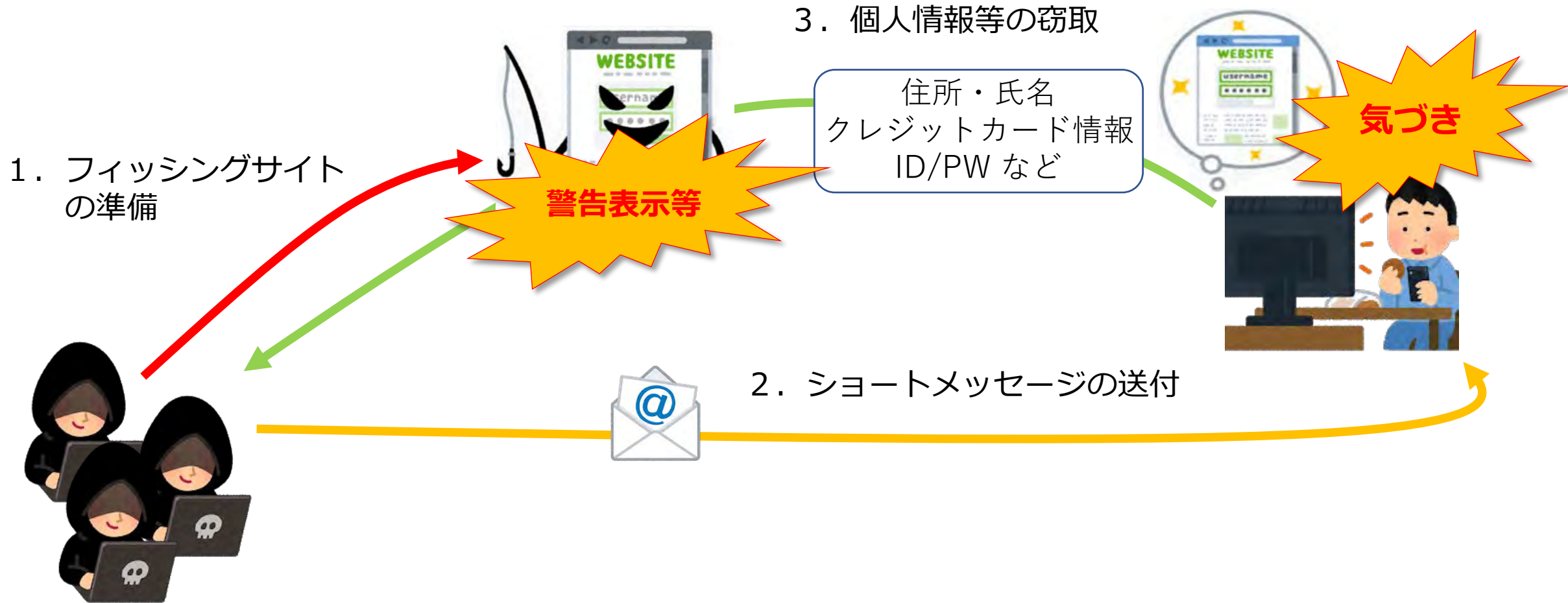


# フィッシングの手口に対する被害防止対策

## 被害防止対策



# 警察における取組

- サイバー犯罪対策は、犯人の検挙による大本の対処と同様に、**被害の未然防止・拡大防止が重要**
- 警察では、関係機関等と連携し、**対策を執る際の御参考にしていただきたい情報**を発信

## 警察庁における取組

### ○警察庁ウェブサイト等による注意喚起



このページは、サイバー犯罪・サイバー攻撃の被害防止を図るため、サイバー犯罪・サイバー攻撃等の情報を公開するものです。

注目情報

統計 令和2年上半年期におけるサイバー犯罪の発生状況

令和2年上半年期は、新型コロナウイルス感染症の影響により、サイバー空間における犯罪の発生が顕著となり、被害の発生が急増しました。

統計 令和元年におけるサイバー犯罪の発生状況

令和元年においては、警察庁が検出したサイバー犯罪の発生が顕著となり、被害の発生が急増しました。

注意 フィッシングによるものや、SNSを利用したサイバー攻撃等と連携した注意喚起

令和元年(2019年)9月からフィッシングによるサイバー攻撃が急増しており、10月及び11月においても被害が急増しました。また、11月における発生件数は573件、被害額は約1億2千万円(2017年)以降、最悪の水増しとなりました。



## 都道府県警察における取組

### ○サイバー防犯教室等における注意喚起



- **サイバーセキュリティカレッジ**  
インターネットを利用した犯罪に巻き込まれないためにインターネットに関する知識と犯罪被害防止の指導を行っています。  
また、公的機関や民間企業等を対象に、インターネット等を利用したコンピューターに対する攻撃からの防御方法やセキュリティ対策についての指導も行っています。

### ○サイバー防犯ボランティアと連携した防犯活動



# フィッシングによる被害を防止するために

## 予防策

### 事前の準備

- ・すでに利用しているサイトは、あらかじめ「ブックマーク」や「お気に入り」に登録しておく。
- ・スマホであれば、正規のアプリをインストールしておく。

### 不審なメールやショートメッセージ受信時の対応


- ・メール本文等に記載されたリンクをクリックしてアクセスをしないようにする。

### サイトアクセス時の対応

- ・「ブックマーク」や「お気に入り」、正規のアプリからアクセスする。
- ・接続先のURLが正しいかを確認する。また少しでも、「おかしいな」と感じたら、アクセスや情報の入力を中断する。

## 被害にあってしまった場合

- ・入力してしまった情報に応じて、すぐに銀行やクレジットカード会社などに連絡をし、必要な手続を行う。
- ・警察への相談・通報については、資料をそろえ、最寄りの警察署に出向いて行るか、まずは、警察相談電話「#9110」またはサイバー犯罪相談窓口で電話相談・問合せをする。



■ 国民一人ひとりが  
サイバーセキュリティの確保に必要な注意を払える状況に！

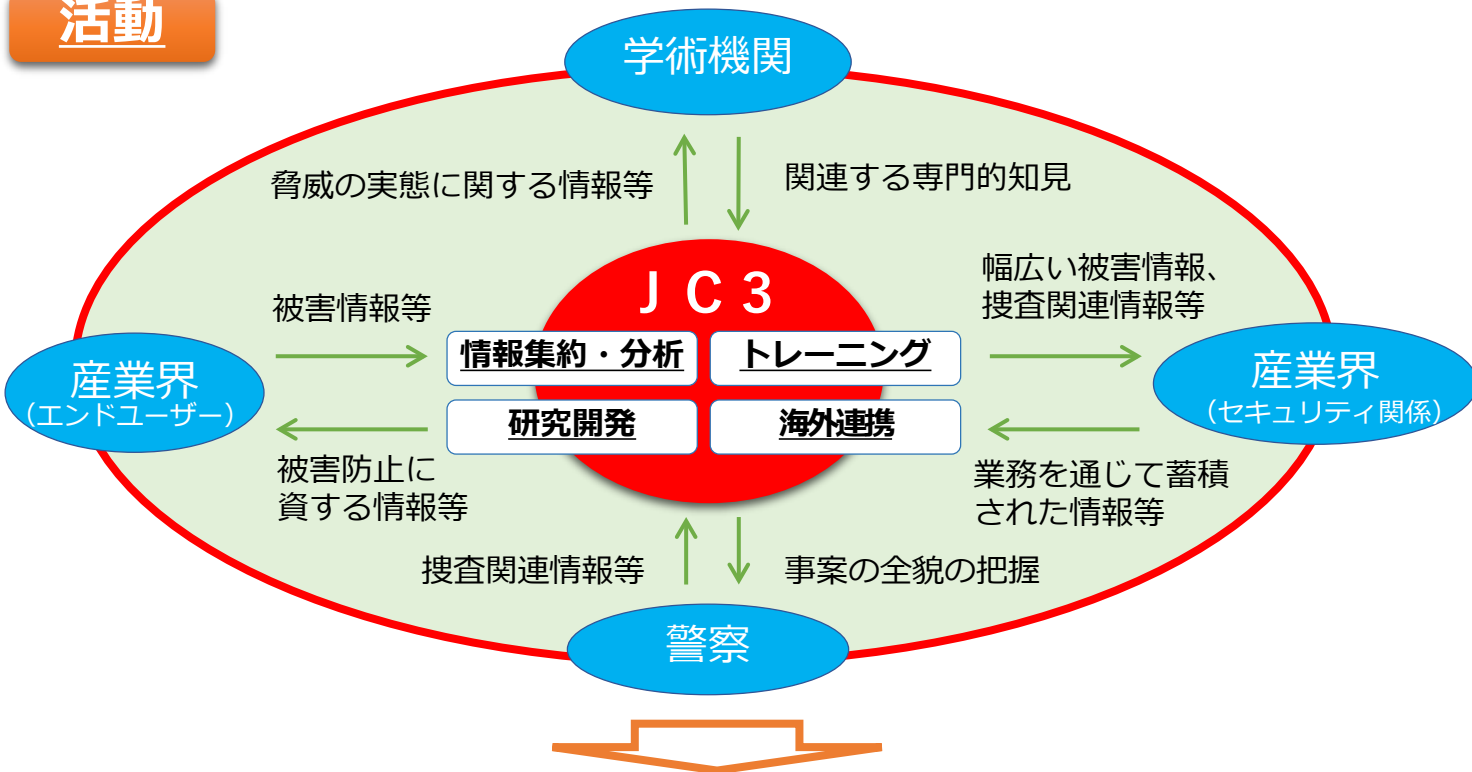
# 日本サイバー犯罪対策センター(JC3)との連携

一般財団法人日本サイバー犯罪対策センター  
(Japan Cybercrime Control Center : 略称 J C 3)

## 概要

産学官（法執行機関）それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を共有することにより、サイバー空間全体を俯瞰した上で、サイバー空間の脅威の大本を特定、軽減及び無効化し、以後の事案発生防止に資するための活動を行うための枠組み。

## 活動



サイバー空間の脅威に関する事象の全貌を把握し、その大本に対処することが可能に

## JC3による取組例

○様々なフィッシングの手口の分析に基づく注意喚起

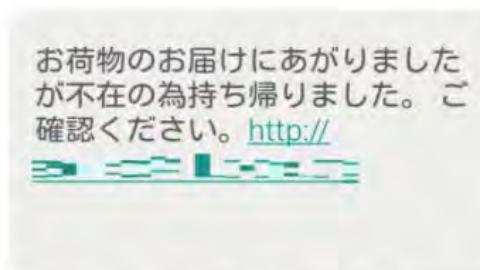


図 運送系企業を装ったSMS

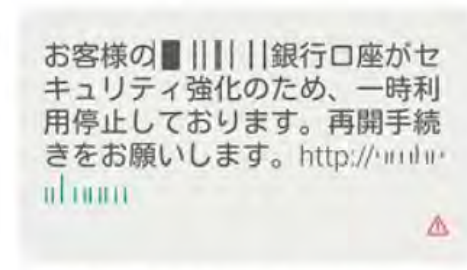
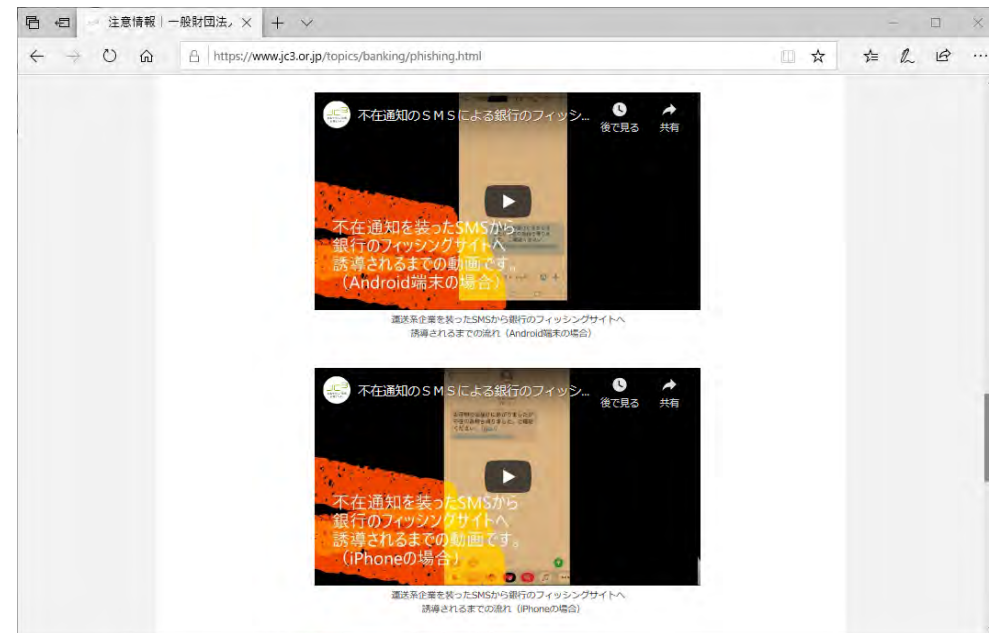


図 フィッシングメール(SMS)



引用：<https://www.jc3.or.jp/topics/banking/phishing.html>

# 官民連携による警告表示の対策等

## 偽サイト等への対策

- 警察庁では、海外サーバに開設された偽サイト等について、**関連情報をウイルス対策ソフト事業者等に提供し、閲覧の際に画面上に警告を表示するなどの被害拡大防止対策を実施**

## セキュリティ対応事業者との連携

- APWG (Anti-Phishing Working Group)



- フィッシング対策協議会

