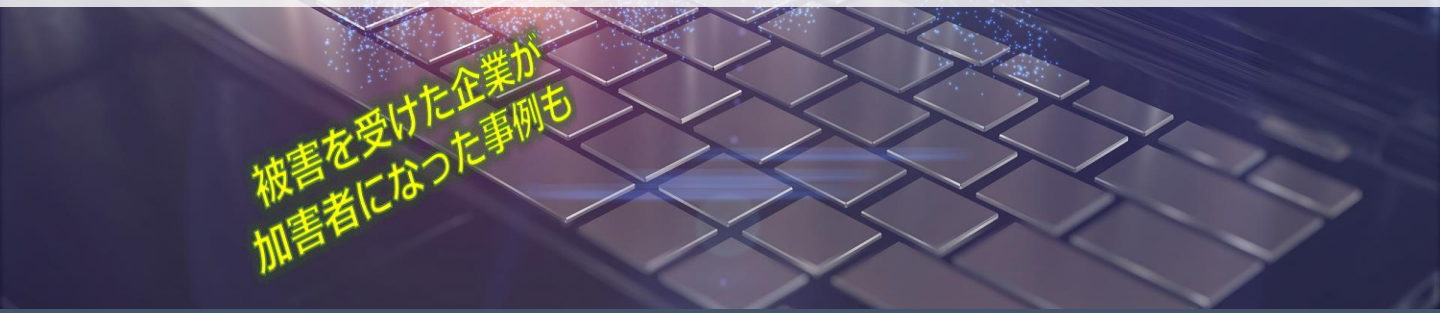
2025年

Cyber Security News

1 月号

先月の報道を中心に、サイバーセキュリティに関してのニュースを抜粋してお届けしています

2024年のセキュリティニュースを振り返る



サイバー攻撃代行業使い、DDoS攻撃関与の疑いで日本の中学生が書類送検

サイバー攻撃の代行サービス使い企業攻撃か 中学生が書類送検

2024年12月11日、警察庁はEUROPOL主導で進められているDDoS攻撃に対する国際共同捜査（OPERATION PowerOFF）より、サービス利用が特定された関係者に日本人が含まれており、3名を摘発したことを公表しました。

サイバー攻撃を代行する海外のネットサービスを使って企業などのウェブサイトにサイバー攻撃を仕掛けたなどとして、中学生2人が書類送検や児童相談所への通告をされていたことが警察庁への取材で分かりました。世界各国では、こうしたネットサービスを利用した人が300人以上いることも分かり、警察庁などが注意を呼びかけています。

また、京都でも2024年11月に1回わずか1.5万円で「DDoS攻撃」を海外の代行業者に依頼した事件で犯人が検挙されており、サイバーの専門的知識がなくても安易に攻撃に踏み切る犯罪が横行し始めています。

国際共同捜査により閉鎖されたサイバー攻撃の代行サイト

摘発された日本人	警察の対応
男	電子計算機損壊等業務妨害の容疑で2024年8月6日にサイバー特別捜査部が逮捕。
少年A	関係都道府県警察が電子計算機損壊等業務妨害未遂の容疑で書類送検。
少年B	児童相談所へ通告。

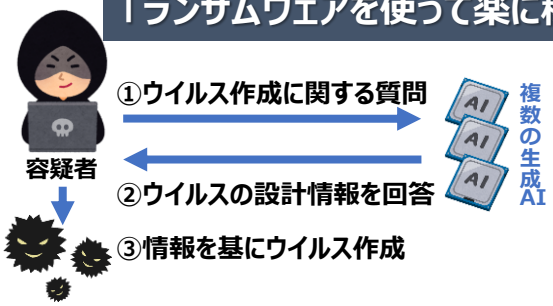
※各種NEWS素材及び各企業のHP掲載内容から抜粋。公表された情報を基に掲載しており、特定の企業を誹謗中傷するものではありません。

「初心者でも扱える安価なランサムウェア」がダークウェブで大量に出回っている

セキュリティ企業「Sophos」の調査では**「初心者でも扱える安価なランサムウェア」が大量に出回っていることが明らか**になっています。
ランサムウェアを用いた攻撃では、**「ランサムウェアの開発者が攻撃も実行する」**というパターンと、**「別の開発者からランサムウェアを購入して攻撃を実行する」**というパターンがあり、近年の主流は「ランサムウェア攻撃で入手した身代金の一部を料金として支払う」という**「Ransomware as a Service Explained （RaaS）」**という販売形態が広がりつつあります。
「Junk gun」と名付けられた安価なランサムウェアは、その安さから脅威アクターの参入障壁を引き下げ、**ランサムウェア攻撃の増加に寄与する**と懸念されており、**中小企業のみならず**、インターネットを活用する個人にも注意が呼びかけられています。

参照元：https://news.sophos.com/en-us/2024/04/17/junk-gun-ransomware-peashooters-can-still-pack-a-punch/

「ランサムウェアを使って楽に稼ぎたかった」生成AIでウイルス作成容疑の男を逮捕

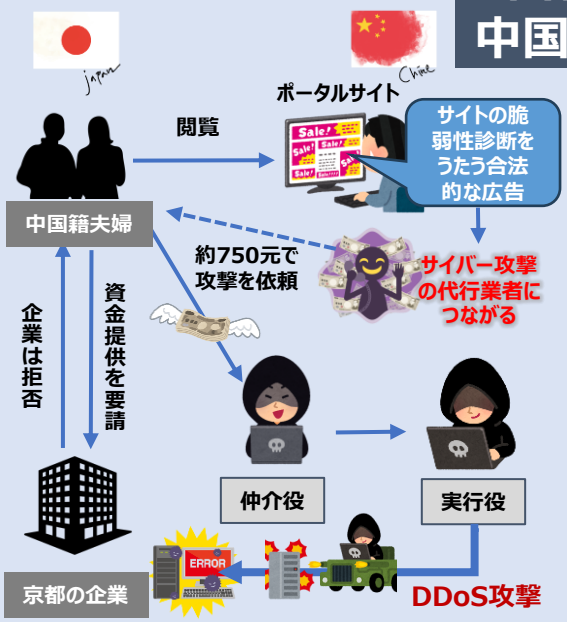


2024年5月27日、生成AIを悪用してランサムウェアを作成したとして警視庁サイバー犯罪対策課が男性を逮捕しましたが、**同容疑者は**元工場作業員で**専門的な知識はなく、ウイルス作成方法を生成AIから聞き出し**、質問の仕方などは**ネット上で情報を得て**いたとのことです。「ランサムウェアを使って楽に稼ぎたいと思っていた」「AIを使えばできると思った」などと供述していました。

また報道によると2024年10月1日には、東京地裁において論告求刑公判が行われ、この男性には**懲役4年が求刑**されています。

代行「DDoS攻撃」事件の構図

1回わずか1.5万円で「DDoS攻撃」中国籍夫婦が悪用した「攻撃代行業者」の実態



最近、DDoS攻撃を代行業者に依頼する犯罪が増加しています。**専門知識がなくても攻撃が可能**で、被害企業はサービス停止や信頼低下のリスクに直面します。

京都では、中国籍の夫婦がスポーツジムの検索サイトに攻撃を行い、1回の攻撃に**約750元（約1万5千円）を支払って**いたとして逮捕されました。攻撃を受けたサイトは10回程度の攻撃を受け、そのたびにサイトが閲覧できない状態が続き、アクセス数が減ったり、広告の契約が解除されたりし、**経済的損失を被っています**。容疑者は、以前その会社で就業体験をしており、業務提携を断られた後に攻撃を開始したとされています。また容疑者は中国の広告を見て**代行業者に依頼**しており、実行役は中国にいるとみられます。DDoS攻撃の代行業者は**世界的に増加**しており、日本の警察当局は海外の捜査機関と連携して実態解明を進めています。サイバー犯罪の専門家によると、ランサムウェアを提供する事業者も存在し、**秘匿性の高いメッセージアプリや暗号資産の普及が摘発を困難**にしています。

海外に“サイバー攻撃依頼”した男を逮捕 「セキュリティの弱そうな中小企業を狙った」と供述

サーバーに大量のデータを送りつけ機能を停止させる「DDoS（ディードス）攻撃」を東京都内の企業に実施したとして、警察庁サイバー特別捜査部は、配管工の男（25）を逮捕しました。男は「ブーター(Booter)」と呼ばれる海外の代行サイトにサイバー攻撃を依頼しており、専門知識がなくても攻撃可能で、リスクの高まりが浮き彫りになっています。
代行業者は「Bootyou（ブートユー）」（閉鎖）というサイトで客を募り、月額4・99ドルから99・99ドルでDDoS攻撃を請け負っていました。高額のプランほど攻撃の時間が長くなる仕組みで、男は月額10ドル程度の契約をしていたという事です。

ビジネス化するサイバー攻撃 「代行業」暗躍で高まる脅威

参照元：日経新聞、読売新聞、時事通信他
https://www.nikkei.com/article/DGXZQOUE055960V00C24A8000000/

代行サイトを使ったサイバー攻撃のイメージ

中小企業が保有する個人情報の具体例と保有率

企業が保有している個人情報は主に下記の通りですが、77%の企業が報告義務を認知していない？

保有する個人情報の内容（複数回答可）※従業員情報は除く。

全体	氏名	生年月日	性別	住所	電話番号	クレジットカード情報	銀行口座情報	メールアドレス	パスワード
アンケート回答数	84.5%	43.9%	53.4%	74.0%	79.1%	2.4%	20.0%	28.4%	1.8%
(3,821者)	(3,230者)	(1,678者)	(2,039者)	(2,827者)	(3,023者)	(92者)	(764者)	(1,086者)	(69者)

パスポート番号	マイナンバー	免許証番号	販売履歴	HP等の閲覧履歴	健康状態（健康診断情報を含む）	病歴	顔画像	その他	無回答
1.1%	13.1%	6.8%	13.8%	0.9%	12.2%	8.5%	5.6%	2.8%	10.2%
(42者)	(500者)	(260者)	(526者)	(33者)	(468者)	(326者)	(213者)	(108者)	(388者)

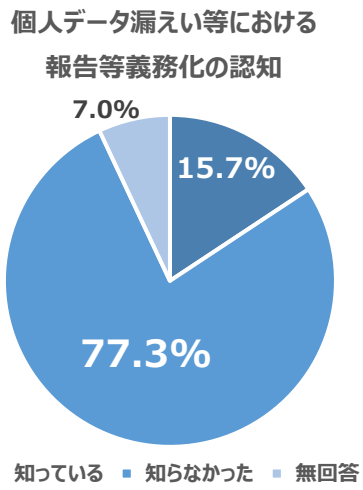
中小事業者の4割が個人情報の取り扱い「わからない」と回答…

中小規模事業者（従業員数100名以下）における個人情報等の安全管理措置に関する実態調査

個人情報保護委員会が11月29日発表した「中小規模事業者における個人情報等の安全管理措置に関する実態調査」の結果によると、中小事業者の4割が個人情報の取り扱いで「何をしてよいかわからない」と回答しています。

・調査対象事業者
国内に本社を置く民間の中小規模事業者から無作為に抽出した 17,000 事業者
・調査実施期間
2024年5月16日～6月28日
・回収数・回収率
発送数：17,000 件
有効回収数：3,821 件
回収率：22.5%

参照元：https://www.ppc.go.jp/news/surveillance/



個人情報の課題に関する回答（複数回答可）

全体	何をしてよいか分からない	個人情報保護等の理解不足	社内・団体内規定が不足	従業員の教育	情報セキュリティー対策	個人情報保護のための資金不足	個人情報保護のための人材不足	電子化による管理の難易度上昇	その他	無回答
	40.0%	26.9%	11.8%	14.5%	18.9%	9.2%	8.9%	17.2%	4.1%	17.7%
3,821	1,530	1,029	452	555	723	352	340	658	157	675

大阪・関西万博でリスク増加

OSAKA, KANSAI, JAPAN EXPO 2025
ぜんぶのいのちと、
ワクワクする未来へ。

2025年は、**大阪・関西万博**が開かれ、関西や大阪が世界的に有名になり、名前を売ろうとするグループが、サイバー攻撃を仕掛ける可能性が高まると懸念されています。かつて日本政府を狙ったサイバー攻撃のキャンペーンでは「霞が関」と似た名前の霞ヶ浦河川事務所（茨城県）のホームページが攻撃された事例もあり、今回も会社名に**「大阪」「関西」**が付いているだけで狙われることも考えらます。**万博と全く関係がなくても**、関西,大阪にゆかりのある企業は、「**攻撃されるかもしれない**」とこれまで以上に注意が必要となります。

中小企業の20%の経営層は「自社はサイバー攻撃に遭わない」と信じている

バラクーダネットワークスジャパンは、市場レポート「日本の中小企業におけるサイバーレジリエンスVol. 2：『人』がセキュリティの成功の鍵を握る」を発行しました。それによると**72%が「ランサムウェア攻撃を防ぐ自信がない」と回答しています。**

- 20% 経営幹部は自社が攻撃されることはないと信じている
- 28% ランサムウェア攻撃を防ぐ自信がある
- 22% サイバーセキュリティを担当する専任のスタッフがいない
- 23% データを安全に復元・復旧するためにオフラインなどの変更不可なバックアップを利用している
- 47% サイバーセキュリティ戦略を社内で策定している

参照元：https://www.barracuda.co.jp/news/pressrelease-241218/

2024年に発生した主な情報漏洩事件

公開日	社名	業種	流出件数	概要
2024/12/09	株式会社三恵	下着通販サイト	約30万件	サイバー攻撃：カード情報や登録個人情報
2024/11/29	ライクキッズ株式会社	保育園・学童	約15万8千人分	ランサムウェア感染：園児や保護者の情報
2024/10/30	株式会社カレルチャペック	小売店	103,289名	サイバー攻撃：ユーザーの個人情報など
2024/10/16	八十二銀行	金融	106,352件	業務提携契約先社員が派遣元に情報送付
2024/09/19	株式会社LIFULL	不動産	217,953名分	サイバー攻撃：LIFULL HOME'S情報 他
2024/09/19	松竹株式会社	エンターテインメント	23万名分	委託先企業のランサムウエア感染
2024/09/17	パーソルキャリア株式会社	人材派遣	549,195名	設計不備：法人顧客情報の担当者情報
2024/08/28	サノフィ株式会社	医薬品販売	735,210 名分	サイバー攻撃：医療機関名、役職、職種 他
2024/08/20	愛知県豊田市	地方自治体	14万8千人	委託先企業のランサムウエア感染
2024/08/20	公文教育研究会：KUMON	学習塾	739,000人分	委託先企業のランサムウェア感染
2024/08/19	愛媛銀行	金融	25万4659者分	委託先企業のランサムウェア感染
2024/08/07	長崎県物産振興協会	一般団体	139,190名分	通販サイトへのサイバー攻撃：ユーザー情報
2024/08/05	三菱電機ホーム機器株式会社	製造業	231万名分	子会社へのサイバー攻撃：ユーザー情報
2024/08/05	株式会社ドワンゴ:KADOKAWA	IT関連企業	254,241名分	ランサムウェア感染：取引先個人情報他
2024/07/30	和歌山県和歌山市	地方自治体	151,421件	委託先企業のランサムウェア感染
2024/07/30	ウォンテッドリー株式会社	IT関連企業	419,746件	設定不備：登録ユーザーの個人情報
2024/07/17	東京ガス株式会社	都市ガス	約416万人分	子会社へのサイバー攻撃：法人の個人情報
2024/06/10	ニデックインスツルメンツ株式会社	製造業	402,530件	ランサムウェア感染：取引先に関する情報
2024/06/06	徳島県徳島市	自治体	200,079件	委託先企業のランサムウェア感染
2024/05/24	株式会社ネクストレベル	プラットフォームサービス	496,119件	サイバー攻撃：登録されているID etc
2024/05/24	積水ハウス株式会社	住宅	828,168名分	サイバー攻撃：お客様と従業員等情報
2024/05/13	株式会社バイオフィリア	ペットフード製造業	226,437件	サイバー攻撃：ユーザーの個人情報
2024/05/09	株式会社イズミ	小売業	7,784,999件	ランサムウェア感染：会員情報の一部
2024/03/29	ワークスタイルテック株式会社	ソフトウェア開発	162,830名分	設定不備：ユーザーの個人情報
2024/02/14	LINEヤフー株式会社	ITサービス	519,506件	サイバー攻撃：ユーザーに関する情報
2024/01/26	株式会社大藤つり具	小売業	約200,000件	ランサムウェア感染、ユーザーの個人情報

※報道・公表された情報から、一部を抜粋しております。件数や人員数は公表時点で漏洩の可能性のあった件数となります。

※各種NEWS素材及び各企業のHP掲載内容から抜粋。公表された情報を基に掲載しており、特定の企業を誹謗中傷するものではありません。