



身近に迫るサイバー空間の脅威

～知っておきたいサイバーセキュリティの勘所～

神 奈 川 県 警 察
サイバーセキュリティ対策本部

[https://www. police .pref.kanagawa.jp/](https://www.police.pref.kanagawa.jp/)



神奈川県警のマスコット
ピーガルくん



サイバー空間の情勢概況

サイバー空間の「公共空間」化



- コロナ禍において、社会のデジタル化が急激に進展し、あらゆる国民、企業等にとって、サイバー空間は「公共空間」として、より一層の重みを持つようになっている



みんなが



大切なことを

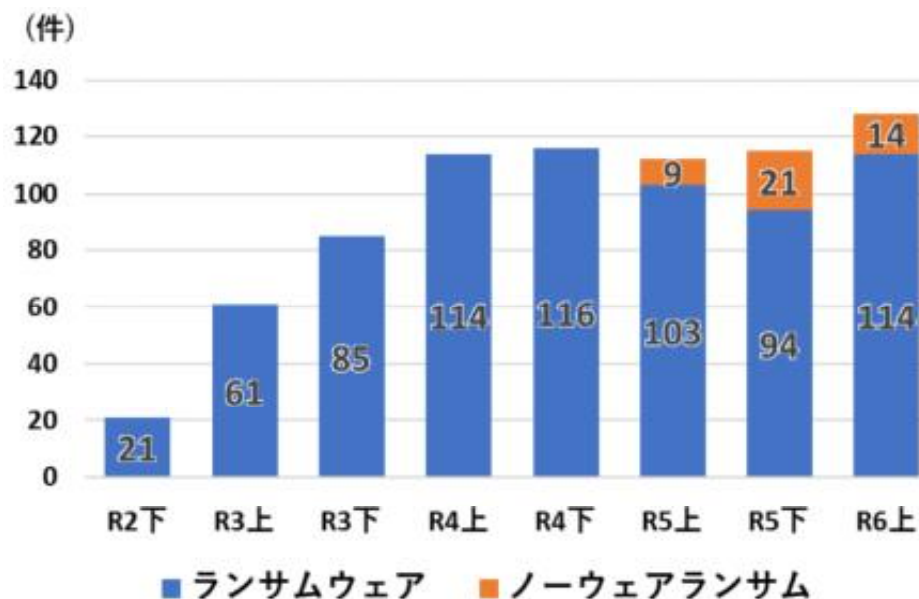


サイバー空間で

サイバー空間の脅威の情勢 極めて深刻



- ランサムウェア被害が依然として高水準で推移
- フィッシングが前年比約10万件増加、不正送金被害も高止まり



【ランサムウェア被害の企業・団体等における被害の報告件数の推移】



【フィッシング報告件数及び不正送金被害額(概数)の推移】

最近多いサイバー相談

騙されないで！こんなトラブルに注意！



！＜サポート詐欺＞

パソコンでサイト閲覧中、突然大音量で警告音が鳴りウイルス感染の警告画面が出た。焦って画面に表示された番号に電話すると、サポート費用を支払うよう言われた。



最近多いサイバー相談

騙されないで！こんなトラブルに注意！



！＜偽情報＞

災害発生に関連して**二次元コード**を添付して寄付金を求める投稿や、義援金や支援物資を募るメールやSMSを本物と信じ込み送金しそうになった。



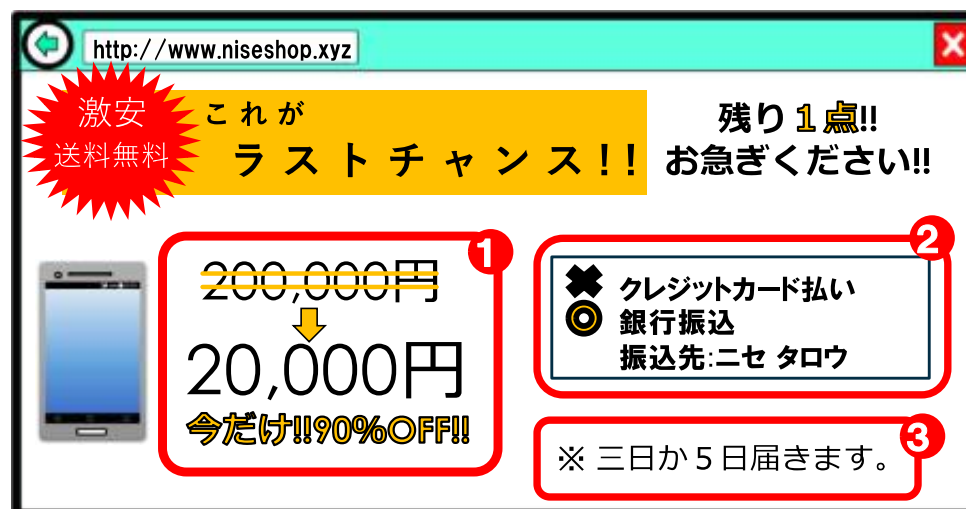
最近多いサイバー相談

騙されないで！こんなトラブルに注意！



！<偽ショッピングサイト>

欲しい商品を検索していると、安く販売しているショッピングサイトを発見したので注文して代金を振り込んだが、到着予定日を過ぎても商品が届かない。



最近多いサイバー相談

騙されないで！こんなトラブルに注意！



！<フィッシング>

ネット銀行から「不正アクセス」、「個人情報の確認」、「取引の停止」などというメールが来たため不安に思い、メール本文に記載されたURLを押してID・PWを入力しようとした。



From：XYZ銀行
件名：【重要】取引停止のお知らせ

本人かどうか確認が取れない
取引がありましたので停止しました。
確認してください。

<http://bank.example.com>



**フィッシングに騙されない！！
知っておきたい勧所**



フィッシング(Phishing)に注意!!

- 実在する企業等を装ったSMSやメールを送りつけ、受信者をフィッシングサイト(偽物のサイト)へ誘導してIDやパスワード等を入力させ、不正に個人情報等を搾取する手口



フィッシング (Phishing)



フィッシング (Fishing)



フィッシングメールの例

From : XYZ銀行
件名 : 【重要】取引停止のお知らせ

本人かどうか確認が取れない取引がありましたので停止しました。
確認してください。
<http://xyz-bank.com>

取引の停止



From : XYZカード
件名 : 【緊急】不正アクセスを検知しました

第三者からの不正なアクセスを検知しました。
確認してください。
<http://xyz-card.com>

不正アクセス



 050xxxxxxx

お荷物のお届けがありましたが、不在の為持ち帰りました。
<http://example.jp>

不在持ち帰り



銀行等を装ったメールやSMSから偽のウェブサイトに誘導し、金融情報や個人情報を不正に入手する手口、それがフィッシングです！



- 銀行口座を操作されて勝手に送金される
- ECサイトで勝手に買物をされる
- アカウントを乗っ取られる

【問題】 フィッシングメールの
対応が間違っているのは??



A メール内のリンクは押さない

B 返信メールで確認する

C すべてのメールを疑う

【問題】 フィッシングメールの 対応が間違っているのは??



B 返信メールで確認する



ボイスフィッシング

- 銀行を名乗って企業に電話をかけ、手続き名目でメールアドレスを聞き出した上で偽メールを送ってIDやパスワードを盗み取る「ボイスフィッシング(ビッシング)」による不正送金被害が急増しています





ボイスフィッシング



犯人

〇〇銀行です。
ネットバンクの電子証明書の
更新手続きが必要です
更新用のリンクを送りますので
メールアドレスを教えてください

はっ、はい
メールアドレスは
●●●●●@●●●●●.co.jp
です



被害者(企業)

電話

1. 犯人が銀行担当者を騙り、被害者(企業)に電話をかけ(自動音声の場合あり)、メールアドレスを聞き出す



ボイスフィッシング



犯人

メールの中のURLに
アクセスしてID/パスワード
を入力してください

From: ●●銀行
件名: 【重要なお知らせ】
下記のURLにアクセスして
ください
<https://●●-BANK~>

はっ、はい

ログインはこちら

お名前

I D:hogehge
PW:password

ログイン

【重要】本サービスの利用には以下の条件に同意する必要があります。
1. 本サービスはインターネット上で提供されるサービスです。
2. パスワードは定期的に更新し、適宜に使用した場合は必ず変更してください。
3. 本サービスが利用できない場合は必ずパスワードを変更してください。



被害者(企業)

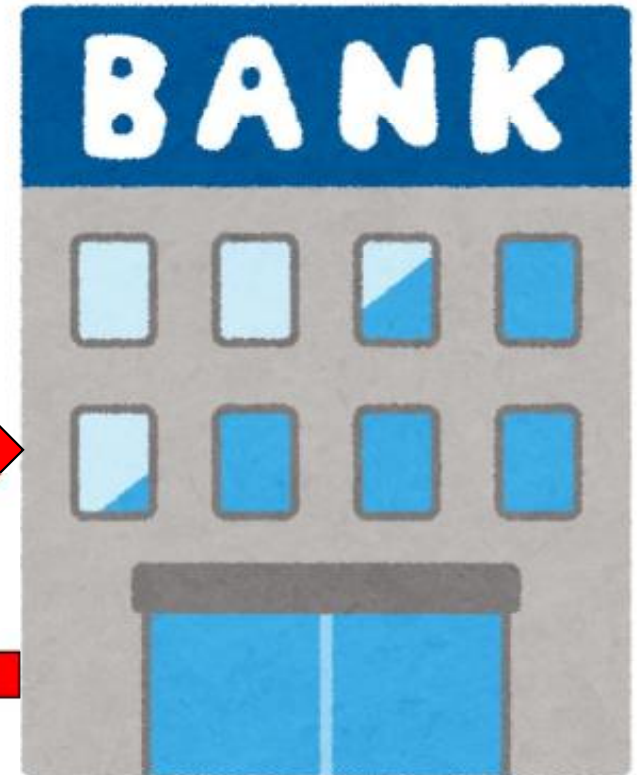
メール

2. 犯人がフィッシングメールを送信し、電話で指示しながら、被害者をフィッシングサイトに誘導。そして、インターネットバンキングのアカウント情報等を入力させて、盗み取る。

ボイスフィッシング



I D:hogehge
PW:password



3. フィッシングサイトに入力させたアカウント情報等を使って、犯人が法人口座から資産を不正に送金する。

ボイスフィッシング被害に 遭わないために！3つの対策



- ◆ 知らない電話番号からの着信は信用しない
- ◆ 銀行の代表電話番号・問い合わせ窓口で確認する

銀行担当者を騙る者から連絡があった場合には、銀行の代表電話番号へ連絡して確認するなど、慎重に対応してください

- ◆ メールのリンクからアクセスしない

インターネットバンキングにログインする場合は、銀行公式サイトや公式アプリからアクセスしてください。

その二次元コード、ほんとに大丈夫？ ～クイッシングの被害が増えています～



クイッシングとは？

悪意のある二次元コードをスマートフォン等で読み込ませて、意図しないサイトなどへ誘導する手口です。



〇〇Payで払えるのね
スキャンしよー

あれ???
いつもの画面が違う？

お支払いはこちらを
読込んでください



その二次元コード、ほんとに大丈夫？ ～クイッシングの被害が増えています～



<相談事例>

- 宅配業者から「再配達を予約するには以下の**二次**
元コードを長押ししてください」というメールが来た
ので長押し、表示された**サイト**に
情報を入力したところ、「●●カー
ドの**不正利用防止**にご**協力**願いま
す」というメールが来たが、使って
いないカード会社だったので**宅配**
業者に確認したところ、再配送の
メールは送っていないと言われた



その二次元コード、ほんとに大丈夫？ ～クイッシングの被害が増えています～



■ 考えられる手口

- ショッピングモールのフードコートで、テーブルに貼られている注文用の**二次元コード**を貼**り替えて**、フィッシングサイトに誘導し、決済情報を搾取する



その二次元コード、ほんとに大丈夫？
～クイッシングの被害が増えています～



■ 考えられる手口

- 展示会などで、フィッシングサイトへ誘導する二次元コードを掲載したチラシを配布する



その二次元コード、ほんとに大丈夫？
～クイッシングの被害が増えています～



■ 二次元コードは見た目だけでは「本物」か「偽物」か
判別できません!!

- 個人情報を入力する前に、リンク先が公式サイトか確認する
- 確認する際は、あらかじめブックマークしておいた公式サイト、または公式アプリを利用する
- 多要素認証を有効にして、ログイン時の安全性を高める

**二 次 元 コ ー ド を安易に読み
込まないよう気を付けましょう！**



リアルタイムフィッシング

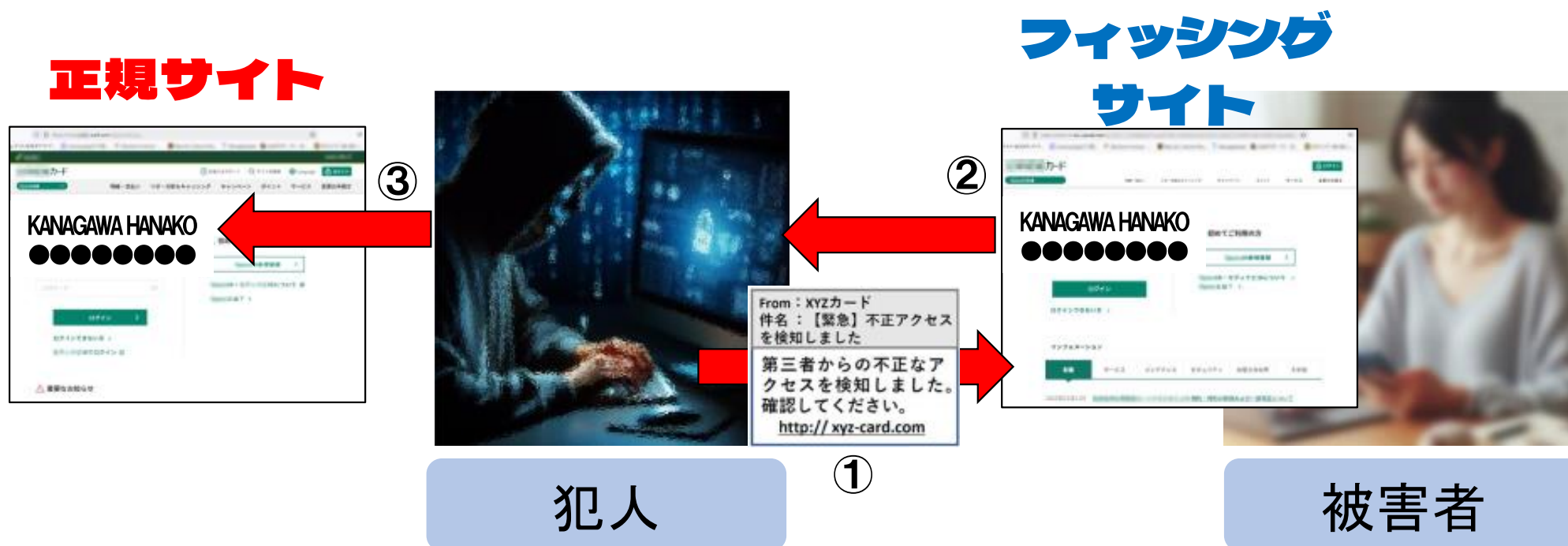
■ リアルタイムフィッシングとは？

- 被害者がフィッシングサイトにアクセスして入力したID/パスワードなどの情報を**リアルタイムで搾取**して**正規サイトに入力**してしまう手口
- ワンタイムパスワードを**求める偽ページを表示**させて搾取されると**ワンタイムパスワードも突破**されてしまう





リアルタイムフィッシング



- ① 犯人が偽のメールやSMSを被害者に送信する
- ② 被害者がフィッシングサイトにアクセスしてID/パスワードを入力
- ③ 入力されたID/パスワードで犯人が正規サイトにアクセス



フィッシング対策の勘どころ

- 普段から使っているサイトやサービス提供会社、有名な企業等からのメールでも・・・
 - ✓ メールやSMSに記載されたURLを安易にタップ(クリック)しない
 - ✓ 送信元のメールアドレス等が普段と同じかどうか確認する
 - ✓ メールの内容、書式、文章等に普段と違う、違和感がないか確認する
- 日頃から習慣づけていただきたいこと
 - ✓ サイトやサービスには、ブラウザのブックマーク等からアクセス、アプリがあればアプリを使う
 - ✓ アプリがある場合には、パスワード設定やカード情報の入力はアプリから行う





ログインさせようとする
メール/SMSは**全部偽物**

※ 人物画像はBing Image Creatorを使用して作成



サイバー犯罪等の
被害者にも加害者にも
ならないために



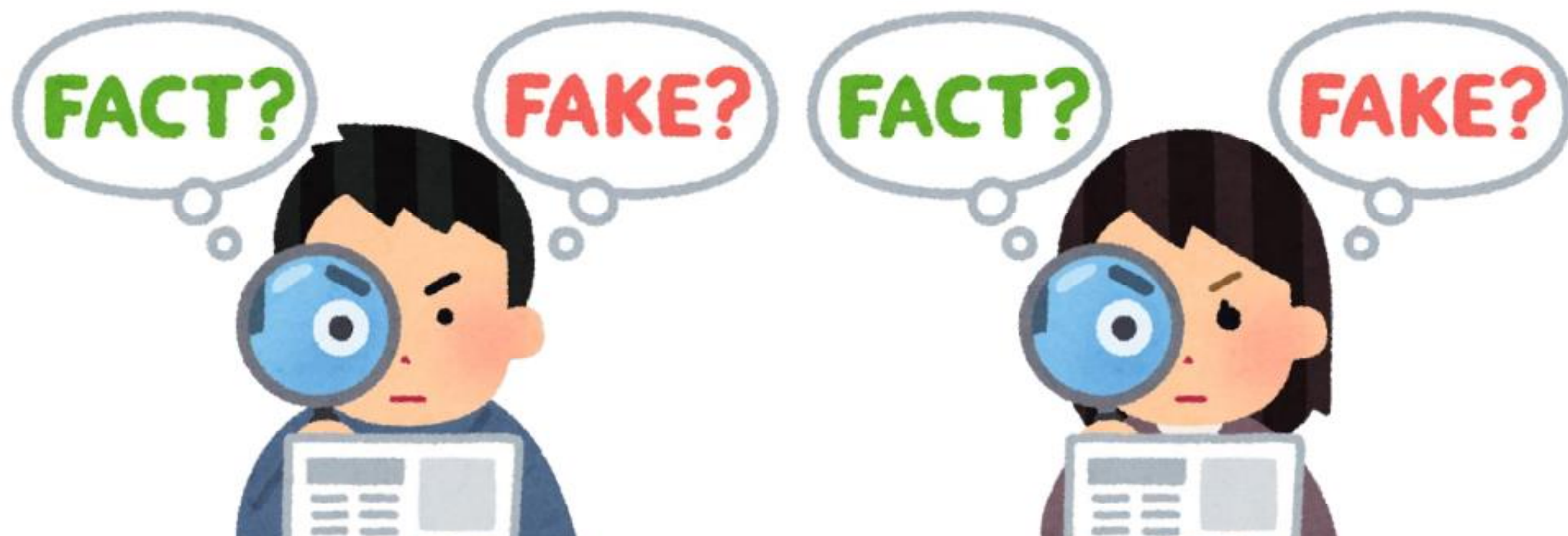
被害のきっかけは「偽～」

- サイバー犯罪、サイバー攻撃で使われる手口では、「偽～」使われています
 - 取引先を装った偽メールを使う標的型メール攻撃により機密情報を搾取される
 - 検索してたどり着いた偽ショッピングサイトで買い物をしてしまい詐欺の被害に遭う
 - 宅配業者、通信事業者を装った偽SMSから不正アプリをインストールしてしまった
 - フリマアプリ運営会社等を装った偽メールに誘導されてID・パスワードを取られた
 - いろいろなサイトを見ていたら、突然、ウィルス感染したという偽警告がでた など・・・





被害のきっかけは「偽～」



「本物」、「偽物」を見極める
「勘どころ」を押さえておきましょう！

偽サイト、偽メールに騙されない ための勘どころ



✓ メールアドレス、URLはおかしくないか？

- 送信元メールアドレス、URLは普段どおりか？

本物：～co**m**pany.co.jp ⇔ 偽物：～co**rn**pany.co.jp

- 見慣れないドメインを使ってないか？

「～.co.jp.～.xyz/～」などの紛らわしいものもある

スマホは画面が狭く、見づらいので特に注意！

✓ 違和感を感じるところがないか？

- 機械翻訳の様な**片言の日本語**がないか？
- **言い回し**や**書式**など**普段と違う**ところがないか？

キッカケはメール！！



- 多くのサイバー犯罪、サイバー攻撃のきっかけはメール！！
- 英文で添付ファイルが付いている怪しいメールではなく、よくある怪しくないメールが危ない！
- 少しでも違和感があれば確認する、家族や友人等に相談する、検索を試みる



メールに気を付けるという当たり前のことを徹底することで被害を防げることが多いことを知っておきましょう！！

そのメール

開く前に、まず

確かめる。



コンピュータ・ウイルスは
メールから感染することが多い
ことを知っていますか？



日頃からの情報収集

- 日々、巧妙化、複雑化するサイバー犯罪、サイバー攻撃に対応していくためには、日頃からの情報収集が不可欠
- 手口を知っているか知らないかが、被害に遭うか遭わないかの分かれ目
- 警察をはじめとしたサイバーセキュリティ関係機関のホームページやSNSなどで確認
- インターネットのニュースサイト等でも情報収集

サイバー社会で必要な3つの力



判断力
(考える力)

自制力
(がまんする力)

責任力

ネットの情報の正否、危険性の有無、
行動の善悪を見極める力が必要

興味本位や好奇心、軽い気持ちで
行ったことが思わぬ犯罪やトラブル
になることがあるため、
誘惑に負けない、
周りに流されない力が必要

ネット社会は自己責任が原則、
自分の行動に責任が取れる力が必要

サイバー社会で必要な3つの力



判断力、自制力、責任力

+ Imagination

- 自分が行なおうとしていることが、どのような結果を生じさせることになるか十分「想像」し、その結果に「責任」が負えないと「判断」したのであれば、「自制」して絶対に行わない

サイバーセキュリティは

知識よりも意識

が大切です

「サイバーセキュリティは技術的に難しいからわからない」と思われがちですが、
当たりまえと思える対策等を確実に行うことで多くの被害は防げます。まずは
意識を高め、そのうえで技術的な知識も身に付けると万全です。

※ 背景画像はBing Image Creatorを使用して作成