

スマホ・SNSを安全に楽しむためのサイバー防犯教室

{ プロが教える「ネットの罠」の見破り方 }

CYBER CRIME PREVENTION : MASTERING DIGITAL FORENSICS & SAFETY

[illegible]

TARGET SCORES			
MF150000000	B=100000000	50%	50+050100
1500000000	B=100000000	100%	50+050100
1500000000	B=100000000	100%	50+050100

```
00000000 : 0000
00000001 : 000000000000
00000002 : 00000000
00000003 : 0
00000004 : 000000000000
00000005 : 000000000000
00000006 : 000000000000
00000007 : 000000000000
```

大人が教えたいこと vs 君たちが本当に知りたいこと

全国のデータによると、中学生の半数以上がネットトラブルを経験します。今日は「マナー」の話はしません。
ハッカーや犯罪者が君たちを狙う「本当の手口(スクリプト)」を解剖します。

大人がよく教えること



ネット上の悪口・
いじめ等のコミュ
ニケーション問題
(68.3%の大人が指導)

中学生が知りたいこと



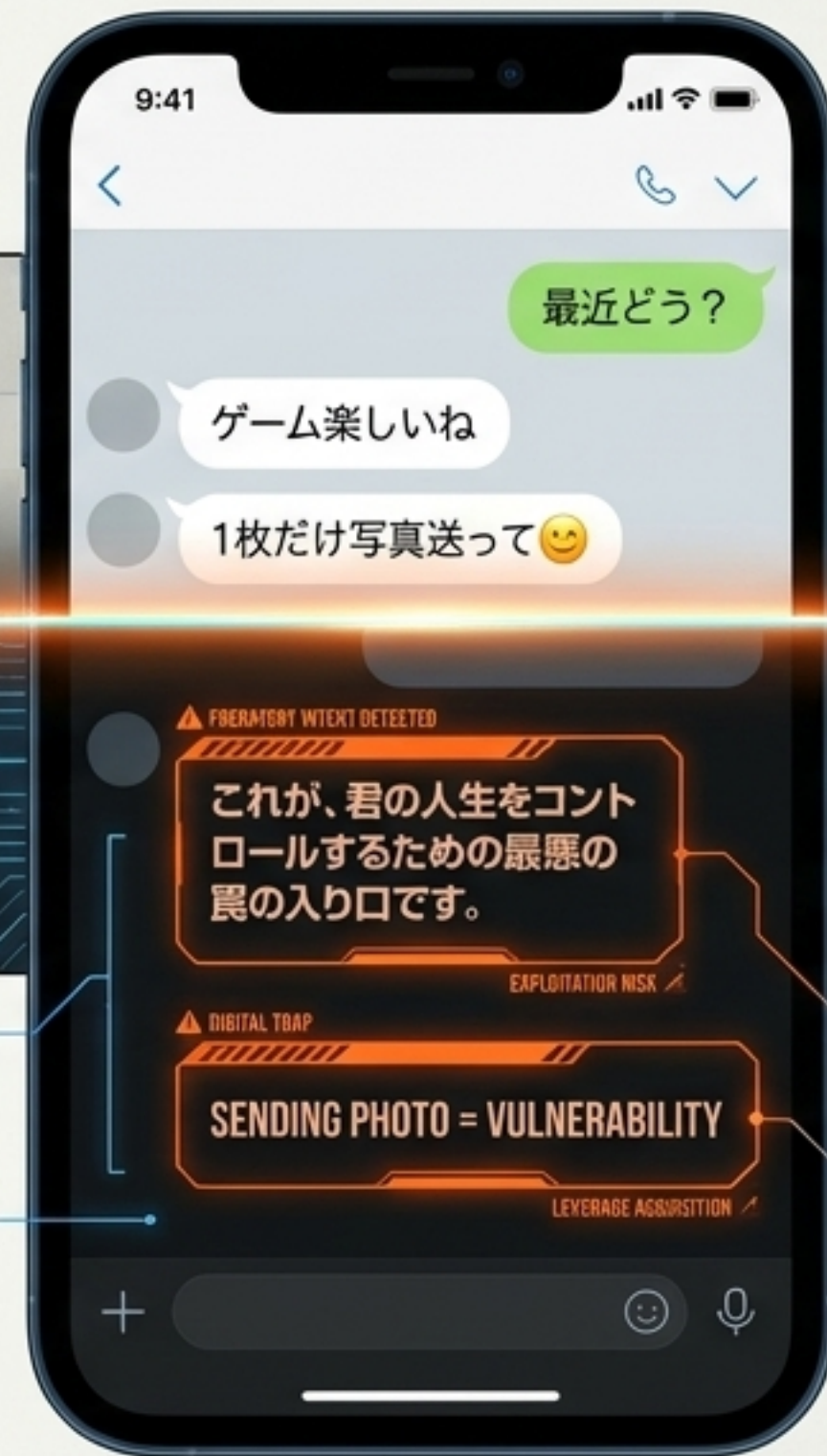
ウイルスや不正
アクセスなどの
セキュリティ対策
(知りたいこと第1位:
28.7%)

脅威①:「写真送って」に潜む罠(セクストーション)

衝撃の事実:この犯罪で「自撮り写真を送らされた」被害者の55%は中学生です。(警察庁データより)

X-Ray

ゲームやSNSで親しくなった相手からの「1枚だけ写真送って」という軽いお願い。これが、君の人生をコントロールするための最悪の罠の入り口です。



セクストーションの解剖図（罠のタイムライン）

フェーズ1：準備（Grooming）
- 「君は特別だ」「悩みを相談してよ」と優しく近づき、徹底的に信頼させる。

フェーズ2：要求（The Ask）
- 「2人だけの秘密にしよう」「写真を見せ合おう」と要求。別の秘密アプリに移動させる。

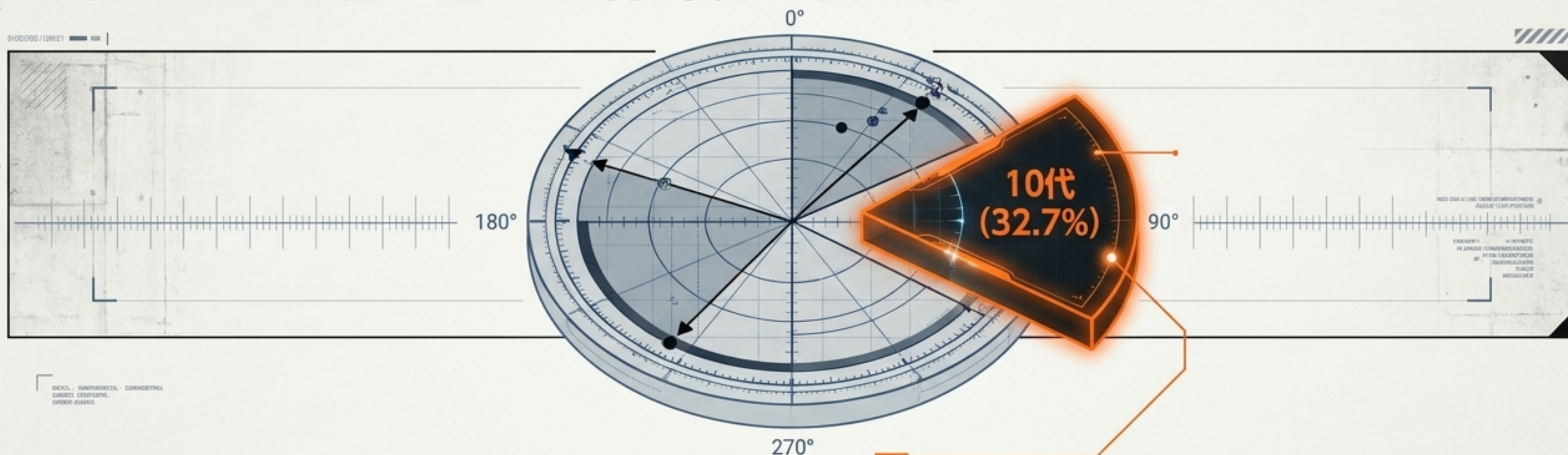
フェーズ3：豹変（The Trap）
- 画像を送った瞬間、態度が豹変。「言うことを聞かないと学校や友達にばらまくぞ」と脅迫材料（人質）にする。

【鉄則】 一度送信した画像は、二度とインターネットから消せません。
どんなに親しい相手でも、**自分の弱みになる写真は絶対に送らないこと。**

STH004 11:00:00 79
STH005 10:00:00 12
STH006 14:00:00 00
STH007

脅威②：君のアカウントが乗っ取られる？

「自分はハッカーに狙われるような有名人じゃない」と思っていないですか？
高度な技術を持った海外の犯罪組織だけではありません。
君のパスワードを狙っているのは、同じ学校の生徒や顔見知りかもしれません。



不正アクセス(乗っ取り)で検挙された
人間の3人に1人(約32.7%)は10代です。

270004 11:00:25.73
270005 11:00:40.10
270006 11:01:00.00
270007 11:01:20.00

アカウント乗っ取りの「本当の手口」

映画のハッカー



黒い画面で高速タイピングし、システムを破壊する。

現実のハッカー



どこかから流出した「使い回しのパスワード」を入力するだけ。（検挙事案の98%がこの手口）

防御プロトコル

1. 使い回し厳禁

ゲーム、Insta、TikTok...同じパスワードを使っていると、1つ漏れただけで全て奪われます。



2. 多要素認証（二段階認証）をオンに

これを設定するだけで、パスワードがバレてもログインを防げます。



脅威③:「簡単・高額」に潜む闇バイトの罠

見えている幻 (Illusion)

「スマホだけで即日現金」
「誰でもできる簡単な副業」

隠された現実 (Reality)

犯罪組織が、使い捨ての「受け子・出し子(逮捕される役)」を募集している罠。



X-RAY SCAN:
ILLICIT RECRUITMENT INTERFACE DETECTED



90° 使い捨ての
「受け子・出し子」

SCAN ID: 398-BETA
THREAT LEVEL: HIGH

闇バイトが「人質」に変わる瞬間

Step 1: 応募

DMを送り、LINEや別のアプリに誘導される。

Step 2: 登録

「仕事の前に、登録確認として学生証やマイナンバーカードの写真を送って」と言われる。

[THE TRAP SNAP - Point of No Return]

Step 3: 脅迫

身分証を送った瞬間、辞めようとする「家に行くぞ」「家族や学校にばらすぞ」と脅され、抜け出せなくなる。

まともな仕事は、あなたを脅しません。
「高額＋簡単」は100%犯罪です。

SCAN ID: 398-BETA
THREAT LEVEL: HIGH

脅威④:「写真1枚から「自宅」がバレる?

何気なく撮ったこの1枚の写真。

ここから、見ず知らずの他人があなたの「自宅の住所」を特定できるとしたら?



この写真を「デジタル・レントゲン」で
解析してみましょう。

SCAN ID: 398-BETA
THREAT LEVEL: HIGH

モザイクアプローチとExifの恐怖

日常のルーティンや、自宅の窓からの景色は絶対にアップしないこと。

Exif情報 - 写真のデータ内に記録されたGPSの緯度経度(誤差わずか3~10m)。AirDropやメールで送るとそのまま残ります。

Exif情報 - 写真、眼やサングラスに反射した駅の看板や景色。

瞳の映り込み - 眼やサングラスに反射した駅の看板や景色。

窓の外の景色 - 太陽の影の角度や遠くの建物から、マンションの階数まで割り出される(モザイクアプローチ)。

電柱やマンホール - 地域特有の模様や形から市町村を特定。

SCAN ID: 398-BETA
THREAT LEVEL: HIGH

ハッカーの台本(嘘を見破る翻訳機)

犯罪者の言葉	本当の意味
「これは2人だけの秘密ね」	「大人が介入してくると困るから孤立させよう」
「48時間以内に払わないとばらまくぞ」	「パニックにさせて、冷静な判断力を奪おう」
「安全確認のために身分証の写真を送って」	「逃げられないように脅迫材料(人質)を確保しよう」
「スマホだけで即日高収入!ノーリスク!」	「リスクと逮捕はお前に押し付けて、金は俺がもらう」

77065 1148:21.73
20000 11504:17.6
21700 11508:13.20
23607

SCAN ID: 398-BETA
THREAT LEVEL: HIGH

47.8

16.9

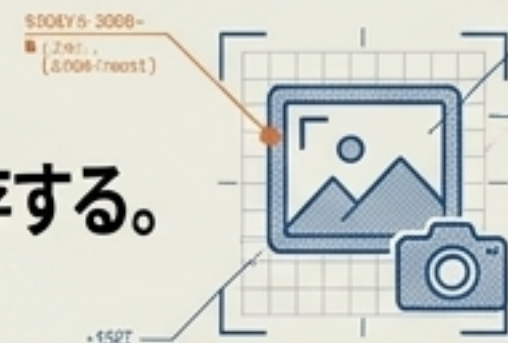
もしも罠に落ちてしまったら（魔の最初の30分）

犯罪者が一番望むのは、君がパニックになり、証拠を消し、誰にも言わずに隠すことです。その逆をやりましょう。

1

1. 絶対に消さない（証拠保全）

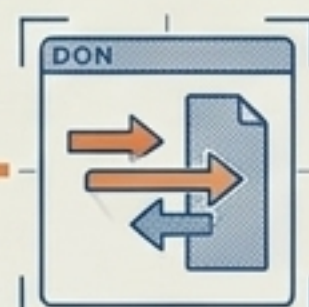
やり取りの画面、相手のアカウントをスクリーンショットで保存する。
警察が捜査するための最強の武器になります。



2

2. 絶対に払わない・送らない

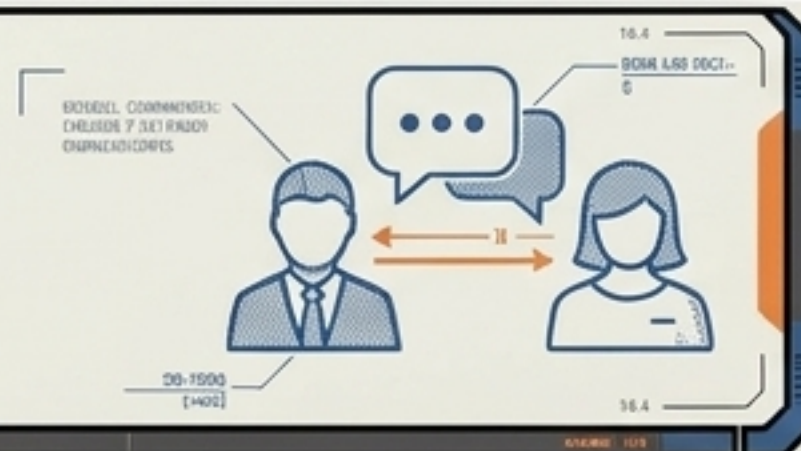
要求に応じても終わりません。
「こいつは脅せば動く」と証明するだけです。



3

3. 絶対に隠さない

一人で解決しようとするのが一番危険。
一番信頼できる大人に、すぐに話すこと。



SCAN ID: 398-BETA
THREAT LEVEL: HIGH

君を守るためのライフライン（緊急連絡先）

親や先生に言いづらい場合でも、プロが君を助けてくれます。今すぐスマホに登録しておいてください。

#9110

警察相談専用電話：
「犯罪かもしれない」と
迷ったときの相談窓口

110

警察の緊急通報：
脅されている、今すぐ
危険が迫っている場合

0120- 007-110

子どもの人権110番：
ネットのいじめや
被害の相談

SCAN ID: 398-BETA
THREAT LEVEL: HIGH

正しい知識が、君を最強にする

今日、君たちはハッカーの台本(手口)を手に入れました。知識は最大の防御です。
デバイスをコントロールするのは、君自身です。デバイスにコントロールされてはいけません。



最後に1つだけ約束してください。

もしも自分が変なトラブルに巻き込まれたり、友達が悩んでいたりしたら、
「ひとりで抱え込まず、一番早く信頼できる大人に話す」こと。

SCAN 10: 398-BETA
THREAT LEVEL: HIGH