서의 정보만 무조건 믿지 말고, 직접 여러 정보를 수집하여 확인해야 합니다.

생성형 AI

채팅이나 음성으로 입력한 질문에 대해 AI 가 글이나 이미지·동영상 등을 자동으로 생성하는 서비스입니다. ChatGPT 나 Copilot(구 Bing Chat), Gemini(구 Google Bard) 등의 서비스가 있습니다. ChatGPT 의 GPT 는 Generative Pre-trained Transformer 의 약자로, 일상 언어로 AI 와 대화할 수 있는 시스템입니다. 다양한 언어를 지원하며

한국어와 일본어도 이용할 수 있습니다. 사용자가 입력한 질문이나 이미지에 대해 마치 사람과 같은 자연스러운 응답이나 이미지를 생성하여 활용 범위가 넓어지고 있습니다.

그러나 생성 결과가 반드시 정확하다고 할 수 없습니다. 또한 생성된 내용이 저작권 침해에 해당할 수도 있으므로 사용 시 주의해야 합니다.

2-2 온라인 게임

1. 과금에 주의하며 사용하십시오

온라인 게임은 인터넷을 통해 동시에 많은 사용자가 참여할 수 있습니다. 대전하거나 함께 적을 물리치는 등 흥미로운 콘텐츠가 많습니다.

하지만 게임에서 아이템을 획득하기 위해 과금이 필요한 경우도 있습니다. 게임에 빠져 과도한 금액을 지출하지 않도록 주의하세요.

또한, 플레이 시간도 스스로 철저히 관리해야 합니다. 밤낮이 뒤바뀐 생활은 생활 리듬을 무너뜨려 건강과 학업에 악영향을 미칩니다.

2. 온라인 게임 상의 사기

온라인 게임 내 채팅을 악용해 이용자를 사기 사이트로 유인하여 개인정보를 무단 취득하는 피싱 사기가 있습니다. 또한 악성코드나 부정 앱을 설치하도록 유도하는 수법도 있습니다.

"등록하면 게임 내에서 쇼핑할 수 있는 화폐를 드립니다", "캐릭터를 강화하는 아이템을 선물합니다", "희귀한 무기를 거래합시다" 등 악의적인 사용자는 교묘한 말로 속이려 하기 때문에 채팅에서 지나치게 좋은 조건을 제시하는 말에는 경계하십시오.

3. 게임 실황

게임 플레이 영상에 실시간 해설을 곁들인 동영상을 게시하는 행위입니다. 그러나 게임에는 저작권이 있으므로 제작사 등의 허락 없이 게시하면 원칙적으로 저작권법에 위반됩니다.

실황 동영상에 대해서는 일정한 가이드라인을 준수하면 게임사가 실황 동영상 게시를 허용하는 경우가 있습니다. (엔딩 장면은 업로드하지 않는 등 일정한 기준을 두고 있습니다.)

2023 년 9 월, 게임의 전체 줄거리를 파악할 수 있는 실황 동영상을 무단 공개하여 수익을 얻은 자가 유죄 판결을 받았습니다. 업로드된 동영상에는 게임의 시작부터 결말까지 모두 포함되어 있었습니다.

게임 실황을 동영상 사이트에 업로드할 경우, 저작권에 충분히 유의하고 어디까지 게시가 허용되는지 확인해야 합니다.

2-3 IT 의 악용

3D 프린터

3D 프린터나 레이저 커터는 설계도에서 3 차원 입체물을 만들어낼 수 있습니다. 그러나 입체물을 만들 수 있다고 해서 아무것이나 만들면 불법이 될 수 있습니다. 설계도를 입수할 수 있더라도 다음과 같은 물품은 절대 제작하지 마십시오.

・총포류(살상능력이 있는 무기)
・모조품(브랜드 제품 등)
・위조화폐
・음란물

IoT 의 문제

지금까지 인터넷은 주로 컴퓨터나 서버 등 IT 기기끼리 연결되어 왔습니다.
최근에는 TV, 디지털 카메라, 에어컨, 스피커, 자동차 등 모든 '사물'이 인터넷에 연결되고 있습니다. 이처럼 지금까지 인터넷에 연결되지 않던 사물까지 연결하는 것을 'IoT(Internet of Things)'라고 합니다. IoT 는 '사물의 인터넷'으로 번역됩니다.

사물을 원격으로 제어할 수 있고, 사물을 통해 정보를 수집할 수 있으며, 사물끼리 대화할 수 있는 등 많은 장점이 있지만, 동시에 보안 위험도 수반합니다. 예를 들어 다음과 같은 문제점이 지적되고 있습니다.

・한 기기에 결함이 있으면 시스템 전체가 취약해진다.
・IoT 기술 자체도 매일 진화하고 있기 때문에 오래된 기기는 시간이 지남에 따라 안전성이 저하된다.
・다른 분야의 기기나 서비스끼리 연결되기 때문에 상호 간의 신뢰성을 보장하기 어렵다.
・개별 사용자가 제조사의 의도와 다른 방식으로 연결·사용하는 경우가 있다.

이러한 상황 속에서 실제로 다음과 같은 사건이 발생하고 있습니다.

・감시 카메라 영상이 해킹되어 유출된다.
・실험 장비가 해킹되어 위험한 상태에 빠진다.
・가전제품이 악성코드에 감염되어 DDoS 공격에 동원된다. (IoT 악성코드)

따라서 각 기기의 취약점을 충분히 점검한 후 인터넷에 연결해야 합니다. 각 기기에는 소프트웨어(펌웨어)가 내장되어 있으므로 보안 취약점이 발견되면 즉시 보안 패치를 적용하십시오.

또한 IoT 기기의 취약한 초기 비밀번호를 그대로 사용하지 않도록 사용 개시 전에 반드시 변경해야 합니다.

한편, IoT 기기는 무선(Over The Air)으로 초기화나 업데이트를 수행하는 경우가 많아 통신이 도청되어 기기가 장악당하는 사례가 있습니다. 따라서 무선 LAN 통신이 암호화되어 있는지 확인하십시오.

제 3 장 인터넷상의 커뮤니케이션

3-1 이메일로 인한 피해

이메일은 간편하고 편리하지만, 다음과 같은 피해를 입을 수 있습니다.

1. 이메일로 인한 문제

사칭

이메일은 다른 사람을 사칭하여 메일을 보낼 수 있습니다. 의심스러운 내용의 메일을 수신했을 때는 답장하지 말고 직접 전화 등으로 본인에게 확인하거나, 경우에 따라서는 시스템 관리자에게 상담해야 합니다.

한 대학생의 ID 와 비밀번호를 도용해 그 대학생으로 사칭한 뒤, 취업이 내정된 기업의 담당자에게 내정 사퇴 이메일을 보낸 대학생이 체포된 사건도 있었습니다. 이러한 사태를 막기 위해 ID 와 비밀번호 관리에 주의해야 합니다.

이메일 사기

최근에는 '환경 보호'나 '아동 복지' 등을 명목으로 한 이메일을 보내 돈을 사취하는 사례도 있습니다. 기부할 때는 반드시 신뢰할 수 있는 단체를 통해 진행하십시오.

스팸 메일(Spam Mail)

사전에 수신자의 허락 없이 무차별적으로 대량 발송되는 메일을 스팸 메일이라고 합니다(스팸 메일 또는 정크 메일이라고도 함). 스팸 메일은 주로 광고성 메일이지만, 사기를 목적으로 하는 경우도 있습니다. 스팸 메일은 네트워크 회선에 부하를 주는 동시에 수신자 측에 통신비를 발생시키기 때문에 불법 행위로 큰 문제가 되고 있습니다. 영리 목적의 다이렉트 메일을 수신자의 동의 없이 발송하는 행위는 위법입니다.

스팸 행위는 SNS 에서도 만연하고 있습니다. 불특정 다수 사용자에게 홍보 메시지를 발송합니다. 악성 스팸 행위를 반복하는 계정을 발견하면 관리자에게 신고하여 이용을 정지시킵시다.

3-2 커뮤니케이션 시 주의사항

1. SNS 에서의 피해

최근에는 만남 사이트에 대한 규제가 강화되면서 SNS 를 만남 사이트 대용으로 이용하는 사례가 있습니다. 그러나 게시물의 내용에 따라 처벌 대상이 될 수 있습니다.

또한 가출한 아동이 피해를 입고 있는 '가출 게시판'도 문제가 되고 있습니다. 소지금이 적은 아동이 숙소를 구하기 위해 상대를 찾는 이러한 게시판은 아동에게 위험이 도사리는 만남의 장이며, 실제로 아동 매춘이나 폭행 등의 범죄로 이어진 사례가 다수 발생하고 있습니다.

이러한 게시판을 발견하면 경찰 등 관련 기관에 신고하여 단속에 협조합시다.

스토킹 행위

일방적으로 호감을 가진 상대, 연애 관계에 있던 상대, 전 배우자 등을 끈질기게 따라다니는 행위는 스토킹으로 「스토킹 행위 등의 규제 등에 관한 법률」(통칭: 「스토킹 규제법」)에서 금지하고 있습니다.

이 법률에서는 실제로 매복하거나 상대방 근처를 배회하는 등의 행위뿐만 아니라, 거부했는데도 계속 메일을 보내는 행위나 X(구 트위터) 등의 SNS 에 끈질기게 글을 올리는 행위도 '반복적 접근 등'으로 금지하고 있습니다. 2021 년에는 본인의 동의 없이 GPS 로 위치 정보를 파악하는 행위나, 거부했는데도 계속 문서를 보내는 행위도 규제 대상에 추가되었습니다.

그루밍

성적 학대를 목적으로 하는 자가 아동에게 접근하여 교묘한 말솜씨로 신뢰를 쌓아 심리적 거리를 좁혀가는 행위입니다.

최근에는 SNS 를 이용한 그루밍(온라인 그루밍)이 문제가 되고 있습니다. 아이인 척하며 편하게 대화할 수 있는 상대라고 생각하게 하거나, 상대의 취미·기호를 파악하여 관심을 끌 만한 정보를 제공하며 친밀감을 쌓으려 합니다. 그 결과, 사이버 스토킹으로 이어지거나 직접 만남을 유도하여 성적 학대까지 발전하기도 합니다.

피해를 방지하기 위해서는 먼저 SNS 에서 알게 된 사람과 가볍게 만나지 않는 것이 중요합니다. 또한 직접 만날 경우에는 충분히 경계하고, 성적 관계를 요구받으면 단호하게 거절해야 합니다.

특정업자

SNS 에 게시된 사진이나 동영상을 단서로 본인의 주소·성명 등 개인정보를 알아내는 사람(또는 그룹)을 특정업자(특정반)라고 합니다. 개인정보를 알아내는 대가로

의뢰인으로부터 보수를 받고 활동하는 경우도 있습니다.

이러한 신상 특정 행위나 의뢰가 스토커에게 악용되는 사례가 있습니다. 따라서 개인정보를 추적할 수 있는 사진이나 동영상을 함부로 SNS 에 게시하지 마십시오.

인물 사진을 업로드한 후, 눈동자에 반사된 풍경으로 위치가 특정된 사례, 창밖 풍경으로 위치가 특정된 사례, 혹은 요리 사진을 올렸을 때 얼굴이 숟가락에 반사되어 신원이 특정된 사례 등도 있습니다.

사인체포 계열 유튜버

눈앞에서 범죄가 발생한 경우, 일반인이 현행범을 체포하는 것은 형사소송법 제 213 조에서 인정되고 있지만, 이것이 허용 요건이 매우 엄격하므로 함부로 시도해서는 안 됩니다. 그러나 범인이 아닌 사람을 범인으로 단정 짓고 체포한 뒤 영상을 촬영하여 올리는 '사인체포형' 유튜버가 문제가 되고 있습니다. 애초에 조회 수 확보를 위해 범죄·체포 장면을 촬영하려는 행위 자체가 위험합니다.

2. 매칭 앱

매칭 앱은 비교적 최근에 등장한 서비스입니다. 인터넷 상에서 사용자들을 연결해주는 앱이라는 점에서, 만남 사이트와 비슷한 목적으로 이용되기도 합니다.

매칭 앱에서는 가입 시 운전면허증이나 여권 등을 통한 연령 확인 절차가 진행됩니다. 또한 본인임을 확인하기 위해 페이스북 계정 연동이나 전화번호 인증 등을 의무화하는 앱도 있습니다. 만남 사이트에는 없는 사용자 인증 절차가 있지만, 알게 된 상대와 실제로 만나면서 문제가 발생할 수 있습니다. 한편, 「만남 사이트 규제법」(정식 명칭: 「인터넷 이성 소개 사업을 이용하여 아동을 유인하는 행위의 규제 등에 관한 법률」)에서는 18 세 미만자를 「아동」으로 정의한 데 이어(제 2 조 제 1 호), 사업자, 보호자, 국가·지방공공단체에 대해 아동이 매칭 앱 등에서 인터넷 이성 소개 사업을 이용하지 않도록 방지해야 한다고 규정하면서(제 3 조~제 5 조), 특히 사업자에 대해서는 아동이 아님을 확인할 의무와 아동의 건전한 육성에 지장을 주는 행위를 방지할 의무를 부과하고 있습니다(제 11 조, 제 12 조).

3. 가짜 SNS 계정

학교 등 법인의 공식 인스타그램 가짜 계정이 문제가 되고 있습니다. 법인을 사칭한 계정을 만들어, 실수로 속아 팔로우한 상대에게 거짓 메시지를 전송합니다.

SNS 를 홍보 활동이나 연락용으로 이용하는 학교가 늘고 있으므로, 인스타그램 외에도 X(구 트위터) 등의 가짜 계정에 주의하고, 진짜 공식 계정인지 가려내야 합니다.

3-3 유해한 정보

1. 범죄를 조장하는 사이트

웹사이트에는 살인 등의 범죄를 청부 받는 사이트가 존재하며, 경찰청이 단속을 진행하고 있습니다.

이러한 사이트는 청부를 받는 척하며 대금을 사취하는 사기 목적인 경우도 있고, 실제로 범죄를 의뢰받아 피해자를 발생시키는 경우도 있습니다. 범죄 조직이 마약 밀매나 부정 계좌 거래에 이용하는 경우도 있습니다.

어떤 경우든 범죄에 연루되거나 자신이 형사 처벌을 받을 수 있는 매우 위험한 사이트입니다. 이러한 사이트에는 절대 연락하지 마십시오.

불법 아르바이트

SNS 를 이용한 고액 임금 아르바이트 모집이 있습니다. 단시간에 큰돈을 벌 수 있다고 내세워 불법 행위를 시키는 이른바 '불법 아르바이트(야미바이토)'입니다. 예를 들어 "가방을 전달해 달라"는 의뢰를 받았는데, 실제로 그 내용물이 불법 약물이었다는 등 본인이 범죄에 가담하고 있다는 사실을 깨닫지 못하는 경우도 있습니다.

최근에는 범죄 조직의 불법 자금(불법 접속이나 송금 사기 등으로 얻은 자금)을 해외로 송금하는 아르바이트 '머니뮬'이 문제가 되고 있습니다. 뮬(Mule)은 노새를 의미합니다. 범죄 조직과 직접 관련 없는 아르바이트생에게 송금을 대행하게 하여 불법 자금의 운반책으로 이용합니다. 본인은 범죄라는 자각 없이 단순히 송금 절차만 했을 뿐이지만, 어느새 자금 세탁(머니 로더링: 자금의 출처를 은폐하는 행위)에 가담한 것이 되어 처벌받을 수 있습니다.

그 외에도 보이스피싱(일본의 오레오레 사기) 등에서 현금을 받는 '수취인' 역할을 시키는 사례도 있습니다.

간단한 일로 큰돈을 벌 수 있는 경우는 거의 없으니, 이런 수상한 아르바이트에 응하지 마십시오.

학생증이나 운전면허증 등의 사본을 보내달라고 요구받아 개인정보를 빼앗길 수 있습니다. 거절하려 해도 범죄 가담을 강요당하는 경우도 있습니다. 함부로 개인정보를 제공하지 않도록 주의하는 동시에, 개인정보 악용 자체가 범죄이므로 범죄 가담을 강요당할 것 같으면 즉시 경찰에 상담하십시오.

3-4 괴롭힘과 협박 행위

1. 사이버 괴롭힘

인터넷상의 블로그나 게시판 등에서 개인이나 집단에 대해 비방과 중상을 가하는 행위입니다. 사이버 괴롭힘은 가해자가 매우 많거나 익명인 경우가 대부분입니다. 또한 개인정보 유출이나 사생활 침해로 이어질 우려도 있습니다. 항상 상대방의 입장을 배려하는 발언을 합시다.

최근에는 소셜 미디어에서 따돌리는 형태의 괴롭힘도 있습니다.

또한 '학교 뒷사이트'라 불리는 특정 학교의 주제를 다루는 비공식 게시판이 존재하여, 괴롭힘과 비방 문제를 더욱 심화시키고 있습니다. 이러한 사이트는 발견하기 어렵지만, 발견하면 학교 선생님 등에게 알려 피해를 최소화합시다.

2. 리벤지 포르노(Revenge Porn)

헤어진 배우자나 교제 상대방의 사적인 성적 사진이나 영상을 인터넷에 유포하는 복수 행위입니다. 스마트폰 보급으로 사진이나 동영상을 손쉽게 촬영할 수 있게 되면서, 괴롭힘 수단으로 리벤지 포르노가 심각해지고 있습니다. 한번 인터넷에 확산되면, 해당 데이터를 인터넷에서 완전히 삭제하는 것은 현실적으로 거의 불가능합니다. "음란한 사진을 인터넷에 올린다"고 협박당한 사례도 있습니다.

이러한 피해를 입지 않기 위해, 교제 상대라 하더라도 경솔하게 성적인 사진을 찍히지 말고, "보내달라"고 부탁받아도 보내지 않도록 주의하십시오.

한편, 「리벤지 포르노 방지법」(정식 명칭: 「사적 성적 영상 기록의 제공 등에 의한 피해 방지 관련 법률」)에 따라 사적으로 촬영한 성적 영상을 인터넷에 공개할 경우, 3 년 이하의 징역형 또는 50 만 엔 이하의 벌금이 부과됩니다.

3. 촬영죄(성적 자세 등 촬영죄)

2023 년에 성적 자세 촬영 등 처벌법(성적 자세를 촬영하는 행위 등의 처벌 및 압수물에 기록된 성적 자세의 영상에 관한 전자적 기록의 삭제 등에 관한 법률)이 제정되었습니다. 아동 포르노나 리벤지 포르노의 원인 중 하나가 되는 도촬이나 불법 촬영 행위에 대한 규제를 강화하기 위한 법률입니다. 이 법률에서 촬영죄(성적 자세 등 촬영죄)가 규정되었습니다. 몰래 촬영 단속에 관한 법률은 이전에도 있었지만, 몰래 촬영이나 불법 촬영 행위의 처벌 범위가 확대되었습니다.

성적 자세 등 촬영죄는 3 년 이하의 징역 또는 300 만 엔 이하의 벌금이 부과됩니다.

촬영 행위 그 자체뿐만 아니라, 그 촬영 데이터의 제공·보관도 처벌 대상이 됩니다.

제 4 장 인터넷 거래

4-1 피싱 사기

1. 피싱(Phishing)

피싱이란 정상적인 이메일이나 웹사이트로 위장하여 비밀번호나 신용카드 번호를 훔쳐내는 사기를 말합니다. 웹 페이지 자체는 쉽게 복제할 수 있기 때문에, 위장 웹사이트를 진짜로 믿은 사람이 개인정보를 넘겨주는 피해가 잇따랐습니다.

주요 수법은 금융기관, 신용카드사, 통신판매업체, 티켓 판매업체 등을 사칭한 이메일을 무차별로 발송한 뒤, 이메일 본문에 기재된 URL 을 통해 금융기관, 이동통신사, 통신판매업체 등의 가짜 사이트로 유도하여 개인정보를 입력하게 하는 것입니다.

최근에는 이메일 대신 SMS(Short Message Service)가 악용되기도 합니다. 이를 '스미싱'(Smishing) 또는 'SMS 피싱'(SMS Phishing)이라고 합니다. 택배 업체 등의 부재 통지를 가장하여 "물품 배송을 위해 방문했으나 부재 중이어서 반송했습니다. 아래 URL 에서 확인해 주세요"와 같은 메시지를 보내 피싱 사이트로 유도하는 수법이 있습니다. 그중에는 악성 앱을 설치하도록 유도하는 경우도 있습니다.
2020 년에는 스마트폰 캘린더에 자신도 모르게 일정이 등록되고, 표시된 URL 을 탭하면 피싱 사이트로 유도되는 수법도 등장했습니다.

이메일 발신자 명의를 쉽게 믿지 말고, 웹사이트 URL 이 정상적인지 확인하세요. 또한 SSL/TLS 등으로 암호화되어 있는지도 확인하십시오.
피싱을 더욱 교묘하게 발전시킨 파밍(Pharming)이라는 수법도 있습니다.

보이스 피싱(Voice Phishing)

피싱과 유사한 사기로, 미끼 이메일로 전화 음성 안내에 접속하도록 유도하여 개인정보를 사취하는 수법을 말합니다. 비싱(Vishing: Voice Phishing)으로 약칭됩니다.

피싱이 위장 사이트의 URL 을 클릭하게 하여 유도한 사이트에서 개인정보를 입력하게 하는 반면, 비싱은 이메일에 전화번호를 기재하여 전화를 걸게 한 뒤 자동 음성 응답 시스템(ARS)을 통해 개인정보를 사취합니다.

이러한 사기에 당하지 않으려면, 이메일에 적힌 전화번호를 무조건 믿지 말고, 공식 사이트 등에서 확인하는 것이 중요합니다.

최근 AI 를 이용한 범죄 수법으로 '음성 딥페이크'가 있습니다. AI 로 고품질의 음성을 생성해 누군가를 사칭하여 사기 전화를 걸고, 위조 사이트로 유도합니다. 아는 사람의 목소리처럼 들리더라도 사기일 가능성을 의심하고, 수상한 요청에 응하지 않도록 주의해야 합니다. 특히 돈 이야기가 나오거나 금융 기관에서 걸려온 전화는 일단 전화를 끊고 공식 번호를 확인하십시오.

4-2 원클릭 사기

1. 원클릭 사기

대금을 편취하는 수법 중 하나로 원클릭 사기가 있습니다. 특정 사이트에서 버튼을 클릭하자마자 갑자기 회비 등의 요금 청구 화면이 나타납니다.

또한, 이메일에 기재된 URL 을 클릭해도 마찬가지로 갑자기 요금을 청구받는 경우가 있습니다.

화면에 "회원 가입이 완료되었습니다", "회비를 아래 계좌로 입금해 주십시오", "1 주일 이내에 절차를 완료하지 않을 경우 법적 조치를 취하겠습니다" 등의 메시지가 표시됩니다.

어떤 경우에는 "귀하의 정보를 읽어냈습니다"라는 메시지와 함께 컴퓨터의 IP 주소나 브라우저 정보 등을 표시하여 마치 개인정보를 취득한 것처럼 보이게 하는 패턴도

있습니다.

그러나 계약이 성립되기 위해서는 사전에 어떤 절차(이용 신청 등)가 이루어져야 합니다. 따라서 이처럼 사이트 운영자로부터 요금 청구가 있어도 대금을 지불할 필요가 없습니다. 이용 약관 표시가 불분명하거나 사이트 설계 자체에도 문제가 있습니다. 이는 「특정 상거래법」에서 정하는 「고객의 의사에 반하여 계약 신청을 하도록 하는 행위」에 해당합니다. 이 법률 및 동법 시행 규칙은 소비자가 혼동하기 쉬운 표시나 버튼 배치를 금지하고 있습니다.

스마트폰 원클릭 사기

PC 사이트에서의 원클릭 사기뿐만 아니라 스마트폰용 사이트에서도 원클릭 사기가 존재합니다. 예전에는 이메일을 이용한 사기가 주류였지만, 최근에는 SNS 에 관심을 끄는 메시지를 게시하여 사기 사이트로 유도하는 수법이 늘고 있습니다. 메시지 안에 적힌 URL 을 탭하면 갑자기 "회원 가입이 완료되었습니다. 이용 요금 10 만 엔을 송금해 주세요"와 같은 청구 화면이 표시됩니다(원클릭 사기라기보다 '원탭 사기'라 해야 할 것입니다).

휴대 단말기의 IP 주소나 기종 정보 등을 제시하며 마치 사용자의 신원을 특정할 수 있는 듯 보여 불안감을 조성하여 대금을 송금하도록 유도하는 수법입니다. 거듭 말씀드리지만, IP 주소나 기종 정보만으로는 개인을 특정할 수 없습니다.

2. 스마트폰 사기 앱

성인 사이트 등에서 동영상을 보려고 하면 전용 재생 앱을 다운로드하도록 유도되며, 설치하면 허위 청구 화면이 반복적으로 표시되어 대금을 편취당하는 사기가 성행하고 있습니다. 이러한 수상한 앱뿐만 아니라, 겉보기에 유용해 보이는 이미지 편집 앱 등으로 위장하는 경우도 있으므로 주의가 필요합니다.

사기 앱을 한 번 설치하면 요금 청구 화면을 닫아도 일정 시간이 지나면 반복적으로 청구 화면이 표시됩니다.

또한 설치 시 사기 앱에 의해 주소록이 유출될 가능성도 있습니다. 안드로이드 기기의 경우 설치 시 '접근 권한' 항목에 표시되는 내용을 반드시 확인하세요. 범인에게 개인정보가 넘어가면 SMS 등을 통한 협박 메시지가 올 수도 있습니다.

4-3 인터넷 쇼핑

1. 인터넷 쇼핑 관련 문제점

인터넷 쇼핑이 보편화되면서 이에 따른 문제도 늘어나는 추세입니다.

주요 문제점

인터넷 쇼핑과 관련하여 다음과 같은 다양한 문제가 발생하고 있습니다.

상품을 주문하고 대금을 선불했는데 상품이 배송되지 않는다.
도착한 상품이 주문한 것과 달랐다. 또는 가짜(위조품)였다.
주문한 기억이 없는 상품의 대금을 청구받았다(예를 들어, 신용카드 정보 등이 유출되었다).
판매자와 연락이 되지 않고 웹사이트도 사라졌다.
문의해도 제대로 대응하지 않는다.
또한, 인터넷 경매에서의 개인 간 거래에서도 유사한 문제가 발생하고 있습니다. 개인 간 거래에서는 상대방을 특정하기 어려워 구매자가 피해를 감수하는 경우가 많습니다.

2. 스텔스 마케팅(Stealth Marketing)

일반 소비자에게 광고임을 알리지 않고 진행하는 홍보 활동입니다. '스테마'로 줄여 부르기도 합니다.
일반 정보 제공자인 척하며, 입소문 형태로 소셜 미디어에 특정 기업의 상품을 홍보하는 글을 올립니다. 이른바 '바이럴 마케팅(사쿠라)'이라 불리는 수법입니다. 이러한 허위 후기를 이용한 스텔스 마케팅은 위법 행위가 될 수 있습니다.

또한 인스타그램 등의 SNS 에서 특정 상품에 대해 '좋아요'를 대량으로 눌러주고 수익을 얻는 '클릭 대행 사업'이나 팔로워 수를 인위적으로 늘려주는 업체도 있습니다. 이러한 허위 후기나 조작된 평가에 속지 않도록 주의해야 합니다. 스텔스 마케팅에서는 '좋아요' 수나 팔로워 수가 부자연스럽게 늘어나므로 진위를 판별해야 합니다.

5-1 컴퓨터 바이러스

1. 컴퓨터 바이러스란

「컴퓨터 바이러스」란 컴퓨터 시스템에 해를 끼치기 위해 만들어진 컴퓨터 프로그램을 말합니다.
컴퓨터 입장에서는 Word 나 Excel 등의 소프트웨어와 같은 「프로그램」입니다. 마치 인플루엔자 바이러스처럼 자신도 모르는 사이에 컴퓨터 내부로 침투해 장애를 일으키거나, 이메일 등을 통해 다른 컴퓨터로 침투하는(감염하는) 모습에서 컴퓨터 바이러스라고 불립니다.

스마트폰도 PC 와 마찬가지로 애플리케이션을 자유롭게 추가할 수 있는 반면, 해당 소프트웨어에 컴퓨터 바이러스가 숨어 있을 가능성이 있습니다.
또한 악의적인 프로그램을 총칭하여 멀웨어(Malware)라고 합니다.

2. 바이러스의 감염 경로
바이러스의 감염 경로는 주로 다음 4 가지입니다. 이 외에도 USB 장치에 내장된 바이러스에 감염된 사례도 있습니다.

이메일　　첨부 파일을 열어 감염됨
웹 페이지　　다운로드한 파일을 실행하거나, 스크립트나 ActiveX 등을 악용한 웹 페이지를 열람하여 감염될 수도 있음
파일 공유　　파일 공유 소프트웨어의 공유 폴더에 감염 파일이 복사되어 감염됨
기록 매체　　바이러스에 감염된 CD, DVD, USB 메모리 등을 통해 감염됨

인터넷을 통해 바이러스는 순식간에 확산되어 피해 규모가 막대해집니다. 외부에서 받은 파일을 열기 전에는 반드시 바이러스 검사를 실시해야 합니다. 또한 브라우저의 경고 메시지에 주의하고, 의심스러운 사이트 열람은 즉시 중단하세요.

지원 사기
사용자의 컴퓨터에 "바이러스에 감염되었습니다"와 같은 가짜 메시지를 표시하고, 공식 업체의 기술 지원을 가장하여 지정된 전화번호로 전화를 걸게 하는 등 지원 비용을 편취하는 수법입니다.
컴퓨터 브라우저에 반복적으로 가짜 경고를 표시해 브라우저를 조작 불가능하게 만들고, 존재하지 않는 가짜 지원 사이트로 유도하는 사례도 있습니다.
"바이러스에 감염되었습니다" 같은 메시지가 표시되어도 당황하지 말고 해당 경고를 무시하십시오.
또한 익숙하지 않은 메시지가 반복적으로 표시될 경우, 정식으로 구입한 백신 소프트웨어로 감염 여부를 확인하십시오.

3. 감염되었다고 생각되면
컴퓨터 바이러스에 감염된 경우 다음 조치를 취하십시오.

- 즉시 네트워크에서 분리합니다.
- 해당 컴퓨터 사용을 중단합니다.
- 시스템 관리자에게 보고합니다.
- 바이러스 백신 소프트웨어로 복구를 시도합니다.
  (정상 컴퓨터에서 바이러스 백신 소프트웨어 개발사 사이트에 접속해 제거 프로그램을 다운로드합니다. 제거 프로그램을 CD 등에 복사한 후 감염된 컴퓨터에서 실행해 복구를 시도합니다.)

바이러스 백신 소프트웨어로 복구할 수 없는 경우, 감염된 시스템을 삭제하고 깨끗한 시스템을 재설치해야 합니다.

4. 컴퓨터 바이러스 대책

・바이러스 검사를 실시한다
・소프트웨어 제조사가 제공하는 최신 버전의 소프트웨어를 사용한다
・출처가 불분명한 소프트웨어는 사용하지 않는다
・지인으로부터 받은 이메일도 첨부 파일은 바이러스 검사를 실시한다
・파일 확장자를 표시하도록 설정한다
・Office 매크로 실행을 금지하도록 설정한다
・스마트폰 바이러스 대책

PC 와 마찬가지로 바이러스 백신 소프트웨어 설치 및 신뢰할 수 있는 출처의 애플리케이션만 다운로드하는 것이 효과적인 대책입니다. 신뢰할 수 없는 출처의 앱은 바이러스 등이 포함될 가능성이 있으므로 사용을 자제하는 것이 현명합니다.

또한 앱을 설치할 때도 다른 사용자의 리뷰 확인을 소홀히 하지 말고 신중하게 판단하도록 합시다.

5-2 시스템 업데이트

1. 보안 취약점에 대한 업데이트 작업

OS 나 브라우저 등의 애플리케이션에서 보안 취약점이 발견될 수 있습니다. 보안 취약점이란 소프트웨어 개발사나 사용자의 의도와 관계없이 네트워크를 통한 침입을 허용하는 결함을 말합니다. 이 취약점이 악용되면 컴퓨터나 네트워크에 무단 침입당하거나 정보가 유출될 위험이 있습니다.

소프트웨어 제조사는 보안 취약점을 발견하면 즉시 '보안 패치'(결함을 수정하는 프로그램)를 개발하여 배포합니다.

개인 소유의 컴퓨터는 본인이 직접 관리해야 합니다. 보안 취약점 관련 뉴스에 평소 관심을 기울이고, 취약점이 발견되면 신속히 보안 패치를 다운로드하여 업데이트를 수행하세요.

Windows 의 경우 보안 패치나 업데이트 프로그램을 자동으로 수신하도록 설정할 수 있습니다. 또한 Windows Update 를 통해 최신 정보를 얻고 업데이트 작업을 수행할 수 있습니다.

브라우저는 웹사이트 열람에 필수적이지만, 심각한 취약점이 발견되기도 합니다. 보안 패치가 배포되기 전까지 해당 브라우저를 사용해서는 안 됩니다. 따라서 평소에 여러 종류의 브라우저를 설치해 두시기 바랍니다.

2. 지원이 종료된 OS 등에 관하여

2020 년 1 월 Windows 7, 2023 년 1 월 Windows 8.1 의 지원이 종료되었습니다. 즉, 소프트웨어 제공사인 마이크로소프트사는 이후 Windows 7, Windows 8.1 에서 취약점이 발견되더라도 문제를 수정하는 프로그램을 개발하지 않습니다. 이러한 OS 를 인터넷에 연결한 채 계속 사용하는 것은 매우 위험합니다.
따라서 지원이 종료된 시스템은 가급적 사용하지 마십시오. 구버전 OS 에서만 작동하는 애플리케이션이 있는 경우, 인터넷에서 분리된 상태로 사용하십시오.
OS 외에도 애플리케이션의 경우, 2022 년 6 월에 Internet Explorer 의 지원이 종료되었습니다. 또한 브라우저에서 동영상 재생에 사용되어 온 Adobe Flash 도 2020 년 말에 지원이 종료되었습니다.
학교나 조직에 따라서는 지원이 종료된 OS 가 설치된 컴퓨터를 네트워크에 연결하는 것을 금지하는 곳도 있습니다.

Windows 지원 종료일

OS	지원 종료일
Windows XP	2014 년 4 월 8 일
Windows Vista	2017 년 4 월 11 일
Windows 7	2020 년 1 월 14 일
Windows 8.1	2023 년 1 월 10 일
Windows 10	2025 년 10 월 14 일

5-3 암호 기술

1. 통신 암호화

인터넷 등에서 통신 중 문서나 이미지 등이 제 3 자에 의해 도청·변조되는 것을 방지하기 위해 일정한 규칙에 따라 데이터를 변환하는 것을 '암호화'라고 합니다.

웹 상에서는 사용자 ID 나 비밀번호를 암호화하여 통신하는 SSL(Secure Socket Layer)이라는 프로토콜이 사용되고 있습니다. 최근에는 SSL 보다 더욱 강력한 TLS(Transport Layer Security)가 표준적으로 사용되고 있습니다. (SSL 이라는 명칭이 정착되어 있기 때문에 TLS 를 SSL 이라고 부르기도 합니다. 또한 SSL/TLS 로 표기되기도 합니다.)

암호화 통신 확인

상업 사이트에서 회원 정보나 상품 구매 시 신용카드 번호를 입력할 때는 SSL/TLS 에 의한 암호화 통신이 이루어지고 있는지 확인해야 합니다.

최근에는 상업 사이트 외에도 도청이나 변조를 방지하기 위해 SSL/TLS 에 의한 암호화 통신으로 설정을 변경하는 경우가 많아졌습니다.

SSL/TLS 에 의한 통신인 경우 브라우저 주소창의 URL 은 일반적인 "http://…"이 아닌 "https://…"이 됩니다. 또한 화면에 자물쇠 아이콘이 표시됩니다. (브라우저에 따라 표시되는 위치나 모양이 다릅니다.)

2. 무선 LAN 도청 방지 대책

회사나 학교 등에서 많은 사람이 자유롭게 인터넷을 이용할 수 있는 환경을 조성하기 위해, 유선 케이블 없이도 접속 가능한 무선 LAN 도입이 보편화되고 있습니다. 그러나 무선 특성상 보안 설정이 되어 있지 않으면 외부인이 LAN 내부 데이터를 엿볼 수 있어, 개인정보가 유출되는 사건이 발생하고 있습니다.

가정 등에서 무선 LAN 을 도입할 경우, 무선 LAN 의 액세스 포인트 역할을 하는 라우터는 반드시 통신 암호화 기능이 있는 제품을 사용하여 불법 접속을 사전에 차단해야 합니다. 일반적으로 무선 LAN 라우터는 출고 시 암호화나 비밀번호 설정이 되어 있지 않으므로, 설명서를 참고하여 직접 설정하십시오.

6-1 저작권

현실 사회와 마찬가지로 네트워크 사회에서도 저작권을 비롯한 지적 재산권은 법률로 보호받고 있습니다. 인터넷 보급으로 누구나 손쉽게 정보를 발신할 수 있게 되면서 지적 재산권에 대한 더욱 세심한 주의가 필요해지고 있습니다.

1. 저작권

저작자의 권리는 저작물을 창작한 시점에서 자동으로 발생합니다. 저작자의 권리에는 저작인격권과 재산권으로서의 저작권이 있습니다.

저작인격권이란 주로 저작자의 정신적 이익을 보호하는 권리로, 공표권, 성명표시권, 동일성유지권의 3 가지로 구성됩니다.

저작권(재산권)이란 저작물을 창작한 자에게 부여되는 독점적 권리로, 일본에서는 저작물이 창작된 시점부터 저작자 사후 70 년간 존속합니다(2018 년 저작권법 개정으로 저작물, 실연 및 레코드의 보호 기간이 저작자 사후 50 년에서 사후 70 년으로 연장되었습니다). 영화나 출판사·신문사 등의 단체 명의 저작물인 잡지, 신문 등은 공개 후 70 년간이 보호 대상이 됩니다. 사후 공개 후 기간 계산은 사망·공개 다음 해 1 월 1 일부터 기산됩니다. 또한 2 차적 저작물(저작물의 번역·편곡)에도 일정 범위에서 저작권이 적용됩니다.

6-2 저작물의 이용과 저작인접권

1. 저작물을 이용하려면

원칙적으로 타인의 저작물을 이용하려면 저작권자의 허락을 얻어야 한다는 것이 저작권법에 규정되어 있습니다. 다만, 아래의 조건을 충족하는 경우에는 그러하지 않습니다.

허락이 필요 없는 것

- 보호 기간이 종료된 저작물(제 51 조~제 58 조) (권리가 소멸됨)
- 사실만을 전달하는 보도(제 10 조 제 2 항) (저작물에 해당하지 않음)
- 헌법, 기타 법령 및 법원의 판결(제 13 조 제 1 호, 제 3 호) (저작물이지만 저작권의 대상이 됨)
- 국가, 지방자치단체의 기관 등이 발하는 고시, 훈령, 통달 기타 이에 준하는 것(제 13 조 제 2 호) (저작물이지만 저작권의 대상이 됨)
- 개인의 사적 이용, 인용, 학교나 도서관 등의 공공 시설에서의 비영리적 이용 등 (제 30 조~제 50 조) (저작권법에서 인정됨)

저작물의 공정 이용

저작권법에서는 개인의 사적 이용, 인용, 학교나 도서관 등의 공공 시설에서의 비영리적 이용이라면 저작권자의 허락 없이 저작물을 복제하거나 가공하는 것이 일정한 조건 하에 인정됩니다.

다만, 인터넷에 공개되는 웹 페이지 등에서의 사용은 '공중에게 제시'에 해당하므로, 개인의 웹 페이지라 하더라도 사적 사용으로 간주되지 않으며, 학교 등의 공공 이용 목적 사이트라 하더라도 불법입니다. 회사 등의 인트라넷 내에서의 사용도 불법입니다(제 49 조 제 1 항 제 1 호).

사적 이용 목적의 복제

개인적으로 또는 가정 내에서 사용하는 경우, 아래 조건 하에 저작권자의 허락 없이 복제하는 것이 허용됩니다(제 30 조).

- 복사 방지 장치를 제거하고 리핑(Ripping: 디지털 데이터를 컴퓨터로 추출)하는 행위는 불가
  (예) 영화 DVD 의 복사 방지 장치를 제거하고 복사하는 행위.
- 불법 복제물을 다운로드하는 행위는 불가
  (예) 스트리밍 사이트에서 이용 허가 표시가 없는 TV 프로그램이나 영화를 불법 콘텐츠임을 알면서도 다운로드하는 행위.

저작물의 정당한 인용 조건

보고서나 논문 등을 작성할 때에는 다음 조건 하에 저작권자의 허락 없이 인용하는 것이 허용됩니다(제 32 조, 제 48 조).

・공개된 저작물로부터의 인용이어야 함
・인용의 필요성과 인용 범위의 필요성이 있어야 함
・자신의 글과 인용 부분의 차이가 명확히 구분되도록 인용해야 함
・어디까지나 자신의 글이 주가 되고 인용문이 참고 수준이어야 함
・출처가 명시되어야 함

2. 저작인접권

실연가나 레코드 제작자, 방송 사업자 등은 '저작물의 전달자'로서의 역할을 한다는 의미에서 저작인접권이라는 권리로 보호받고 있습니다. 각 저작인접권은 방송권, 송신가능화권, 양도권, 대여권, 복제권 등으로 구성됩니다.

저작인접권 침해의 구체적 사례로는 콘서트를 녹화한 영상을 인터넷에 공개하는 행위나 구입한 CD 의 음원 등을 인터넷상에서 배포하는 행위가 있습니다(또한 이러한 행위는 저작권 자체도 침해합니다). 제 3 자가 이용할 경우 저작권자와 저작인접권자의 허락이 필요합니다.

6-3 저작권 침해 행위

저작권법을 위반하지 않으려면 타인이 작성한 것을 무단으로 사용하지 않는 것이 원칙입니다. 타인의 저작물을 복제, 인용하거나 웹 페이지 등에 게재하고자 할 때는 '허락이 필요하지 않은' 것으로 인정되는 경우를 제외하고는 반드시 허락을 받아야 합니다.

1. 소프트웨어 라이선스 계약

소프트웨어 라이선스 계약이란 소프트웨어 사용 허가 계약을 말합니다. 설치 가능한 컴퓨터 대수나 사용 기간 등을 정한 것입니다. 소프트웨어는 라이선스 계약 내용에 따라 이용해야 합니다. 소프트웨어를 무단으로 복제·배포하면 처벌 대상이 됩니다.

2. 인터넷상의 저작권 침해 행위

인터넷상에서 다음과 같은 행위는 저작권 침해에 해당하며 금지됩니다. 범죄이므로 각별히 주의해야 합니다.

불법 게재·업로드 (인용 형식을 따르고 극히 일부일 경우 허용될 수 있음)

・책이나 잡지 내용을 스캐너 등으로 스캔하여 무단으로 웹 페이지 등에 게재하는 행위.
・출간 전 책을 인터넷에 게시하는 행위("조기 유출")
・TV 나 비디오에서 추출한 동영상 등을 무단으로 웹 페이지 등에 게재하는 행위
・TV 프로그램에서 녹화한 비디오 등을 무단으로 웹 페이지에서 판매하는 행위
・타인이 촬영한 사진을 무단으로 웹 페이지 등에 게재하는 행위
・연예인(아이돌) 사진을 가공(콜라주)한 것(아이콜라)을 웹 페이지 등에 게재하는 행위 (자신이 촬영한 사진이라도 초상권 침해나 명예훼손이 될 수 있습니다.)
・타인의 웹페이지 이미지나 사진, 저작물 복사본 등을 무단으로 자신의 웹페이지에서 사용한다.
・ 저작권자의 허락 없이 프로그램을 인터넷이나 학내 LAN 에서 다운로드 가능한 상태로 만든다.
・ 타인이 제작한 프로그램이나 이를 개정한 것을 파일 공유 소프트웨어를 이용해 무단으로 배포한다.
・CD 나 레코드, 또는 타인이 제작한 곡에서 추출한 음원을 그대로 또는 MP3 형식이나 MIDI 형식으로 변환하여 네트워크 상에 무단으로 배포하는 행위.
・발신자의 허락 없이 이메일을 공개하는 행위.
(경우에 따라 사생활 침해나 명예훼손에 해당할 수 있습니다.)
・ 불법 복제된 소프트웨어나 음악·영상을 불법임을 알면서도 인터넷 경매 등에 출품하는 행위.
・ 게임 실황 동영상을 허가 없이 업로드한다. 게임 플레이 중 화면(정지화면, 동영상 모두)은 저작물이므로 무단 업로드는 금지된다. (게임사에 따라 허용하는 경우도 있으나 확인이 필요하다.)
・ 생성 AI 로 제작한 글이나 이미지도 원본 글이나 이미지의 유사성과 의존성이 인정되는 한 저작권 침해에 해당하므로 인터넷 업로드 시 각별히 주의한다.

불법 다운로드(범죄입니다)

・ 불법으로 업로드된 음악이나 영상을 불법임을 알면서도 다운로드(녹음 또는 녹화)하는 행위는 불법입니다. 또한 저작권법이 2020 년에 개정되어 2021 년 1 월부터는 인터넷에 공개된 만화나 서적, 논문, 소설, 프로그램 등 모든 저작물에 대해 불법으로 업로드된 것을 알면서 다운로드하는 행위는 불법이 되었습니다.

패스트 무비(Fast Movies)

패스트 무비란 영화 본편을 영상이나 정지 화면으로 편집하여 10 분 정도의 동영상으로 요약한 것을 말합니다. 패스트 시네마, 줄거리 동영상이라고도 합니다.

패스트 무비가 동영상 공유 사이트에 업로드되면 영화를 보러 가지 않아도 줄거리를 알게 되어 영화 배급사에 심각한 손실을 주는 저작권 침해 행위로 큰 문제가 되고

있습니다.

2022년 11월에는 저작권 침해 행위로, 패스트 무비 게시자에게 5억 엔의 손해배상을 명하는 판결이 내려졌습니다(도쿄 지방재판소 2022년 11월 17일 판결).

동영상 편집은 컴퓨터로도 쉽게 할 수 있지만, 패스트 무비를 제작하여 업로드해서는 안 됩니다.

스포일러 사이트

스포일러 사이트란 만화의 이미지가 아닌, 그 줄거리를 공개하는 웹사이트를 말합니다. 만화 속 대사를 그대로 복제하는 것은 인용으로 간주되지 않으며, 저작권법 위반에 해당합니다.

3. 배경에 찍힌 이미지

촬영한 사진이나 녹화한 동영상을 블로그 등에 공개하는 경우가 있습니다. 본래 의도한 피사체 외에 배경에 작게 포스터나 그림이 찍히거나, 거리에서 흘러나오던 음악이 우연히 녹음된 경우, 저작권 침해에 해당하지 않습니다.

다만, 다음과 같은 경우는 저작자의 이익을 부당하게 해치므로 원칙적으로 저작권자의 허락이 필요하니 주의하십시오.

- 본래의 촬영 대상으로 포스터나 그림을 촬영하여 블로그에 게재하는 경우.
- 그림이나 포스터를 주로 보여주기 위한 목적으로 녹화하여 영상을 인터넷으로 전송하는 경우.
- 본래의 촬영 대상에 부가가치를 부여하기 위한 목적으로 캐릭터를 함께 찍은 사진을 웹상에서 공개하는 경우.

6-4 사생활과 초상권

1. 사생활 침해

네트워크 상에서 본인이 원하지 않는 형태로 개인정보가 유출·공개되는 사건이 발생하고 있습니다. 아래는 네트워크 상에서 적지 않게 목격되는 사생활 침해 행위입니다. 사생활은 인격권의 하나로서 법률에 의해 보호받고 있으므로, 이러한 행위는 절대 해서는 안 됩니다.

- 타인의 얼굴 사진을 본인 동의 없이 공개한다. (다음 항목 '초상권·퍼블리시티권'에서 상세히 설명합니다.)
- 개인적인 이메일 본문 또는 일부를 본인의 허락 없이 공개하는 행위. (이메일에도 저작권이 있습니다.)

・타인의 이메일 주소, 주소, 전화번호 등의 개인정보를 무단으로 공개하는 행위.
・타인의 범죄 경력, 병력, 직업 경력, 학력 등을 공개하는 행위.
・본인의 동의 없이 누구와 함께 행동하고 있다는 등의 내용을 SNS 나 블로그에 공개하는 행위.

프라이버시에 대한 생각은 시대와 함께 변해왔습니다. 사회의 정보화가 진전됨에 따라 모든 사람이 '프라이버시를 침해받지 않을 권리'를 가지고 있다는 생각이 널리 퍼지고 있습니다. 자신에 관한 정보, 타인에 관한 정보를 다룰 때에는 이 점을 잊지 않도록 합시다.

2. 초상권·퍼블리시티권

초상권이란 사람이 자신의 초상(얼굴이나 모습의 사진 등)에 대해 가지는 권리입니다. 현재 일본에는 초상권을 규정하는 법률은 없지만, 권리로서 인정되고 있습니다.
초상권에는 다음 두 가지가 있습니다.

인격권으로서의 초상권

인격권은 개인의 인격적 이익을 보호하는 권리입니다. 즉, 무단으로 자신의 사진 등을 사용당하지 않을 권리입니다. 타인의 초상을 함부로 공개하여 사생활을 침해하는 행위는 불법입니다. 이는 일반인인지 유명인인지에 관계없이 누구나 주장할 수 있는 권리입니다.

재산권으로서의 초상권

유명인(연예인이나 프로 스포츠 선수 등)은 브로마이드 등의 초상을 이용해 경제적 이익을 창출할 수 있습니다. 재산권에 기반한 초상권은 이러한 경제적 가치를 보호하고 제 3 자가 무단으로 이용하지 못하도록 하는 권리입니다. 일반적으로 '퍼블리시티권'이라고 불립니다.

초상권, 퍼블리시티권을 침해하지 않기 위해 다음 사항에 주의해야 합니다.

・사진이나 동영상을 촬영할 때는 피사체가 되는 본인의 허락을 받는다.
・사진에 찍힌 사람에게는 흐림 처리 등을 한다.
・유명인의 사진을 무단으로 사용하지 않는다.

6-5 개인정보 보호법

1. 개인정보 보호법이란

정보화 사회에서 빈번하게 발생하는 개인정보 유출과 부정 이용에 대응하여 개인의 권리와 이익을 보호하기 위해 제정된 법률입니다. 즉, 개인의 사생활 정보를

보호하기 위한 법률이며, 개인정보를 취급하는 사업자는 정보를 외부에 유출해서는 안 된다는 규정을 담고 있습니다.
이 법률에서는 개인정보의 적정한 취급에 관한 기본 이념, 민간 사업자의 준수 사항, 벌칙 등이 정해져 있습니다.
정식 명칭은 「개인정보 보호에 관한 법률」(이하 「개인정보 보호법」으로 약칭)로, 2003 년 5 월에 공포(일부 시행)되어 2005 년 4 월부터 전면 시행된 법률입니다. 2015 년, 2020 년, 2021 년에 각각 개정되었으며, 2020 년 개정과 2021 년 개정 일부는 2022 년 4 월 1 일부터 시행되었습니다.

2003 년　개인정보보호법 제정(2005 년 전면 시행)
2015 년　대폭 개정(2017 년 전면 시행. 3 년마다 재검토 규정이 포함됨)
2020 년　개정(2022 년 4 월 1 일 전면 시행. 3 년마다 재검토에 따른 개정)
2021 년　개정 (2022 년 4 월 1 일 일부 시행)

(1) 「개인정보」의 정의
개인정보란 생존하는 특정 개인을 식별할 수 있는 정보를 말합니다. 2015 년 개정으로 보호 대상이 되는 개인정보의 정의가 명확화되어 다음 3 종류가 정해졌습니다.

・개인정보
생존하는 개인의 주소·성명·생년월일·성별 등 특정 개인을 식별할 수 있는 것
・개인식별기호
특정 개인의 신체 일부 특징을 디지털화한 정보(지문 데이터 등)
개인 고유 기호(여권번호, 면허증번호, 마이넘버 등)
・특별관리개인정보
인종, 신조, 병력, 범죄 경력 등 민감정보

(2) 개인정보의 유용성 확보(활용)을 위한 정비
・익명가공정보(특정 개인을 식별할 수 없도록 개인정보를 가공하여 얻은 개인에 관한 정보) 규정이 2015 년 개정에서 신설되었습니다.
・가명가공정보(다른 정보와 대조하지 않는 한 특정 개인을 식별할 수 없도록 가공된 개인정보) 규정이 2020 년 개정에서 신설되었습니다.

(3) 개인정보 보호 강화
개인정보를 취득할 경우, 본인에게 사전에 이용 목적을 명시해야 합니다.
또한 수집한 개인정보를 제 3 자에게 제공하는 경우, 사전에 본인의 동의를 얻어야 합니다.

(4) 개인정보보호위원회 설치
개인정보보호위원회가 2016 년 1 월 신설되어 개인정보 처리 사업자에 대한 감독 권한이 이 위원회에 일원화되었습니다. 또한 2021 년 개정으로 해당 위원회는 개인정보 처리 사업자뿐만 아니라 국가 행정기관, 독립행정법인, 지방자치단체의

개인정보 처리를 일원적으로 감시·감독하게 되었습니다.

(5) 기타

또한 2015 년 개정으로 다음과 같은 사항이 변경 또는 신설되었습니다.

・ 기존 법률에서 대상에서 제외되었던 5,000 명분 이하의 개인정보를 취급하는 사업자에게도 개정법이 적용됩니다.

・옵트아웃(개인 데이터의 제 3 자 제공에 대해 사전에 통지하거나 본인이 알 수 있는 상태로 해 두고, 본인이 반대하지 않는 한 동의한 것으로 간주하여 제 3 자에게 제공하는 것) 절차가 엄격화되어, 본인에 대한 통지 사항 등을 개인정보보호위원회에 신고해야 한다.

・ 일본 국외로의 개인정보 제공에 관한 제한, 개인정보보호법의 국외 적용, 개인정보보호위원회에 의한 외국 집행 당국에 대한 정보 제공에 관한 규정이 신설되었다.

2. 마이넘버

1. 마이넘버 제도란

개인에게 12 자리 번호인 '마이넘버(개인번호)'를 부여하여 여러 기관에 존재하는 개인 정보가 동일인의 정보임을 확인하는 데 사용됩니다. 마이넘버는 2015 년 10 월에 통지되었습니다. 2016 년 1 월부터 사회보장, 세금, 재해 대책의 행정 절차에 이용되었으며, 2021 년부터는 건강보험증으로도 이용 가능해졌습니다. 기존의 건강보험증은 2024 년 12 월 2 일부터 신규 발급이 중단되고, 건강보험증 이용 등록을 한 마이넘버 카드(마이넘버 건강보험증)로 일원화되었습니다.

7-1 불법접속금지법

1. 불법접속금지법이란

「불법접속행위의 금지 등에 관한 법률」(이하 '불법접속금지법')이 2000 년 2 월부터 시행되었습니다. 이 법률은 급증하는 사이버 범죄의 방지, 네트워크 상의 질서 유지, 고도 정보통신사회의 건전한 발전을 목적으로 합니다.

이후 법 개정이 이루어져 현재는 불법 접속 자체 외에도 불법 접속의 기반이 되는 피싱 등의 불법 접속 준비 행위도 금지되었으며, 처벌도 강화되었습니다.

2. 불법접속금지법 개요

「불법 접속 행위」란 다음과 같은 행위를 말합니다.

・타인의 ID 와 비밀번호로 접근한다. (사칭)

・시스템이나 소프트웨어의 취약점(보안 구멍)을 이용해 접근한다.(크래킹)

「불법 접속 준비 행위」란 다음과 같은 행위를 말합니다.

・불법 접속 목적으로 타인의 ID·비밀번호를 취득한다.
・본인의 동의 없이 그 ID·비밀번호를 불법 접속을 목적으로 하는 제 3 자에게 제공한다(악질적인 불법 접속 조장 행위).

「불법 접속 조장 행위」란 타인의 비밀번호 등을 본인의 동의 없이 제 3 자에게 제공하는 행위입니다. 제 3 자에게 불법 접속 의도가 없더라도 범죄에 해당합니다. 이러한 범죄에 휘말리지 않기 위해 자신의 ID·비밀번호를 타인에게 알려주어서는 안 됩니다.

・부정하게 취득한 타인의 ID·비밀번호를 불법 접속 목적으로 보관한다.
・타인의 ID·비밀번호를 입수하기 위해 피싱 사이트를 제작하여 공개한다.
・ID·비밀번호 입력을 요구하는 피싱 메일을 발송하여 타인의 ID·비밀번호를 입수하려 한다.

7-2 소셜미디어를 통한 불법 행위와 법률

1. 게시판에서의 범행 예고

"＊월＊일, ＃＃역을 폭파하겠다"는 식의 범행 예고가 게시판 등에 게시되어 큰 소동을 일으키는 경우가 있습니다.

게시 동기는 대부분 "어떤 소동이 벌어지는지 보고 싶다"는 호기심에서 비롯됩니다. 예고된 장소나 그 인근에서는 회사나 학교를 휴업하는 등 많은 사람들에게 영향이 미칩니다.

게시판의 범행 예고는 중대한 범죄 행위로, 형법의 사기업무방해죄 또는 위력업무방해죄에 해당할 수 있습니다.

최근에는 단속을 강화하기 위해 게시자를 추적·특정할 수 있게 되었습니다. 또한 웹상의 범행 예고를 자동으로 탐지하는 프로그램도 개발되었습니다.

한편, 풍설을 유포해 회사나 개인의 신용을 훼손하거나 업무를 방해하는 행위는 신용훼손죄·업무방해죄에 해당하며, 대량의 스팸 메일을 유포하거나 자살 소동을 일으키는 등 업무를 방해하는 행위는 사기업무방해죄 또는 위력업무방해죄에 해당합니다.

2. 업무방해 등 피해 게시물

대학생들이 테마파크에서 장난을 치며 찍은 사진을 X(구 트위터)에 게시하는 등 비상식적 행위가 크게 보도되었습니다.

그 외에도 아르바이트 점원이 소셜 미디어에 게시한 장난 사진으로는

・편의점 아이스 케이스 안에 들어간 사진
・햄버거 가게에서 번 위에 누워 있는 사진
・피자 가게에서 피자 반죽을 얼굴에 대고 있는 사진
・라면 가게에서 조리 전 소시지를 물고 있는 사진

등이 있었으며 잇따라 발생했습니다.

게시한 당사자들에게는 단순한 장난일지라도 업무 방해 등 심각한 문제로 발전할 수 있습니다. 심지어 해당 매장이 폐업에 몰리는 경우도 있습니다. 아르바이트 장소 등에서 얻은 당사자만 아는 내부 정보 등을 게시하는 것도 신중해야 합니다.

위와 같은 행위는 신용훼손죄·업무방해죄로 처벌받을 수 있을 뿐만 아니라 손해배상 청구를 당할 수도 있습니다.

친구들끼리의 장난으로 넘길 수 없는 일이니, 절대 이런 게시물을 올려서는 안 됩니다.

3. 헤이트 스피치

「헤이트 스피치 대책법」(정식 명칭: 「본방 외 출신자에 대한 부당한 차별적 언동의 해소를 향한 노력의 추진에 관한 법률」)은 민족·인종에 대한 차별적 언동, 이른바 「헤이트 스피치」의 해소를 추진하기 위해 제정된 법률입니다. 기본 이념으로 차별적 언행이 용납되지 않음을 선언하고 있습니다. 2016 년 6 월에 시행되어, 헤이트 스피치 해소를 위한 노력이 국가와 지방자치단체에 요구되고 있습니다.

소셜 미디어에서의 차별적 게시물은 이 법률에 저촉될 수 있으므로 주의해야 합니다.

4. 사생활 보호

"지금 A 군과 B 씨가 함께 걷고 있습니다"와 같은 글을 올리면, 사실이라 하더라도 사생활 침해, 경우에 따라 명예훼손이 될 수 있습니다. 타인의 정보를 허락 없이 함부로 게시해서는 안 됩니다.

또한 스마트폰 내장 카메라 등으로 동의 없이 타인의 사진을 찍거나, 이를 함부로 SNS 등에 공개해서는 안 됩니다.

5. 모욕죄

2020 년 여자 프로레슬링 선수가 인터넷상의 비방·중상을 견디지 못하고 자살하는 사건이 발생했습니다. 사후에도 고인을 모욕하는 글이 계속되자 유족은 모욕죄로 소송을 제기했습니다. 결과적으로 유죄 판결이 내려졌으나, 매우 가벼운 벌금에 그친 점이 문제가 되었습니다.

이에 따라 2022 년 모욕죄를 엄벌화하는 내용의 개정 형법이 가결·성립되었습니다.

모욕죄는 30 일 미만의 구류 또는 1 만 엔 미만의 과료였으나, 이번 개정으로 1 년 이하의 징역 또는 금고 또는 30 만 엔 이하의 벌금 또는 구류 또는 과료에 처해지게 되었습니다.

7-3 전자상거래에 관한 법률

1. 전자소비자계약법

인터넷 쇼핑 등을 이용할 때 클릭 실수나 주문 수량 오류가 발생할 수 있습니다. 「전자소비자계약법」(정식 명칭: 「전자소비자계약에 관한 민법의 특례에 관한 법률」)은 이러한 조작 실수의 가능성을 고려하여 사이트 운영자에게 주문 확정 전에 반드시 주문 내용 확인 화면을 표시하도록 의무화하고 있습니다. 이러한 확인 화면이 마련되지 않은 경우에는 실수로 클릭해도 착오를 이유로 계약을 무효화할 수 있습니다.

한편, 원클릭 사기(무료라고 생각하고 클릭했는데 갑자기 유료 사이트 회원 가입 화면이 표시되어 대금을 청구받는 경우)에 의한 허위 청구와 같은 경우에는 전자소비자계약법을 적용할 필요도 없이, 애초에 계약 자체가 성립하지 않습니다. 따라서 대금을 지불할 필요가 없으니, 기억에 없는 청구가 오더라도 모두 무시하십시오. 다만, 본인의 주소나 성명을 상대방에게 알려준 경우에는 간이법원의 소액소송 절차 등을 이용해 지불을 요구해 올 수도 있습니다. 법원이 발송한 정식 서류인 경우에는 무시하지 말고 즉시 경찰에 상담하십시오.

2. 티켓의 부정 전매

콘서트나 스포츠 등의 티켓이 터무니없이 높은 가격으로 인터넷 경매에 출품되는 사례가 많습니다. 전매 목적으로 대량 구매하는 업자나 개인 때문에, 정말 티켓을 원하는 사람이 구하지 못하거나 정가로는 구매할 수 없는 문제가 심각해지고 있습니다.

이에 따라 「티켓 부정 재판매 금지법」이 제정되어 2019 년 6 월 14 일부터 시행되고 있습니다.

정식 명칭은 「특정 공연 입장권의 부정 재판매 금지 등에 의한 공연 입장권의 적정한 유통 확보에 관한 법률」입니다.

이 법에 따라 정가를 초과하는 가격으로 전매하는 행위가 금지되었습니다. 위반 시 처벌은 1 년 이하의 징역 또는 100 만 엔 이하의 벌금, 혹은 그 양쪽입니다.

전매 목적으로 티켓을 구입하려 하거나, 전매가 금지된 티켓을 인터넷 경매에 출품하는 등의 행위는 해서는 안 됩니다. 또한, 부정한 전매 경로로 티켓을 구입하지 않도록 합시다.

7-4 컴퓨터 바이러스 관련 범죄

컴퓨터 바이러스를 제작·보관·제공하는 행위는 범죄에 해당합니다. 형법상 '악성코드 등 무단 명령 전자기록에 관한 죄', 통칭 '컴퓨터 바이러스 범죄'라고 합니다. 컴퓨터 바이러스로 인한 실질적 피해가 없더라도 다음과 같은 사례에서 처벌 대상이 됩니다.

컴퓨터 바이러스의 제작·제공 (형법 제 168 조의 2)

무단으로 타인의 컴퓨터에서 실행시키기 위한 목적으로 컴퓨터 바이러스를 제작하거나 제공한 경우 성립합니다. 백신 소프트웨어 개발·연구 등 정당한 목적의 제작은 해당하지 않습니다.

바이러스를 제작·제공하는 행위는 3 년 이하의 징역 또는 50 만 엔 이하의 벌금에 처해집니다.

컴퓨터 바이러스의 취득·보관(형법 제 168 조의 3)

무단으로 타인의 컴퓨터에서 실행시키기 위한 목적으로 컴퓨터 바이러스를 취득하거나 보관한 경우 범죄로 성립합니다.

이메일 등을 통해 바이러스에 감염된 피해자의 경우에는 해당하지 않습니다.

바이러스를 취득·보관하는 행위에 대해서는 2 년 이하의 징역 또는 30 만 엔 이하의 벌금이 부과됩니다.

SNS 를 통한 바이러스 확산과 바이러스죄 적용 범위

2019 년, 브라우저 크래셔 URL 을 게시판에 올린 중학생이 보호관찰 처분을 받았습니다. 브라우저 크래셔란 브라우저에 의도하지 않은 팝업 창이 반복적으로 표시되는 프로그램입니다.

컴퓨터바이러스죄에서 규정하는 컴퓨터바이러스의 제작·제공에 해당하는 행위인지 여부가 논란이 되었습니다. 단순한 장난이라는 가벼운 마음에서도 큰 문제로 이어질 수 있으므로, 이러한 행위는 삼가야 합니다.