
一輪車


宝くじ桜

子宮がん検診車

宝くじは、みんなの暮らしに役立っています。


救急普及啓発広報車


宝くじドリームジャンボ絵本

集会用テント


「健康手帳」(冊子)


ベンチ

リスザル展示施設

宝くじは、少子高齢化対策、災害対策、公園整備、教育及び社会福祉施設の建設改修などに使われています。

一般財団法人日本宝くじ協会は、宝くじに関する調査研究や公益法人等が行う社会に貢献する事業への助成を行っています。

一般財団法人 日本宝くじ協会
https://jla-takarakuji.or.jp/

投資詐欺

投資についてアドバイスを行います。専用のアプリをダウンロードし、登録料をお支払い下さい。

闇バイト

1日5〜15万円稼げます!

グレーなアルバイト募集
稼げる仕事
高額バイト
即日払い

特殊詐欺

ランサムウェア

警告
暗号化を解除して欲しいなら金を支払え

－WARNING－
データを公開されたくなければ金を払え

あなたも、家族も狙われている!?

新時代のサイバー犯罪 徹底攻略BOOK

発行：公益財団法人 全国防犯協会連合会

この冊子は、宝くじの社会貢献広報事業として助成を受け作成されたものです。

闇バイト　犯罪実行者募集　匿名・流動型犯罪グループ　ランサムウェア　不正送金　投資詐欺　詐欺広告

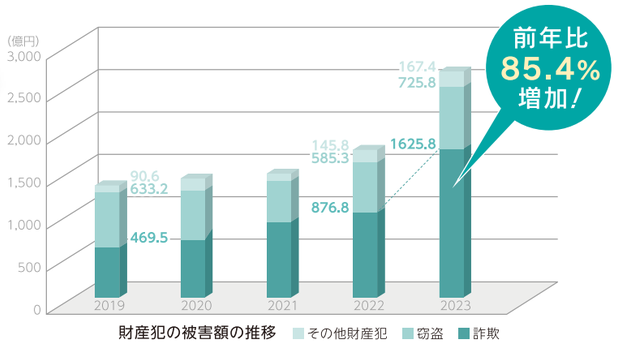
特殊詐欺、サイバー犯罪被害の深刻化が止まらない！

社会課題の解決に向けて、私たちにできることとは？

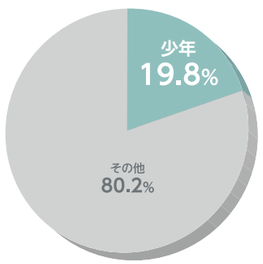
警察庁が公表した2023年の犯罪情勢によると、刑法犯の認知件数は前年比17%増の70万3,351件。
なかでも、特殊詐欺の認知件数は約2万件、被害額は約452.6億円と2年連続で増加、
SNSなどを通じてつながる犯罪グループが新たな脅威になっている実態があります。

Report 1　強盗・恐喝・窃盗・詐欺など財産犯の被害額が大幅増

なかでも、詐欺による被害額は前年比85.4%増の1,626億円!
インターネットを利用した詐欺の増加が関係していると見られています。



財産犯の被害額の推移　その他財産犯　窃盗　詐欺



受け子総検挙人員の割合

Report 2　特殊詐欺の「受け子」の5人に1人が少年　その裏にはSNSで闇バイトを募るトクリュウ※1の存在が

2023年の特殊詐欺関連統計によると、警察の検挙件数は7,212件（前年比8.6%増）、検挙人数は2,455人（前年比0.1%減）。このうち431人が20歳未満の少年であり、その約7割が「受け子」で、受け子の総検挙人員の約2割を少年が占めています。

※1：トクリュウ…匿名・流動型犯罪グループ。SNSを通じるなどした緩やかな結び付きで離合集散を繰り返す犯罪グループ。

Report 3　企業・団体等におけるランサムウェア被害が止まらない!

ランサムウェアと呼ばれる不正プログラムによる被害は全世界で深刻化、日本でも高い水準で被害件数が推移しています。信用面、金銭面でも大きなダメージを受ける企業が後を絶ちません。

あやしい情報にまどわされたり、ネット詐欺に遭ったりせず、
インターネット・SNSを安心・安全に使いこなすために、
一人ひとりが家庭や職場などで心がけたい
「サイバーセキュリティ」のポイントと最新事情を紹介します。

レッサイバーパンダ
マッ太くん

2023年 社会問題となったサイバー関連事件簿

CASE 01

広域強盗事件の実行役を集める手段として「闇バイト」がクローズアップ

2023年1月、東京都内で高齢女性が殺害された強盗殺人事件が発生し、その犯行態様の凶悪さが世間を震撼させました。後の捜査で、首謀者の男らは、フィリピンに拠点を置きながらSNSで実行役を募集し、日本国内で強盗や特殊詐欺を多数敢行していたことが判明しました。

CASE 02

特殊詐欺の受け子や出し子、強盗などの「闇バイト」IHC※2のサイト管理者等への削除要請は2,979件

警察庁は、強盗や特殊詐欺など闇バイトが絡む犯罪の摘発や対策を強化。10月には「匿名通報ダイヤル」の対象に闇バイト、SNS上で接点を持ち離合集散する匿名・流動型犯罪グループが関与する犯罪を追加し、情報料の上限を100万円に引き上げました。

※2：IHC…インターネット・ホットラインセンター（警察庁委託事業）

CASE 03

有名人をかたる「なりすまし広告」被害多発 SNS型投資詐欺（2023年）の被害額は約278億円

「○○さんが投資のアドバイスを行う」などの偽広告を入り口としたSNS型投資詐欺が多発。投資専門家や著名人を名乗る手口が多く、投資への関心の高まりや、インターネットで手軽に投資ができる環境への変化などが背景にあると見られています。

独立行政法人 情報処理推進機構（IPA）選出　情報セキュリティ10大脅威 2024

サイバー空間の脅威の情勢は、深刻な状況が続いています。
インターネットバンキングの不正送金被害は、発生件数5,578件、被害総額約87.3億円、それぞれ過去最多に!（2023年）
メガバンクを装ったSMS※3等のメールを通じて、フィッシングサイト（偽のログインサイト）へ誘導し、
IDやパスワード、ワンタイムパスワード等の個人情報を窃取して預金の不正送金を行う事案も多発しています。

「個人」向け脅威（五十音順）

- インターネット上のサービスからの個人情報の窃取
- インターネット上のサービスへの不正ログイン
- クレジットカード情報の不正利用
- スマホ決済の不正利用
- 偽警告によるインターネット詐欺
- ネット上の誹謗・中傷・デマ
- フィッシングによる個人情報等の詐取
- 不正アプリによるスマートフォン利用者への被害
- メールやSMS等を使った脅迫・詐欺の手口による金銭要求
- ワンクリック請求等の不当請求による金銭被害

だましの手口は常に更新されています。
最新の情報をチェックして、警戒をおこたらないことが大切です。

※3：SMS…ショートメッセージサービス

「闇バイト」募集から実行までの手口

ココが危ない!! 闇バイト

犯罪行為の実行要員を募る「闇バイト」。収入を得るつもりが、犯罪に手を染めてしまう結果とならないよう、注意したいポイントを紹介します。

ちょっと待った!

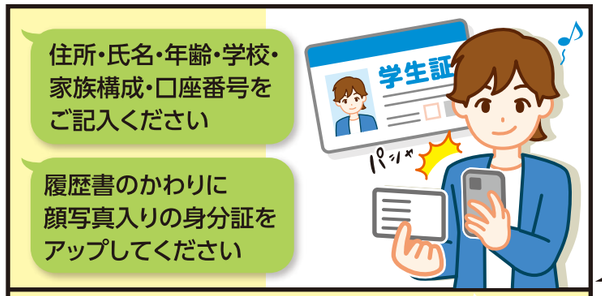
簡単で高収入! そんな仕事はありません!

甘い言葉の裏には何かがあると考えましょう。また、やさしい文章で応募を誘いながら、仕事内容はわかりづらくしてあるのもポイントです。投稿者（リクルーター）と直接コンタクトを取って詳細を聞く流れへと誘導するのです。

ちょっと待った!

あやしい求人には、興味本位で応募しない!

自分から応募しなくても、X（旧Twitter）やInstagramなどのSNSを経由してメッセージが送られてくることがありますが、興味本位にアクセスするだけでもリスクが高まります。連絡をとってしまうと、その後は匿名性が高いメッセージアプリに誘導されてやりとりが始まり、応募のためとして個人情報を要求されます。



ちょっと待った!

学生証や身分証、顔写真を送るよう要求されたらやりとりは終了!

面接もなく、早い段階で免許証や学生証等、顔写真のデータを送るよう指示されたら、まず詐欺を疑いましょう。うっかり問い合わせてしまっても、ここで気づけばまだ引き返せます。

ちょっと待った!

詐欺や犯罪へ加担するように強要されたら、そこで立ち止まり、相談を!

応募したもののやめたくなったとしても、逃れられない状況へ追い込むのが犯罪者の手口です。「家に押しかける」「親族に危害を与える」などと脅されたり、実際に個人情報をアップされてしまう事例もあります。困った状況になったら、周囲の大人や警察、または相談機関などに迷わず助けを求めましょう。

ちょっと待った!

犯罪者集団にとって、闇バイトの応募者は「使い捨ての駒」

闇バイトの代表的な役割として、受け子（被害者から金銭やカードを受け取る）、出し子（口座から現金を引き出す）、かけ子（被害者に電話をかけて被害者をだます）、などがあります。「指示に従っているだけ」と犯罪に加担しているという意識が薄れたり、「逮捕されるまでやめられない」などの悪循環に陥ってしまいます。

ちょっと待った!

「闇バイト」の実態は、犯罪実行者の募集! 絶対に応募してはいけません!

- 「高額報酬」「即金」「書類を受け取るだけ」など、一見好条件ながら業務内容が不明確な求人情報は危ない
- 募集情報に「受け子」「出し子」「運び」等の隠語が使用されていたり、匿名性の高いアプリでの連絡が求められたりする場合は犯罪に関わる危険性が大

特殊詐欺は詐欺の中でも特に悪質性が高い犯罪のため、たとえ一回「受け子」をしただけでも共犯者として詐欺罪・窃盗罪の容疑で逮捕・起訴され、初犯でも実刑判決は免れません。

詐欺罪	10年以下の懲役
窃盗罪	10年以下の懲役または50万円以下の罰金
強盗罪	5年以上の懲役

さらに、被害者への損害賠償が求められます

相談先はこちら

- 警察相談専用電話　#9110
- 都道府県警察の少年相談窓口（警察庁HP）
  https://www.npa.go.jp/bureau/safetylife/syonen/soudan.html

SNSで実行犯を募集する手口による強盗や特殊詐欺の

「被害者」にも「加害者」にもならないために、知っておきたいこと

「被害者」にならないために

1 「私は大丈夫」と思わず「狙われない」ための心がけを!

- SNSに過度に個人情報を載せない
  特に高級車やブランド品などで「お金持ち」をPRしない
- 住所、家族構成、旅行の情報などが特定できる写真は掲載しない
- 自宅にかかってくる電話で個人情報を聞かれても話さない
- 家族、友人以外の訪問者はインターホンでのみ対応する
- 宅配の荷物は宅配ボックスや「置き配」を活用

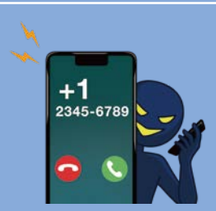
2 犯人からの電話を受けずにすむ設定を!

- 固定電話を常に留守番電話設定にして、直接電話には出ない
- 自動通話録音警告機器、防犯機能付きの電話機を導入する
- 自分から「○○です」と名乗らない

Point

国際電話番号を利用した特殊詐欺が急増しています。
知らない「国際電話番号」からの電話には、出ない・かけ直さないこと

国際電話不取扱受付センター（連絡先0120-210-364）に申し込めば、固定電話・ひかり電話を対象に国際電話番号からの発着信を無償で休止できます。



不審な電話を受けたら

警察相談専用電話 #9110 に相談を

「加害者」にならないために

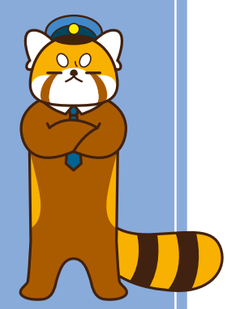
1 「そんなつもりじゃなかった」とならないよう慎重に行動する、情報弱者にならない

近年、特殊詐欺グループは拠点を海外に移しています。東南アジアを中心に、「コールセンターで月収100万円」「海リゾート・短期・高収入」「簡単な翻訳作業」などの甘い言葉に誘われて、海外で「かけ子」として犯罪に加担させられたり、組織内のトラブルにより暴行を受ける、加害者として現地警察に拘束されるなどのケースが多発しています。短期間で簡単に高収入を得られる「おいしい仕事」は日本だけでなく海外でもあり得ません!

Point

「闇バイト」は「高収入」どころか「人生台無し」、法律や社会のルールに反した違法な行為です

「危険を冒して次々と犯罪を実行したにもかかわらず、一切の報酬が支払われなかった」「警察に密告された結果、逮捕されてしまった」といった事例に見られるように、犯行グループは約束の報酬を元から支払うつもりはなく、少年を都合よく利用した後、簡単に「捨て駒」として切り捨てます。
たった一度でも手を染めれば最後には必ず警察に検挙されます。なぜなら、脅し等により、警察に逮捕されるまで使われ続けるからです。関わって得られるものは何もありません。
また、犯罪によって被害者やその家族に一生消えることのない深い傷を与えることとなり、他人の人生も台無しにするのです。



2 危ない目に遭いそうになったら積極的に相談!

あやしい情報に出遭った場合は、ぜひ公的機関や相談窓口に情報を提供しましょう。万が一、関わってしまった場合でも立ち止まり警察などに相談することで、新たな被害者を生まないことにつながります。

相談先はこちら

- 都道府県警察の少年相談窓口（警察庁HP）
- 政府広報オンライン 匿名通報ダイヤル 0120-924-839
- 警察が委託を行っている通報先 インターネット・ホットラインセンター（IHC）
- 警察相談専用電話 #9110

「ランサムウェア」誰もが攻撃の対象に!

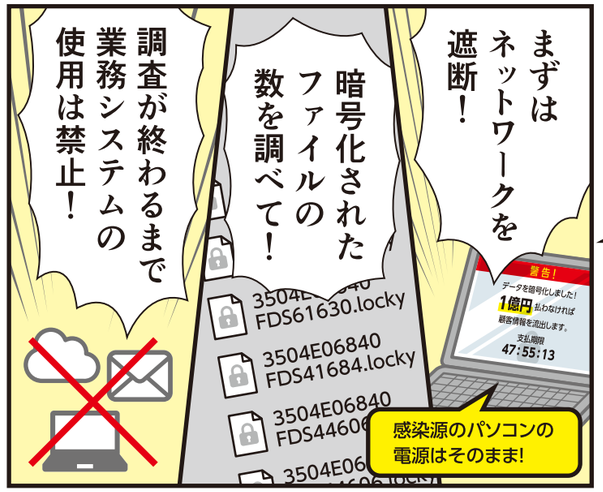
ココが危ない!! ランサムウェア

データや機器を人質に身代金を要求する「ランサムウェア」の被害が深刻です。企業や組織だけでなく、個人一人ひとりが最新の動向を知り、対策を意識することが大切です。

ちょっと待った!

特定の企業・団体等の 規模を問わず被害が発生!

攻撃者は、顧客や経理情報、商品のデータなどを暗号化して使用できなくしたのち、元に戻すことと引き換えに身代金を要求してきます。さらに近年は、データの暗号化に対する身代金に加えて、「金銭を支払わなければデータを公開する」などと要求する「二重恐喝」の被害やデータの暗号化を省略し、窃取した情報の公開への対価を要求する「ノーウェアランサム」が増えています。



ちょっと待った!

慌てず、まずは感染した機器を ネットワークから遮断

他のコンピュータへの被害の拡散を防ぐために、ランサムウェアの感染を確認したら、ただちにLANケーブルを抜くなど、コンピュータを社内ネットワークやインターネットから切断してください。

ちょっと待った!

身代金は支払わず、 警察や専門機関へ相談

身代金の支払いはビットコインなどの暗号資産で要求されることが多く、たとえ支払ったとしてもデータが復旧できるとは限らず、さらなる脅迫につながる恐れもあります。ランサムウェアの被害に遭った場合は、保存した通信ログ等を持参して、最寄りの警察署またはサイバー犯罪相談窓口に通報・相談してください。

相談先はこちら ■サイバー犯罪相談窓口

ちょっと待った!

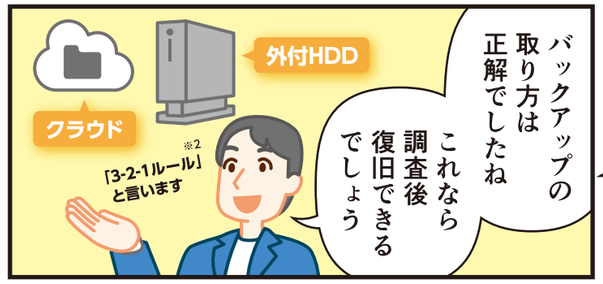
初動対応が大切! 種別特定、侵入原因を調査

一般的な復旧までの流れは、ランサムウェアの種別や侵入経路を特定したら、セキュリティソフトやウイルス駆除ツールで除去、データ復元となります。ランサムウェアの特定とデータの復元は、ウェブサイト「No More Ransom」(11頁参照) を利用することで可能な場合があります。

不正な侵入、情報の漏洩…VPN機器を狙った攻撃が増加!

VPN機器の脆弱性とは、VPN接続を実現する機器のOSやソフトウェアにおける欠陥や弱点のことで、機器本体やOSが古かったり適切な接続がされていなかったりすると、サイバー攻撃に遭う可能性があります。多くの場合はメーカーが公開するアップデートを機器に適用することで解決できます。

※1：VPN (Virtual Private Network 仮想専用通信網) …インターネット上で安全な通信を実現するための技術

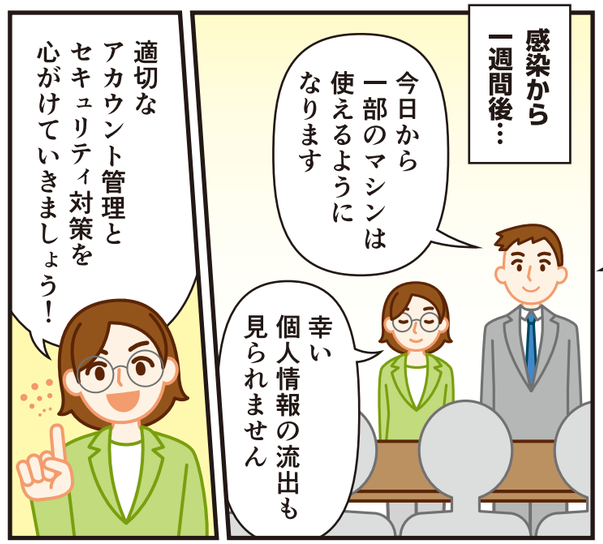


ちょっと待った!

バックアップは 複数の媒体に、が基本

感染前のデータのバックアップがあれば、暗号化されたデータを復旧できます。外付けデバイスやクラウドストレージ上など複数の媒体に、定期的にバックアップを作成しておく対策を日頃から行いましょう。

※2：3-2-1ルール…「データを3つ作成」して「2つの異なるメディアで保存」し、「1つは別の場所で保管」します。



ちょっと待った!

復旧後も常に警戒を! セキュリティ意識を 底上げしていくことが大切

- ■ネットワーク担当者だけでなく、社員一人ひとりがセキュリティを意識する
- ■信頼できるアンチウイルスソフトを導入する
- ■OSやソフトウェア・VPNを常に最新の状態にしておく
- ■ネットワーク監視のセキュリティを導入する
- ■インシデント対応計画を策定しておく
- ■認証方法の強化

ランサムウェアに感染すると?

端末やデータが使用できないだけでなく、さまざまな被害が引き起こされる可能性があります。

基幹システムが使えなくなり、業務停止に追い込まれる	取引先やグループ企業にも支障をきたす	機密情報の抜き取り・漏洩、個人情報の流出により社会的な信頼を失墜	調査や復旧にかかる費用、多額の賠償金が発生する

ランサムウェアの脅威に負けない!

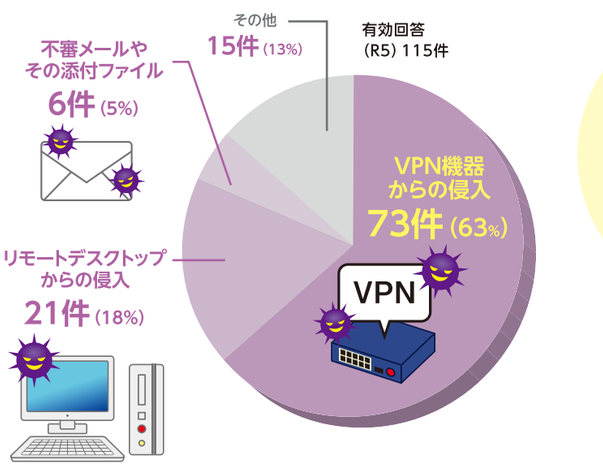
インターネット・SNSを安全に利用していくために知っておきたいこと

「私には関係ない」「自分は大丈夫」ではありません

1 攻撃者はセキュリティの「穴」を探索し、脆弱性を突いてくる!

以前は、メールやウェブサイトを狙う犯行が一般的でしたが、最近はリモートワークの普及に伴い、「VPN機器」や「リモートデスクトップ」の脆弱性をついた攻撃が増加しています。
修正プログラム（パッチ）の適用やシステムのアップデートといった対策とともに、定期的な見直しや検討を行い、セキュリティの体制を整備しておくことが必要です。

ランサムウェアの代表的な感染経路



参考文献：警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」
企業・団体等におけるランサムウェア被害の実態　図表25：感染経路
注：図中の割合は小数第1位以下を四捨五入しているため、
総数が必ずしも100にならない。

ランサムウェアは、
ハードディスクやファイルを
暗号化し、端末等に
ダメージを与える
「マルウェア（悪意がある
不正なソフトウェア）」の
一種です

病院、スーパー、
大手ゲーム会社など
身近な企業が次々と
VPN機器経由で
被害にあっています

Check

ランサムウェアの攻撃を受けると、個人への影響も無視できない状況に…!

個人にも直接影響を与えることが想定される被害リスクは、次のようなものがあります。

システム障害の発生により
- オンライン上サービスの遅延・使用停止
- 物流がストップしてしまう　など

個人情報の流出により
- アカウントの乗っ取り、なりすまし、クレジットカードの不正利用
- 新たなサイバー攻撃の踏み台にされる　など

2 普段からセキュリティ意識を持ち ルールを守って安心・安全に利用することが重要

ランサムウェアをはじめ、金銭や情報の窃取を目的としたサイバー犯罪はあとを絶ちません。また、個人による情報持ち出し、メールの誤送信などのヒューマンエラーによる事故も多く、あらためて基本的な対策を徹底することが重要です。

独立行政法人
情報処理推進機構（IPA）選出　**情報セキュリティ10大脅威 2024**「組織」向け脅威

- 1位 ランサムウェアによる被害
- 2位 サプライチェーンの弱点を悪用した攻撃
- 3位 内部不正による情報漏えい等の被害
- 4位 標的型攻撃による機密情報の窃取
- 5位 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
- 6位 不注意による情報漏えい等の被害
- 7位 脆弱性対策情報の公開に伴う悪用増加
- 8位 ビジネスメール詐欺による金銭被害
- 9位 テレワーク等のニューノーマルな働き方を狙った攻撃
- 10位 犯罪のビジネス化（アンダーグラウンドサービス）

Check

あらゆるセキュリティの脅威に対し共通していることは「基本の対策をしっかり行うこと」です。
基本に従い、普段からセキュリティ意識を高めましょう。

- ■不審なメールやウェブサイトは開かない
- ■信頼できないソフトウェアをインストールしない
- ■パスワードは適切に設定・管理する
- ■セキュリティに関する情報を常に入手し、リテラシーを高める

相談先はこちら

IPA 情報セキュリティ安心相談窓口
主にウイルスや不正アクセスに関するアドバイスを提供する窓口

No More Ransom プロジェクト
ランサムウェアに関する情報や復号ツールが入手できます

警察庁 サイバー事案に関する相談窓口
都道府県警察の連絡先、警察署一覧へのリンクもあります

インターネット・ホットラインセンター（IHC）
インターネット利用者の通報窓口