



# サイバー警察局便り

Cyber Police Agency Letter 2025 Vol.6 (R7.9)

## 身边にサイバー攻撃の危険が迫っています！

『令和7年上半期サイバー空間をめぐる脅威情勢』を  
警察庁ウェブサイトにおいて公表しました。

<https://www.npa.go.jp/publications/statistics/cybersecurity/index.html>



### ！ ランサムウェア被害が半期として過去最多 ！

#### 〔情勢〕

中小企業の被害も半期で77件と過去最多

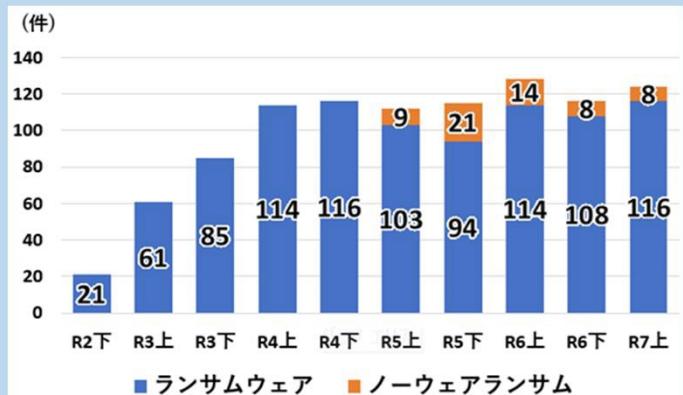
#### 〔対策〕

- VPN機器等のぜい弱性対策
- 認証情報の適切な管理
- バックアップやログの適切な取得
- サイバー攻撃を想定した業務継続計画（BCP）の策定



←対策をもっと知りたい方はこちら  
<https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html>

#### ランサムウェア被害の報告件数



### ！ 証券口座への不正アクセスが急増 ！

#### 〔情勢〕

証券会社をかたるフィッシングが増加

証券口座への不正アクセス・不正取引が増加

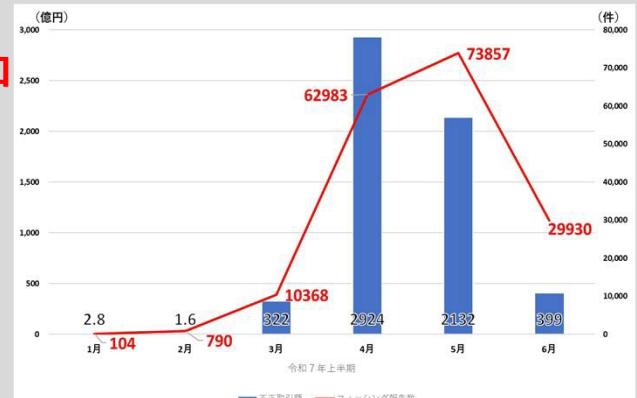
#### 〔対策〕

- ブックマークや正規アプリを活用
- 多要素認証（ワンタイムパスワード）や  
生体認証の活用・通知サービスなどを導入
- こまめに口座残高やログイン履歴を確認



←対策をもっと知りたい方はこちら  
<https://www.npa.go.jp/bureau/cyber/countermeasures/basic.html>

#### 証券口座不正取引額と証券口座に関するフィッシング報告件数



## 被害に遭ってしまったなら警察に通報・相談してください

最寄りの警察署又はサイバー犯罪相談窓口 → <https://www.npa.go.jp/bureau/cyber/soudan.html>



警察庁

National Police Agency

# 中小企業で被害多数 ランサムウェア

## サイバー攻撃のリスクを考慮した管理体制の構築を！

中小企業のランサムウェア被害は前年比で約4割の増加



被害未然防止の要は基本的対策の継続  
・VPN機器等のソフトウェア更新  
・パスワードの強度確保 等



被害拡大防止のために必要な備え  
・サイバー攻撃を想定したBCPの策定  
・オフラインを含むバックアップの取得  
・被害調査に必要不可欠なログの取得



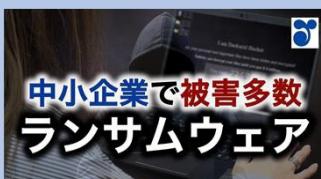
被害発生時は警察へ通報・相談を

※政府広報オンライン「中小企業で被害多数 ランサムウェア」より

詳しくは、政府広報オンライン動画  
「中小企業で被害多数 ランサムウェア」

警察庁制作協力

<https://www.gov-online.go.jp/useful/202506/video-298784.html>



動画「ランサムウェア対策の基本」

<https://www.gov-online.go.jp/vertical/online/video-478.html>

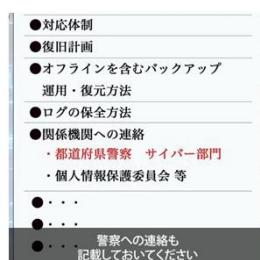
記事「ランサムウェア、あなたの会社も標的に?被害を防ぐためにやるべきこと」

<https://www.gov-online.go.jp/useful/article/202210/2.html>

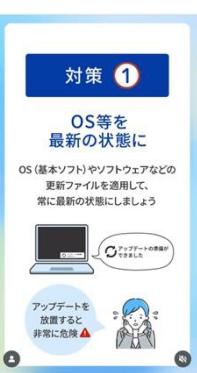
政府広報 SNSでも関連動画を公開中



X



Instagram



神奈川県警察サイバーセキュリティ対策本部



警察庁  
National Police Agency

# 騙されないで！こんなトラブルに注意！



## 例えばこんなこと...、ありませんか？

### ！<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。



### ！<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、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>



### ！<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。



## だまされている可能性「大」→まずは相談を！！

悩んだらまずは落ち着いて、身近な人に相談してみましょう。  
以下の相談窓口もありますのでご活用ください。



### 最寄りの警察署又はサイバー犯罪相談窓口

<https://www.npa.go.jp/bureau/cyber/soudan.html>

### 消費者ホットライン

☎188 (全国共通)

### IPA情報セキュリティ安心相談窓口

☎03-5978-7509



独立行政法人

国民生活センター

IPA

独立行政法人

情報処理推進機構



警察庁

National Police Agency

神奈川県警察サイバーセキュリティ対策本部

# そのメール、フィッシングかも！

## こんなメールやSMSに要注意！

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



050xxxxxxxx

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://xxx.com>

不在持ち帰り



メールやSMSによるフィッシング被害が発生中！！

## フィッシングに騙されるとどうなるの？

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

## フィッシングに対してできること



- メールやSMSに記載されたリンクをクリックしない  
→ 内容の確認は、公式サイトやアプリを利用する
- 携帯電話会社等の迷惑メッセージブロック機能を活用する
- 生体認証を活用する（パスワードを利用しない。）

※詳細なフィッシング対策はこちら ⇒ <https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html>



神奈川県警察サイバーセキュリティ対策本部



警察庁  
National Police Agency



# WARNING



## フィッシング詐欺に気を付けて！

- 証券会社を騙るフィッシング詐欺の被害が多くなっています！
- 【緊急】【重大】焦らせるメールは**特に注意してください！！**
- 詳しくは神奈川県警察ホームページをご覧ください。 [HPはこちら](http://www.chiba.police.jp)



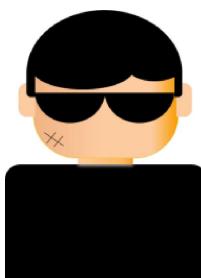
# 今、企業の資産（法人口座）がねらわれている！！

## 電話に注意！「ボイスフィッシング」による不正送金被害が急増

### 【手口の概要】

- 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。
- 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。
- 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。

※架電イメージ

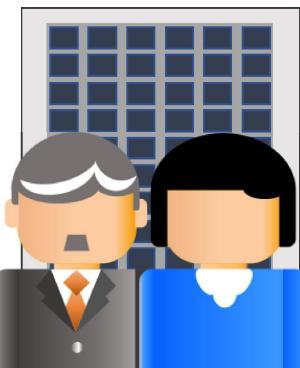


犯人



○○銀行です。  
ネット銀行の電子証明書の  
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。

電話



被害者(企業)

## 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。

◆ メールに記載されている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。

もしも、被害に遭ってしまったなら警察に通報・相談を！

最寄りの警察署又はサイバー犯罪相談窓口 → <https://www.npa.go.jp/bureau/cyber/soudan.html>



神奈川県警察サイバーセキュリティ対策本部



警察庁  
National Police Agency

# 関係者からのメール？それ本当？

## もしかしたら、標的型メール攻撃かも？

日本国内の学術、シンクタンク、政治家、マスコミに関する個人や組織に対して、安全保障や先端技術に係る情報窃取を目的とした組織的なサイバー攻撃が行われています。



## 被害に遭わないためには？

- 1 交流相手からのメールであっても普段と異なる状況がないか注意する
- 2 違和感があれば添付ファイルの開封やリンクをクリックしない
- 3 不審に感じたら送信者に確認する

MirrorFaceによるサイバー攻撃について（注意喚起）

<https://www.npa.go.jp/bureau/cyber/koho/caution/caution20250108.html>



神奈川県警察  
サイバーセキュリティ対策本部



警察庁  
National Police Agency