

暴露型ランサムウェア攻撃統計

CIGマンスリーレポート 2026年6月号 Rev 1.00
(2026年5月分)

2026

5

目次

総括と監視対象 (レポート①～④)

今月のハイライト	p.3
ランサムウェア関連記事 今月のピックアップ	p.4
監視中のランサムウェア攻撃グループ情報 (拠点数と一覧)	p.5
監視中のランサムウェア攻撃グループ情報 (ランサムウェア使用の割合)	p.6

グローバル統計 (レポート⑤～⑱)

年間統計 (全世界)	p.7～8
攻撃グループTOP10 (全世界)	p.9～12
被害国TOP10 (全世界)	p.13～16
被害国TOP10 (アジア)	p.17～20
業種TOP10 (全世界)	p.21～24

日本関連組織を対象とした統計 (レポート⑲～㉓)

被害数の推移に関する統計 (全世界及び国内)	p.25～26
資本金別の統計 (国内)	p.27～28
公表と暴露に関する統計 (国内)	p.29～30
公となった国内被害組織 概要一覧	p.31～33
公となった国内被害組織における拠点割合	p.34
公となった国内被害組織における業種割合	p.35

中小企業における被害分析 (レポート㉔～㉗)

資本金別 (中小企業)	p.37
公となった国内被害組織における業種割合 (中小企業)	p.38
公となった国内被害組織における拠点割合 (中小企業)	p.39
公となった国内被害組織 概要一覧 (中小企業)	p.40～41

多重被害に関する分析 (レポート㉘～㉙)

繰り返し暴露された事案数の集計と 攻撃グループ間の関係	p.43
多重被害に遭った被害組織の傾向と分析	p.44

業種に関する分析 (レポート㉚)

業種に関する分析 - 製造	p.46
業種に関する分析 - サービス	p.47
業種に関する分析 - 情報通信	p.48
業種に関する分析 - 建設・建築	p.49
業種に関する分析 - 医療	p.50
業種に関する分析 - 卸売・小売	p.51
業種に関する分析 - 金融・保険	p.52
業種に関する分析 - 法律	p.53
業種に関する分析 - 教育	p.54
業種に関する分析 - 運輸	p.55

その他

CIGのコンテンツ紹介	p.56
本資料に関する留意事項及び二次利用について	p.57

総括と監視対象

2026

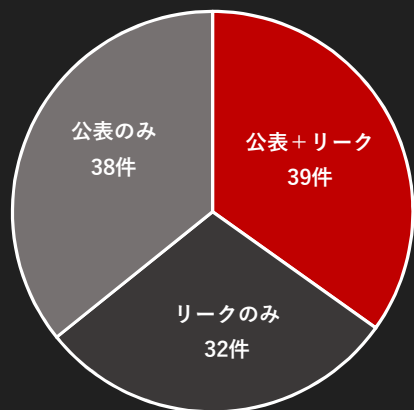
5

今月のハイライト

● 公表情報とリーク情報から読み解く、公表の実態とリークサイト掲載までの猶予

暴露型ランサムウェア攻撃の被害は、被害組織による公表と、攻撃者によるリークサイトへの掲載という二つの経路で表面化する。本分析では、2026年1月～5月の国内被害109件の公表・掲載状況を整理したうえで、公表およびリークのある全39件を対象に、両者の先後関係、攻撃グループ別の掲載傾向、認知からリークサイト掲載までの所要日数を順に分析し、リークサイト掲載までの猶予を明らかにする。

① 日本関連組織の被害公表・リーク掲載状況



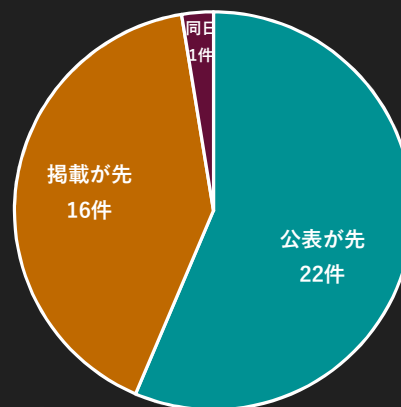
※ 対象:2026年1月～5月の国内被害 109件

2026年1月～5月、国内組織のランサムウェア被害として公表またはリークサイトへの掲載が確認された件数は計109件であった。

このうち約7割(77件)は被害組織が公表した事案で、その約半数の39件は攻撃グループのリークサイトにも掲載されていた。公表のみの38件には、暗号化のみの攻撃や、対外的インパクトを基準とした選別・重要インフラ等を意図的に非掲載とするグループの方針等が含まれる。

本分析では、公表・リークサイト掲載の双方が確認された39件を対象とする。

② 被害公表とリークの先後関係



※ 対象:公表とリークが存在する全39件

公表とリーク双方がある39件について先後関係を調べると、公表が先行するケースがやや多いものの、リークサイトへの掲載が先行する例も約41%にのぼり、先後に明確な偏りは見られない。

被害の早期公表は、流出情報を悪用した詐欺・なりすまし等の二次被害の防止や、関係先への説明責任を果たすうえで有効と言える。一方で、調査の途上で公表する場合、その後の進展により公表内容と異なる事実が判明するリスクも伴う。

こうした利点とリスクの両面を踏まえ、各組織が個別の状況に応じて最善の対応を模索しているのが実情といえる。

③ 対象事案における攻撃グループ別掲載件数

日本関連組織としては The Gentlemen と Qilin、SAFEPAY による被害が顕著

攻撃グループ	掲載件数
The Gentlemen	9件
Qilin (Agenda)	6件
SAFEPAY	5件
その他	計19件

※ 対象:公表とリークのある全39件

公表とリーク双方がある39件のうち、掲載が1～2件程度にとどまるグループがある一方で、The Gentlemen (9件)とQilin (6件)、SAFEPAY (5件)の掲載が目立つ。上位3グループで全体の半数超を占め、特定グループへの集中傾向が見られる。

④ 事案認知から掲載までの所要日数

攻撃グループ	平均	最短	最長	件数
全体	21.0	0	113	35
The Gentlemen	8.6	3	16	8
Qilin (Agenda)	20.7	5	35	6
SAFEPAY	37.0	33	41	4

※ 対象:公表に認知日が記載されている35件

事案認知日が公表されている35件について、公表上の認知日からリークサイトで確認した掲載日までの所要日数を調査した。

主要な3グループに着目すると、The Gentlemenで約9日、Qilinで約21日、SAFEPAYで約37日と日数にばらつきが見られる。

全35事案の平均は約21日にすぎず、中には数日以内の掲載事例も存在する。

リークサイトへの掲載により、侵害の事実が外部に明らかになるほか、窃取データが公開された際にはその分析も必要となる。事案の認知からリークサイト掲載までは平均で約21日にすぎず、約半数(18件)は2週間以内、中には数日以内で掲載された事例もある。平時からの備えと対応計画の事前整備の重要性が改めて示された。

【The Gentlemenランサムウェア：防御回避TTPの分析】 (出典: Huntress 2026/05/21)

Huntress社が、ランサムウェアグループ「The Gentlemen」による2つの被害事例を分析。スケジュールタスクとPowerShellを使い、Defenderの無効化や除外設定の追加、イベントログの消去等の防御回避が確認。
<https://www.huntress.com/blog/the-gentlemen-ransomware-defense-evasion-ttps>

【ランサムウェア攻撃者に悪用された「First VPN Service」】 (出典: FBI / IC3 2026/05/21)

FBIが犯罪者向けVPN「First VPN Service」のテイクダウンについて公表。Avaddonなど25以上のランサムウェアが偵察・侵入・DDoSに悪用していたとし、IOCとMITRE ATT&CKに基づくTTPおよび対策を示した。
<https://www.ic3.gov/CSA/2026/260521.pdf>

【データベースの身代金用ウォレットのうち、実際に支払いが行われたのはわずか38%】 (出典: Ransomnews.com 2026/05/26)

Ransomnews Research Teamは、過去5年分の調査をもとに、公開データベースを狙った自動化型の身代金要求・消去攻撃の実態を報告。支払いが確認されたのは追跡可能なウォレットの約38%にとどまる。
<https://ransomnews.com/database-ransom-economics-2026/>

【Silent Ransom Group：IT担当者を装うソーシャルエンジニアリング型恐喝手口】 (出典: FBI / IC3 2026/05/26)

FBIはSilent Ransom Group (別称Luna Moth等) が法律事務所を狙い、IT担当者を装った電話・メールに加えて、物理的に現地訪問して端末へストレージを挿入しデータ窃取を試みる手口を警告。
<https://www.ic3.gov/CSA/2026/260526.pdf>

【ランサムウェア攻撃グループ「The Gentlemen」の内部チャットログから見えた攻撃の実態】 (出典: 三井物産セキュアディレクション 2026/05/26)

ランサムウェアグループThe Gentlemenの内部チャットログとみられるデータが流出。標的選定、侵入経路、内部探索と横展開、データの窃取・暗号化、バックアップ妨害など、攻撃手口が記録されている。
<https://www.mbsd.jp/research/20260526/the-gentlemen/>

【VECT：自身のツールでも復号できないランサムウェア】 (出典: Morphisec 2026/06/04)

Morphisec社がVECT 2.0ランサムウェアのWindows版について実装上の欠陥を複数報告。ファイルがリネームのみ・部分暗号化・不整合・損傷等の状態になり、攻撃者自身のデクリプタでも復旧困難になると指摘。
<https://www.morphisec.com/blog/vect-ransomware-that-cant-decrypt/>

【CISA、ゼロデイ悪用されたCheck Point VPN脆弱性について連邦機関に3日以内の対処を命令】 (出典: Bleeping Computer 2026/06/09)

米CISAは、Check Point VPNの認証バイパス脆弱性CVE-2026-50751をKEVカタログに追加し、連邦政府機関に3日以内の対処を命じた。同脆弱性はQilinランサムウェア関連アクターによるゼロデイ悪用が報告。
<https://www.bleepingcomputer.com/news/security/cisa-orders-feds-to-patch-check-point-flaw-exploited-by-ransomware-gangs/>

【ランサムウェア集団「The Gentlemen」を運営しているのは誰か?】 (出典: KrebsOnSecurity 2026/06/10)

KrebsOnSecurityは、「The Gentlemen」の管理者について、OSINTの突き合わせでロシア在住とみられる人物に結びつく手掛かりを示した。さらに、PRODAFT社も高い確信度で裏づけたと追記。
<https://krebsonsecurity.com/2026/06/who-runs-the-ransomware-group-the-gentlemen/>

【ランサムウェア犯が使う暗号資産洗浄サービス『AudiA6』を欧州警察主導で摘発 (3.36億ユーロ規模)】 (出典: Europol 2026/06/11)

Europol主導の国際捜査が、ランサムウェア攻撃者らに利用された暗号資産洗浄サービス「AudiA6」を摘発したと発表。3億3,600万ユーロ超を洗浄し、ウクライナ・ロシア籍の管理者2名がジョージアで逮捕された。
<https://www.europol.europa.eu/media-press/newsroom/news/ransomware-gangs-cut-eur-336-million-audia6-crypto-laundering-pipeline>

【Contiランサムウェア関連の詐欺共謀でウクライナ国籍の被告が有罪答弁】 (出典: 米司法省 2026/06/12)

米司法省は、ランサムウェアグループContiの展開に関与したウクライナ国籍のOleksii Lytvynenkoが電信詐欺の共謀罪で有罪を認めたと発表した。同人はアイルランドから引き渡され、最大20年の禁錮刑に問われる。
<https://www.justice.gov/opa/pr/ukrainian-national-pleads-guilty-wire-fraud-conspiracy-connection-conti-ransomware>

【マルウェア「ランサムウェア」の脅威と対策 (脅威編)・(対策編)】 (出典: 警視庁 2026/06/19)

警視庁がランサムウェアの脅威と対策をまとめた解説ページ (脅威編・対策編) を公開。脅威編で令和7年の被害数や二重恐喝の動向、侵入経路の実態を、対策編で基本的な対策や初動対応などを解説。

(脅威編) https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/ransomware_threat.html

(対策編) https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/ransomware_taisaku.html

※ 外国語で発表されたニュースタイトルは日本語へ翻訳済み

※ 本レポート記載の各ニュース概要は生成AIにより作成

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

監視中のランサムウェア攻撃グループ情報 (拠点数と一覧)

● 当月監視対象の攻撃グループ数：**333** ^(※1) ^(※2)

→ 当月リークサイト掲載の活動を確認した攻撃グループ数：**62**

● 当月監視対象の攻撃グループ一覧 (●：当月から新しく監視対象に加えた攻撃グループ)

※1) レポート公開月に出現した攻撃グループは次月号に反映

※2) 活動停止した攻撃グループを含む

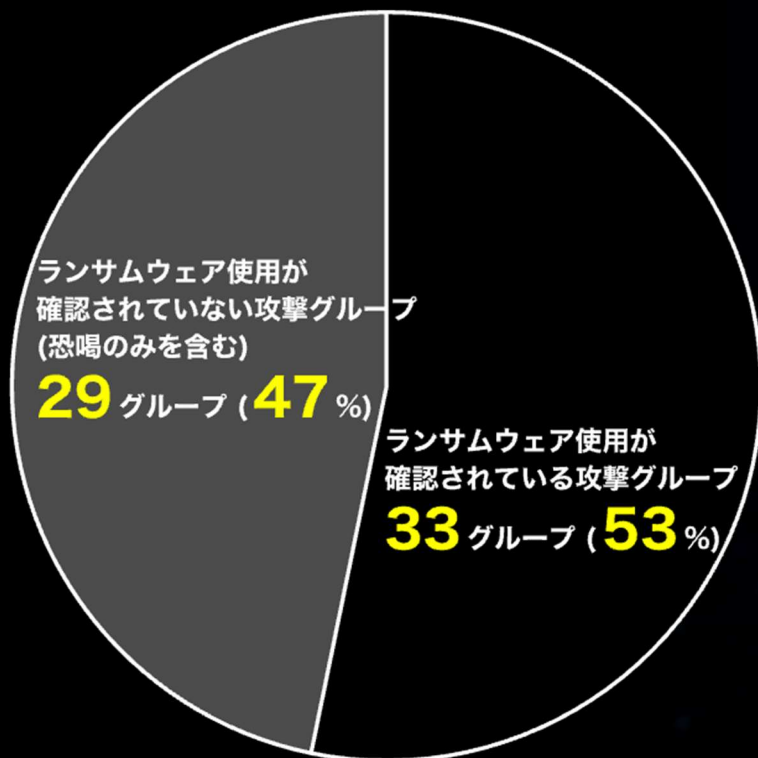
OAPT ● ODAY Omega (Omega) 8BASE Abyss AiLock AKIRA AKO ALP-001 Alpha (MYDATA) AlphV (BlackCat) Anubis Apos Security APT73 (Eralieg) ARACHNA ARCUS MEDIA Argonauts Arkana ArvinClub Astro (Astra) Atomsilo AUDIT AurOra Avaddon AvosLocker AWARE Axxes AzzaSec Babuk Babuk (2025) BASHE ● BAVACAI BEAST Benzona BERT BianLian BLOODY (BLOODY) Bl4ckT0r (BlackTor) Black Basta BlackByte BlackDolphin BlackField	BlackLock BlackMatter Black Nevas Blackout BLACKSHRANTAC BlackSuit BLACKWATER BLUEBOX BLUESKY BQTLOCK Brain Cipher BRAVOX Brotherhood BULLY Business Data Leaks CACTUS Cephalus CHAOS (2025) CHEERS ChileLocker (Arcrypter) CHORT Cicada3301 CiphBit CipherForce CipherLocker CLOP (CLOP) Cloak ● CMD ORGANIZATION COINBASE CARTEL Conti Cooming Project Crazy Hunter Team CROSSLOCK CRYO CryptBB CRYPTNET CRYPTO24 CryptOn GD LockerSec Cuba Cyclops D4RK4RMY DAGON	DAIXIN dAn0n (danon) Dark Angels DARKBIT DARKPOWER DarkRace DarkRypt Dark Shinigamis Darkside Dark Vault DataCarry Brain Cipher Datakeeper Brotherhood DEVMAN DEVMAN 2.0 Dire Wolf Dispossessor[Databroker] Donex Donut Leaks DoppelPaymer dotAdmin DragonForce DragonRansomware DUNGHILL eCh0raix (eChoraix) El_Cometa EL DORADO EMBARGO Endurance Entropy Everest EXITIUM FOG Frag FSOCIETY / FLOCKER FSTeam FulcrumSec Funksec GD LockerSec Genesis GLOBAL Grief	Groove Gunra / Fresh Gunra HANDARA [Hacktivist] Haron HELLCAT Helldown HelloGookie Hitler (AGL0BGVYCG) Hive HolyGhost Hotarus Hunters International HYFLOCK ● ICARUS ICEFIRE IMN Crew INC Ransom Insane INSOMNIA INTERLOCK J GROUP KAIROS Karakurt Karma Kawa4096 Kazu KILLSEC Kittykatkrew Knight Kraken (HelloKitty) KRYBIT Kryptos Kyber LAMASHTU LAMBDA La Piovra LAPSUS\$ LAPSUS\$ Group ● LEAK BAZAAR LeakedData (Silent Ransom Group) LEAKNET LILITH	Linkc LockBit LOKI Lorenz LostTrust LunaLock LV LYNX M3RX MADCAT MAD LIBERATOR MALAS MalekTeam Mallox Mamona RIP MBC Medusa MEDUZA LOCKER MEOW Metaencryptor Midas MIGA Minteye Morpheus MNT6 Mogilevich [fraud] MOISHA Money Message Monti Morpheus ● Mortar Mount Locker MS13-089 N3tw0rm (NetWorm) N4UGHTYSEC (NAUGHTYSEC) NASIR SECUTRIY Nefilim NetRunner Nevada NightSky NightSpire NITROGEN	NoEscape Nokoyawa NONAME (VFOKX) NONAME [2023年確認] Nova NULLBULGE Obscura Obscura 2.0 Onyx Orca Orion Leaks OSIRIS PROJECT Pandora Pay2Key Payload Payload.bin Payouts King PEAR PLAY PLAYBOY PRINZ EUGEN Prometheus PRYX PUTIN TEAM Pysa / Mespinoza Qilin (Agenda) QIULONG Quantum RABBIT HOLE RADAR RADIANT Ragnar Locker Ragnarok RA GROUP RALord Rancoz RansomBay Ransom Cartel Ransom Corp RANSOMCORTEX Ransomed.vc	Ransom EXX RansomHouse RansomHub Ransomware Blog Ranzy RA WORLD Raznatovic RedAlert (N13V) Red Ransomware Group (Red CryptoApp) Relic Revil (Sodinokibi) Reynolds Rhysida Risen ROOK root Royal Rransom RunSomeWares Rusty Locker Sabbath (54bb47h) SAFEPAY SARCOMA SATAN LOCK SATANLOCK V2 Scattered LAPSUS\$ Hunters Secp0 Securotrop SenSayQ SHADOWBYT3\$ shaoleaks SHINYHUNTERS Sicarii SIEGEDSEC Silent Sinobi SKIRA TEAM SLUG Snatch Solidbit Space Bears	Sparta Spook ● SPY CORPORATE STORMOUS Sugar Suncrypt SynACK TeamXXX TENGU Termite The Gentlemen THE GREEN BLOOD GROUP ThreeAM (3AM) TIMC ● TITAN TridentLocker TRIGONA TRINITY ● TRIPLE X TRISEC Underground UnSafe SARCOMA Valencia VanHelsing VanirGroup Vect Vice Society V IS VENDETTA VSOP WALocker Warlock WEREWOLVES Weyhro WORLD LEAKS x001xs XING Team XP95 Yanluowang Yurei Zeon Zero Tolerance
---	--	---	--	---	--	---	--

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

監視中のランサムウェア攻撃グループ情報 (ランサムウェア使用の割合)

● 現在活動中の攻撃グループにおけるランサムウェア使用の割合 (2026年 **5**月)

(※当月にリークサイト掲載を確認した攻撃グループ全 **62**グループ中)



暴露型攻撃グループの中にはSTORMOUSやKarakurtなど、ランサムウェアの使用が明確に確認されていない攻撃グループや、ランサムウェアを使用せず窃取データで恐喝のみを行う集団（恐喝グループ）も存在する。

一例として、BianLianやCLOPなどがデータを暗号化せずに恐喝を行う手法に移行しているとされる。

左の円グラフは、2026年5月に活動中である事が確認された全62グループにおけるランサムウェア使用の割合の内訳を示した図である。

年間統計

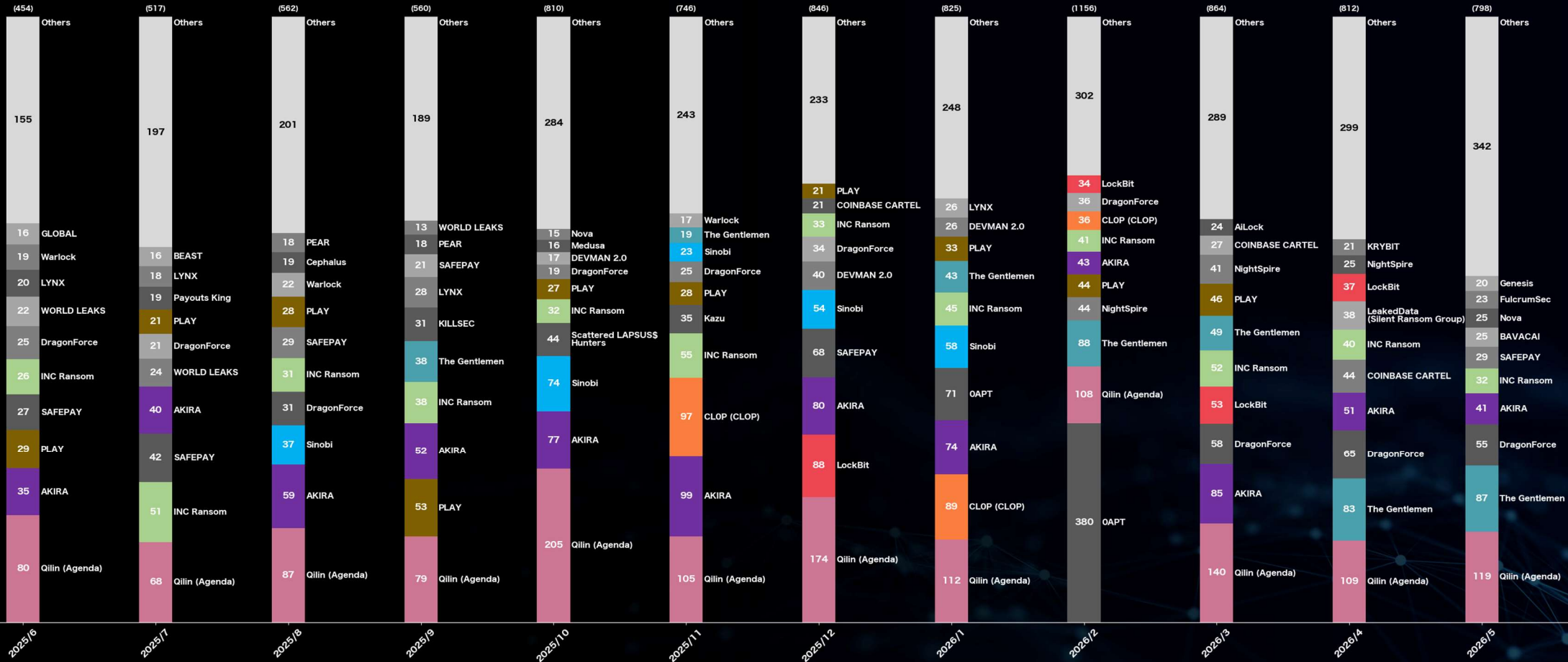
(全世界)

2026

5

攻撃グループ割合で見る被害数の年間統計 (全世界)

(過去1年間 / 2025年6月～2026年5月)



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

暴露型ランサムウェア攻撃統計CIGマンスリーレポート2026年6月号 Rev 1.00

攻撃グループ 月別統計

(全世界) (過去3ヶ月分)

2026
5

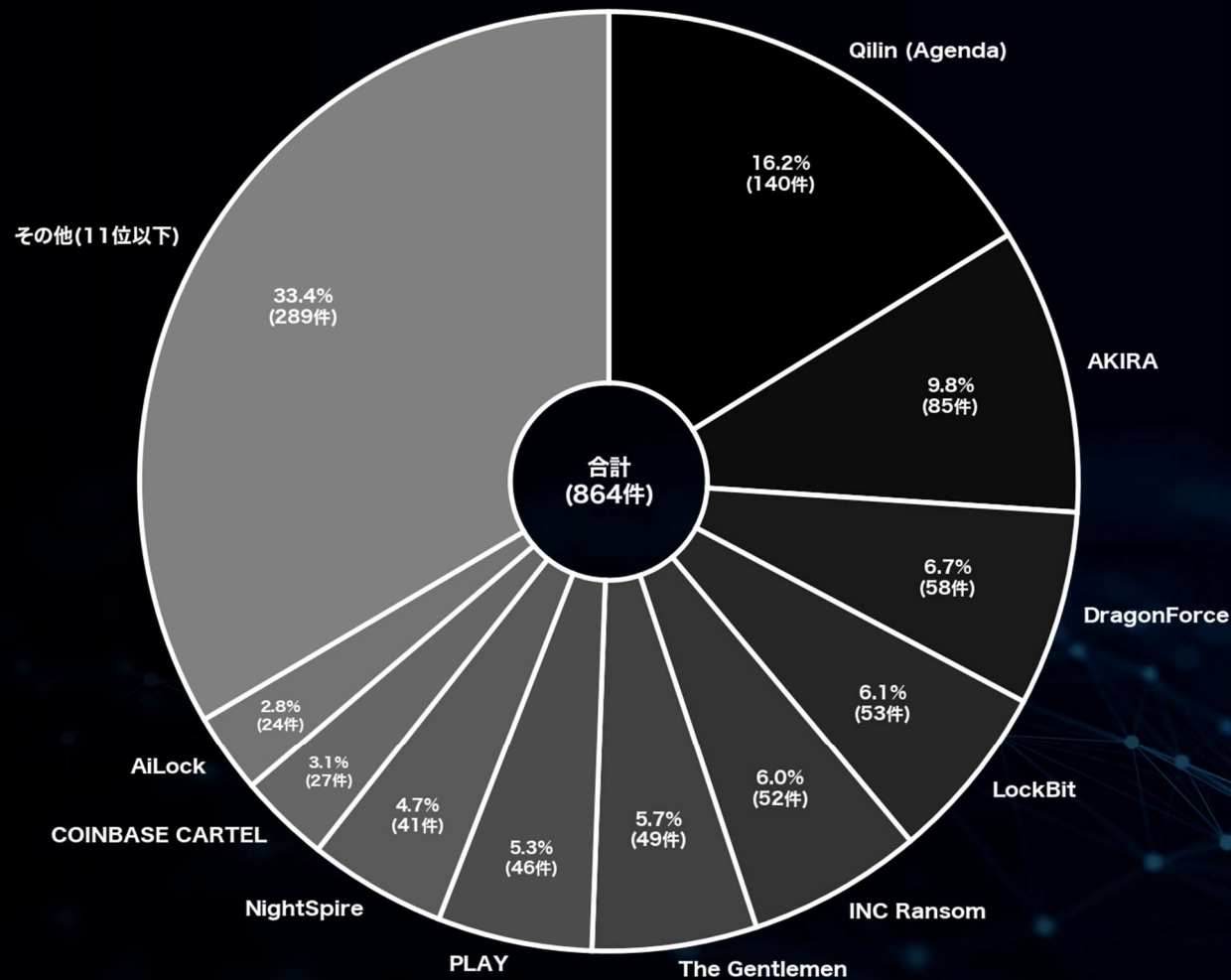
月別内訳 攻撃グループ TOP10 (全世界)

(2026年 3月)

▼ランサムウェア攻撃グループの勢力割合
(リークサイトの掲載数による比較)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

攻撃グループ名	件数	割合(%)	前月比(件数)
Qilin (Agenda)	140	16.2	+ 32
AKIRA	85	9.8	+ 42
DragonForce	58	6.7	+ 22
LockBit	53	6.1	+ 19
INC Ransom	52	6.0	+ 11
The Gentlemen	49	5.7	- 39
PLAY	46	5.3	+ 2
NightSpire	41	4.7	- 3
COINBASE CARTEL	27	3.1	+ 17
AiLock	24	2.8	+ 24



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

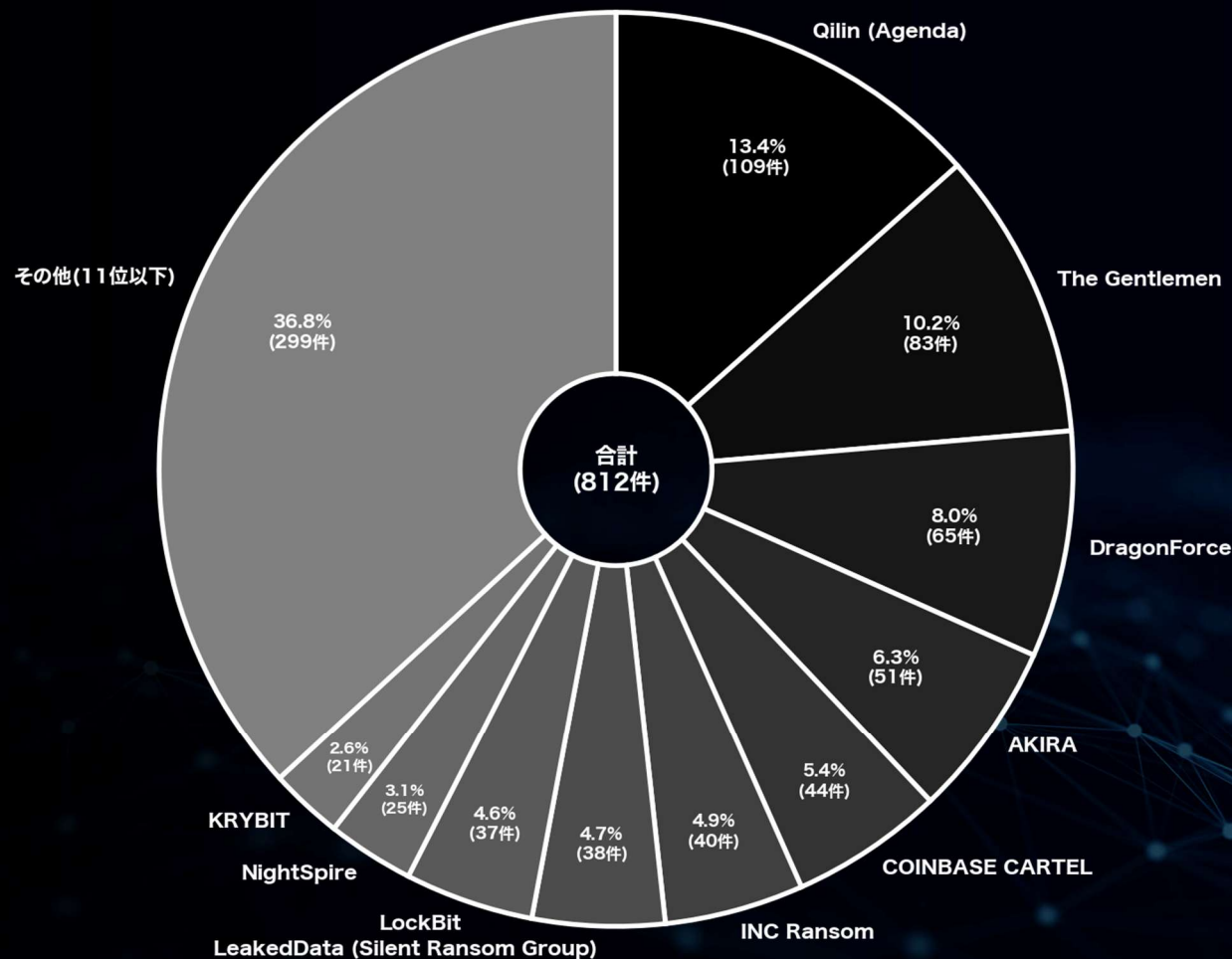
月別内訳 攻撃グループ TOP10 (全世界)

(2026年 4 月)

▼ランサムウェア攻撃グループの勢力割合
(リークサイトの掲載数による比較)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

攻撃グループ名	件数	割合(%)	前月比(件数)
Qilin (Agenda)	109	13.4	- 31
The Gentlemen	83	10.2	+ 34
DragonForce	65	8.0	+ 7
AKIRA	51	6.3	- 34
COINBASE CARTEL	44	5.4	+ 17
INC Ransom	40	4.9	- 12
LeakedData (Silent Ransom Group...)	38	4.7	+ 23
LockBit	37	4.6	- 16
NightSpire	25	3.1	- 16
KRYBIT	21	2.6	+ 21



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

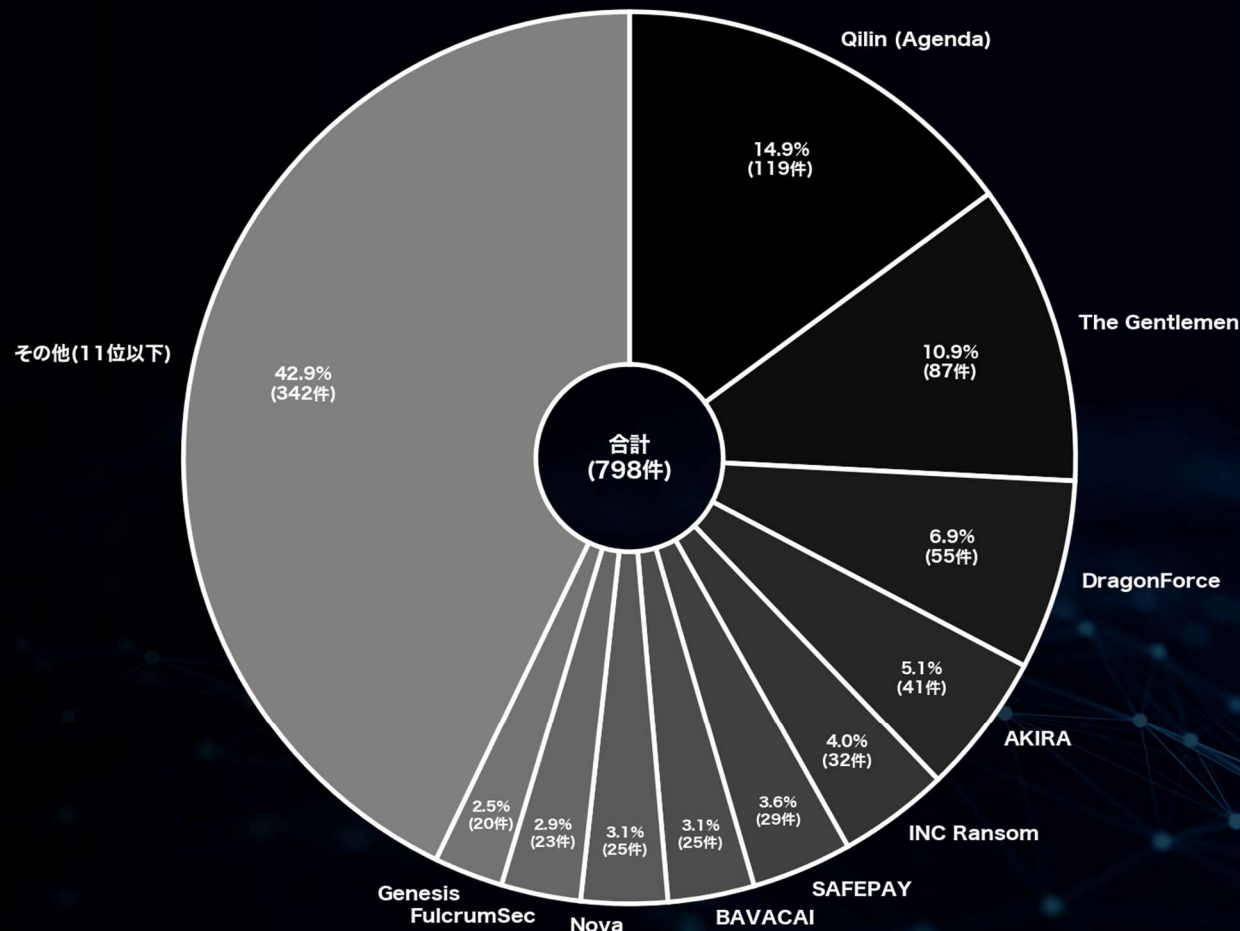
月別内訳 攻撃グループ TOP10 (全世界)

(2026年 5 月)

▼ランサムウェア攻撃グループの勢力割合
(リークサイトの掲載数による比較)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

攻撃グループ名	件数	割合(%)	前月比(件数)
Qilin (Agenda)	119	14.9	+ 10
The Gentlemen	87	10.9	+ 4
DragonForce	55	6.9	- 10
AKIRA	41	5.1	- 10
INC Ransom	32	4.0	- 8
SAFEPAY	29	3.6	+ 19
BAVACAI	25	3.1	+ 25
Nova	25	3.1	+ 18
FulcrumSec	23	2.9	+ 23
Genesis	20	2.5	+ 18



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

被害国 月別統計

(全世界) (過去3ヶ月分)

2026
5

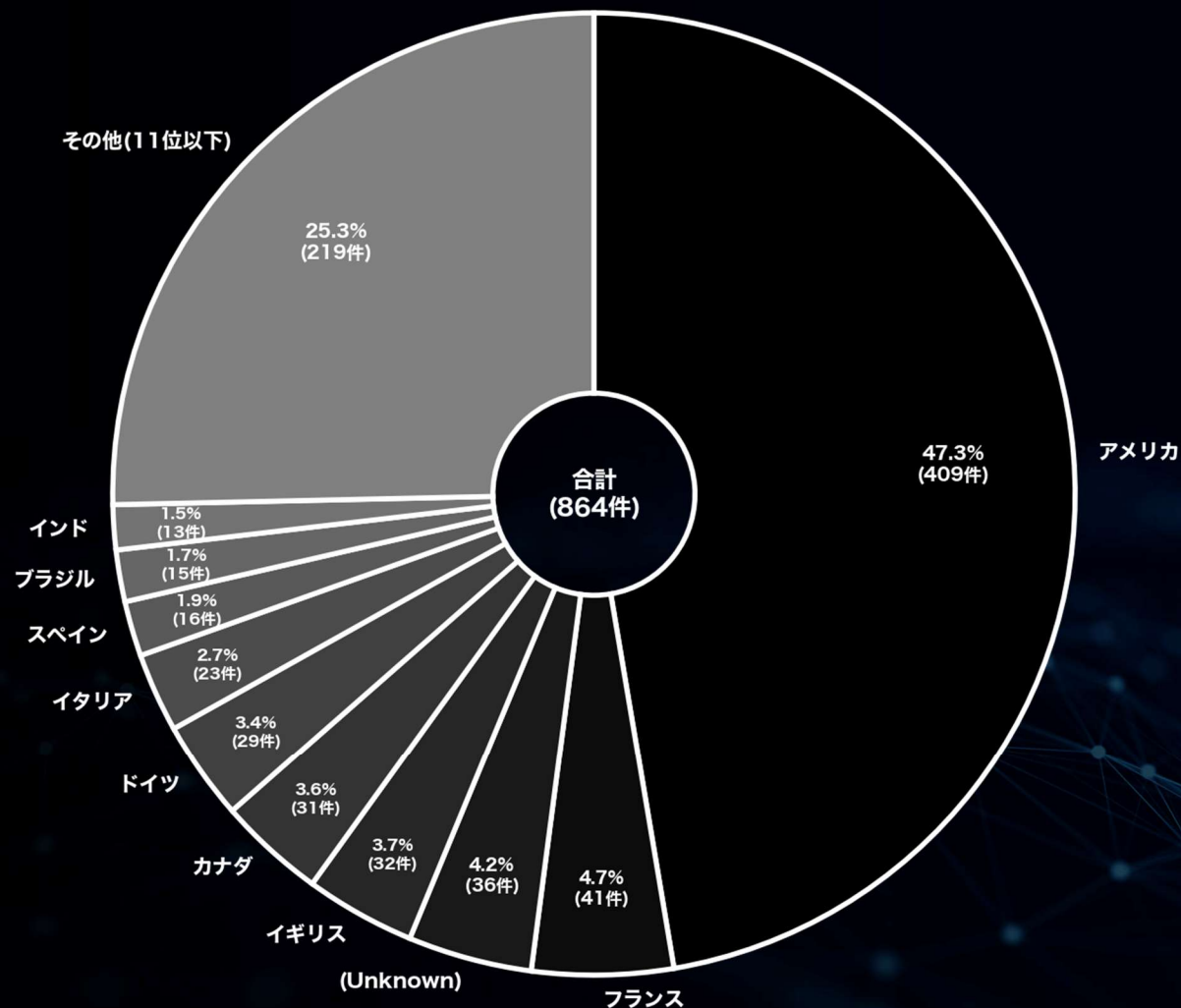
月別内訳 被害国TOP10 (全世界)

(2026年 3月)

▼ランサムウェア攻撃を受けた被害国の割合
(リークサイトの掲載数による比較)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
アメリカ	409	47.3	- 40
フランス	41	4.7	+ 8
(Unknown)	36	4.2	- 115
イギリス	32	3.7	- 11
カナダ	31	3.6	- 10
ドイツ	29	3.4	± 0
イタリア	23	2.7	- 3
スペイン	16	1.9	+ 3
ブラジル	15	1.7	- 10
インド	13	1.5	- 4



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

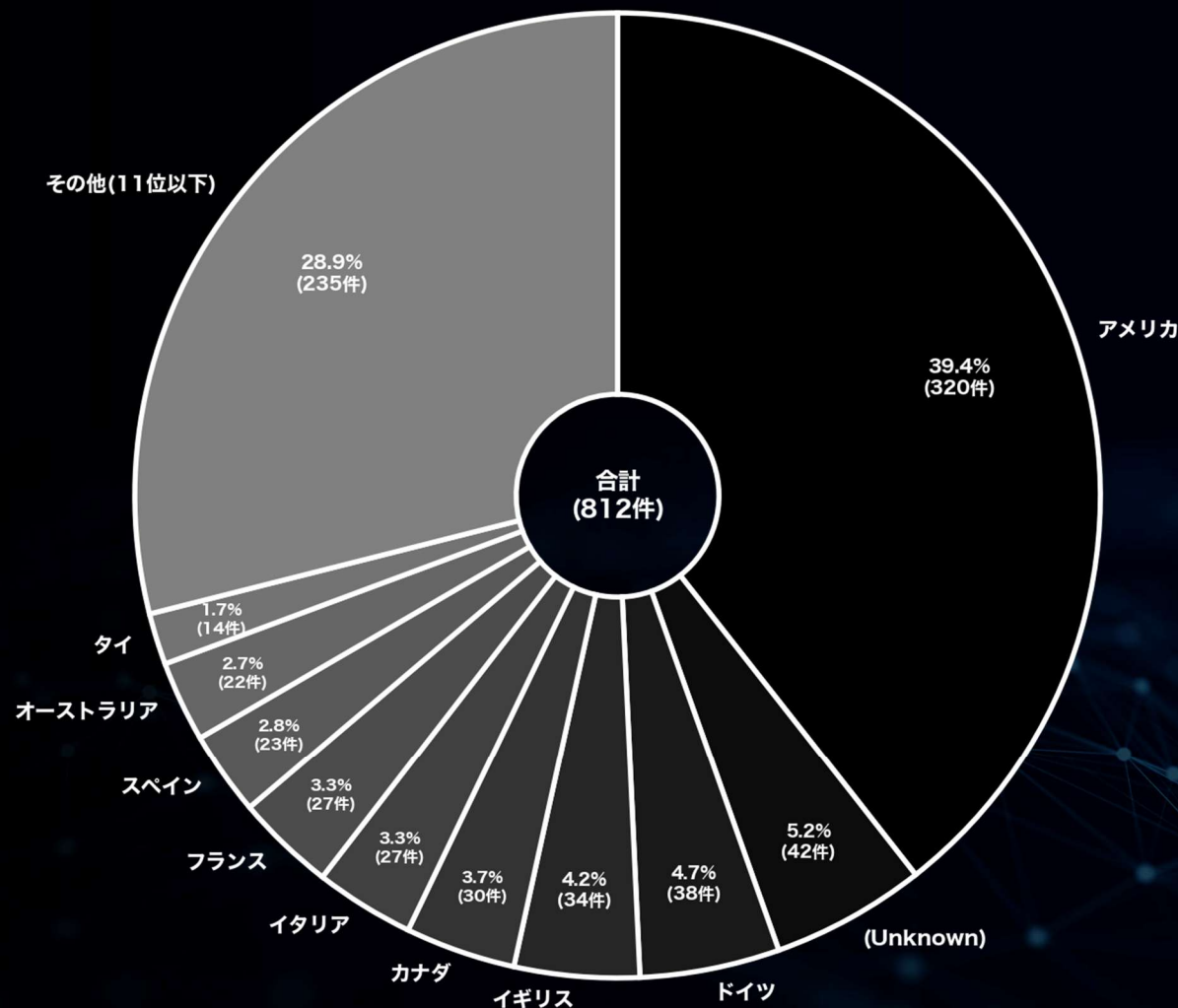
月別内訳 被害国TOP10 (全世界)

(2026年 4 月)

▼ランサムウェア攻撃を受けた被害国の割合
(リークサイトの掲載数による比較)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
アメリカ	320	39.4	- 89
(Unknown)	42	5.2	+ 6
ドイツ	38	4.7	+ 9
イギリス	34	4.2	+ 2
カナダ	30	3.7	- 1
イタリア	27	3.3	+ 4
フランス	27	3.3	- 14
スペイン	23	2.8	+ 7
オーストラリア	22	2.7	+ 12
タイ	14	1.7	+ 4



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

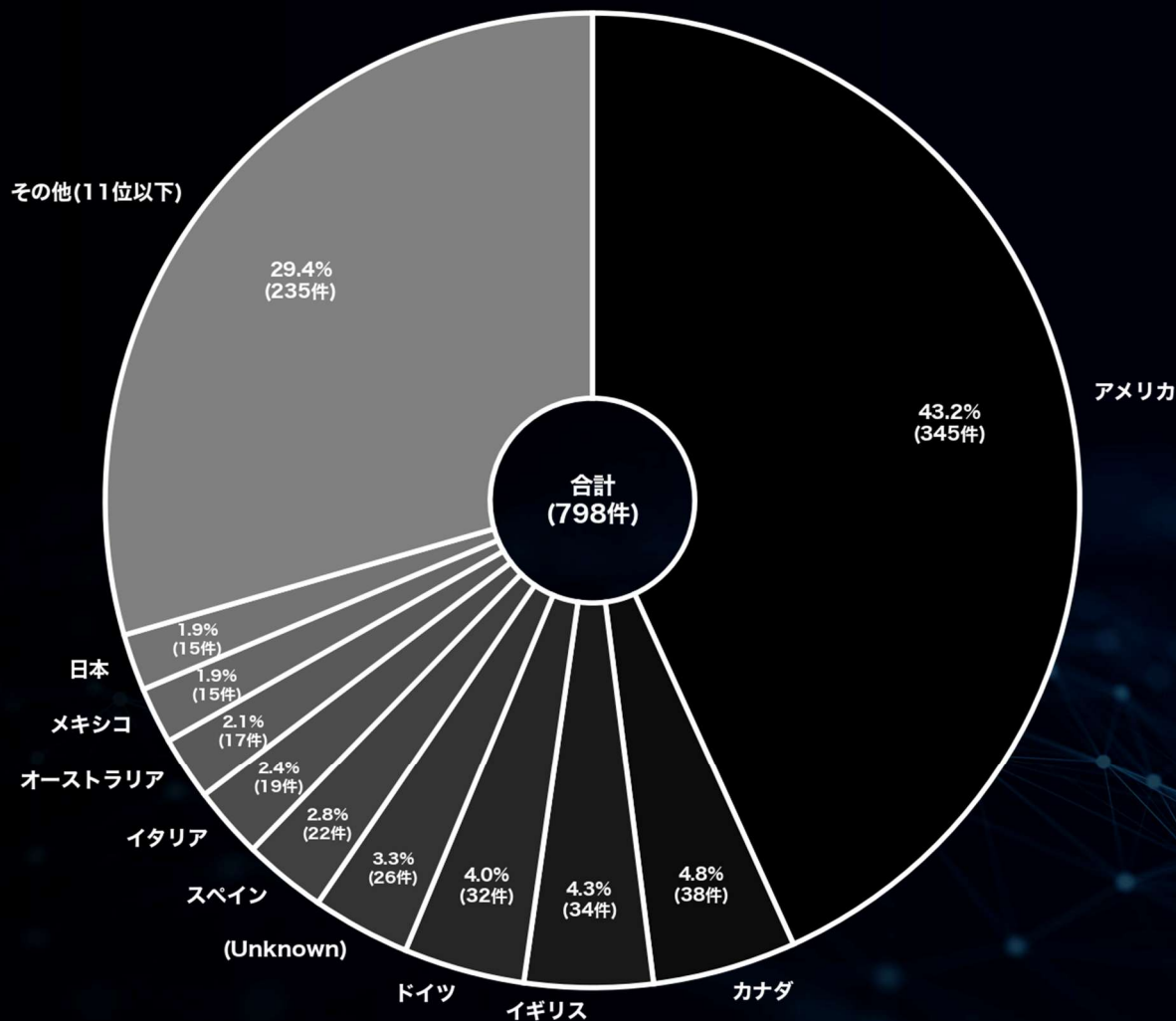
月別内訳 被害国TOP10 (全世界)

(2026年 5月)

▼ランサムウェア攻撃を受けた被害国の割合
(リークサイトの掲載数による比較)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
アメリカ	345	43.2	+ 25
カナダ	38	4.8	+ 8
イギリス	34	4.3	± 0
ドイツ	32	4.0	- 6
(Unknown)	26	3.3	- 16
スペイン	22	2.8	- 1
イタリア	19	2.4	- 8
オーストラリア	17	2.1	- 5
メキシコ	15	1.9	+ 9
日本	15	1.9	+ 3



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

被害国 月別統計

(アジア) (過去3ヶ月分)

2026
5

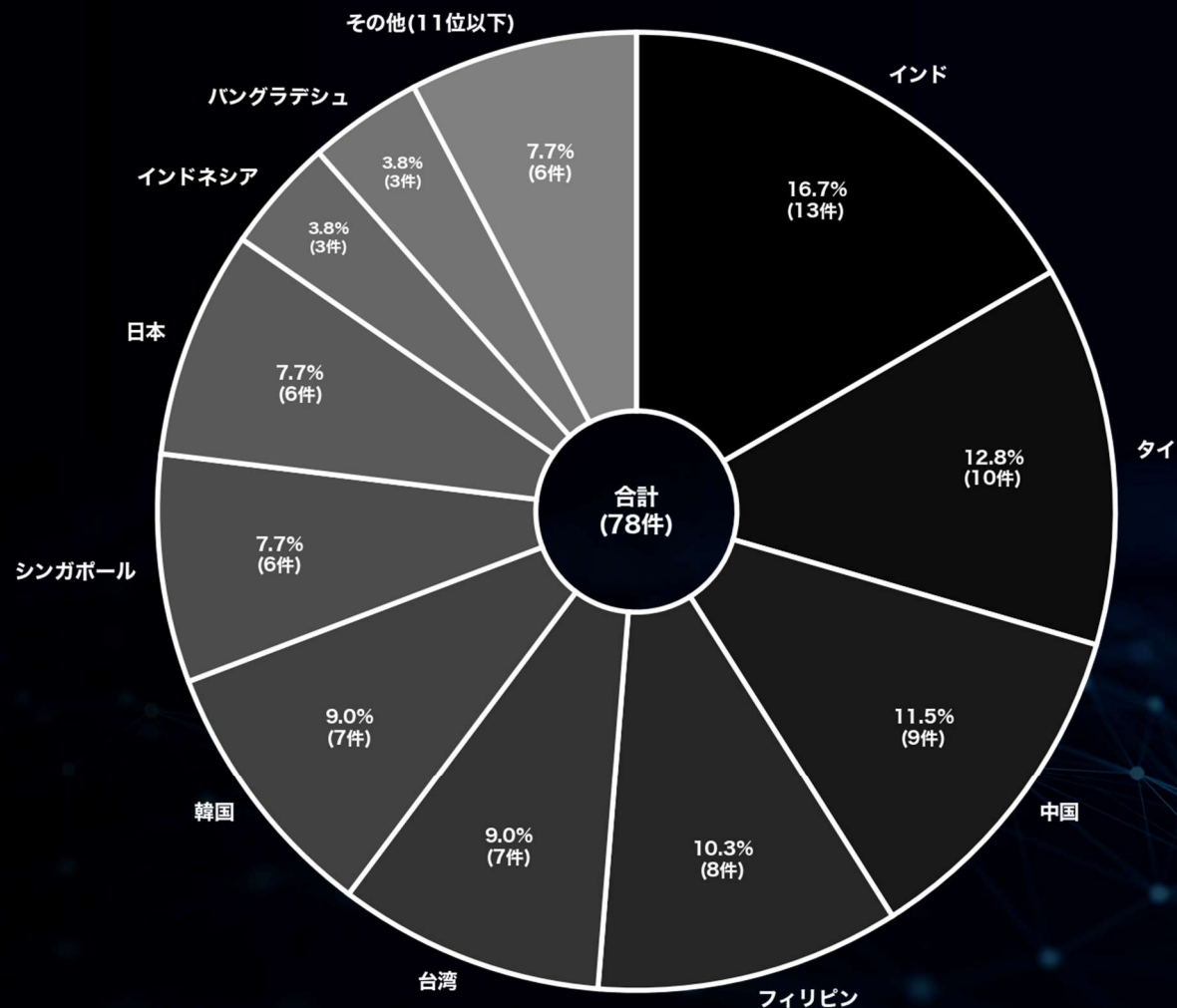
月別内訳 被害国TOP10 (アジア)

(2026年 3月)

▼ランサムウェア攻撃を受けたアジア諸国の割合
(リークサイトの掲載数による比較)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
インド	13	16.7	- 4
タイ	10	12.8	- 11
中国	9	11.5	+ 2
フィリピン	8	10.3	+ 5
台湾	7	9.0	- 8
韓国	7	9.0	- 5
シンガポール	6	7.7	- 9
日本	6	7.7	- 24
インドネシア	3	3.8	- 2
バングラデシュ	3	3.8	+ 3



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

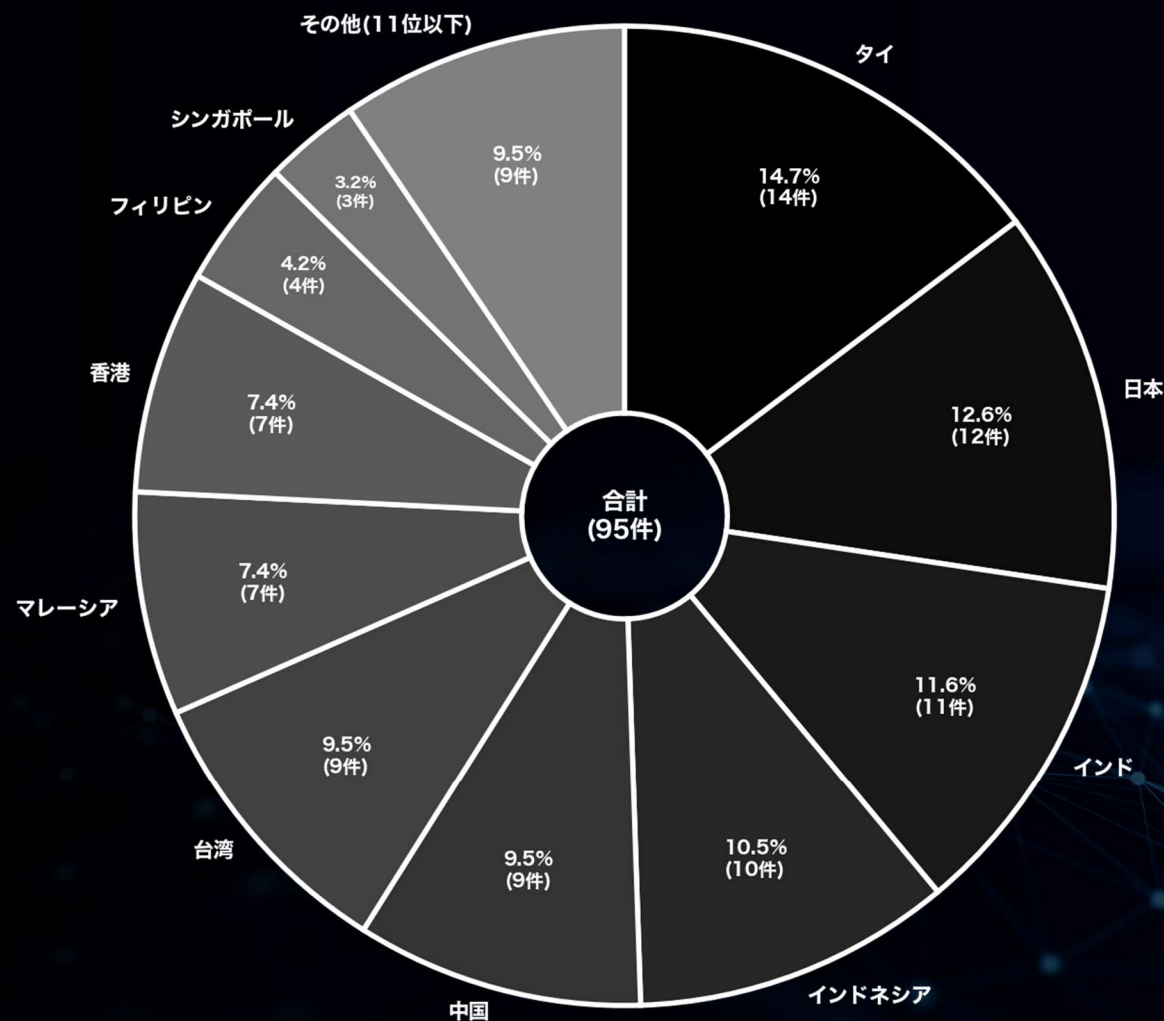
月別内訳 被害国TOP10 (アジア)

(2026年 4 月)

▼ランサムウェア攻撃を受けたアジア諸国の割合
(リークサイトの掲載数による比較)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
タイ	14	14.7	+ 4
日本	12	12.6	+ 6
インド	11	11.6	- 2
インドネシア	10	10.5	+ 7
中国	9	9.5	± 0
台湾	9	9.5	+ 2
マレーシア	7	7.4	+ 5
香港	7	7.4	+ 5
フィリピン	4	4.2	- 4
シンガポール	3	3.2	- 3



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

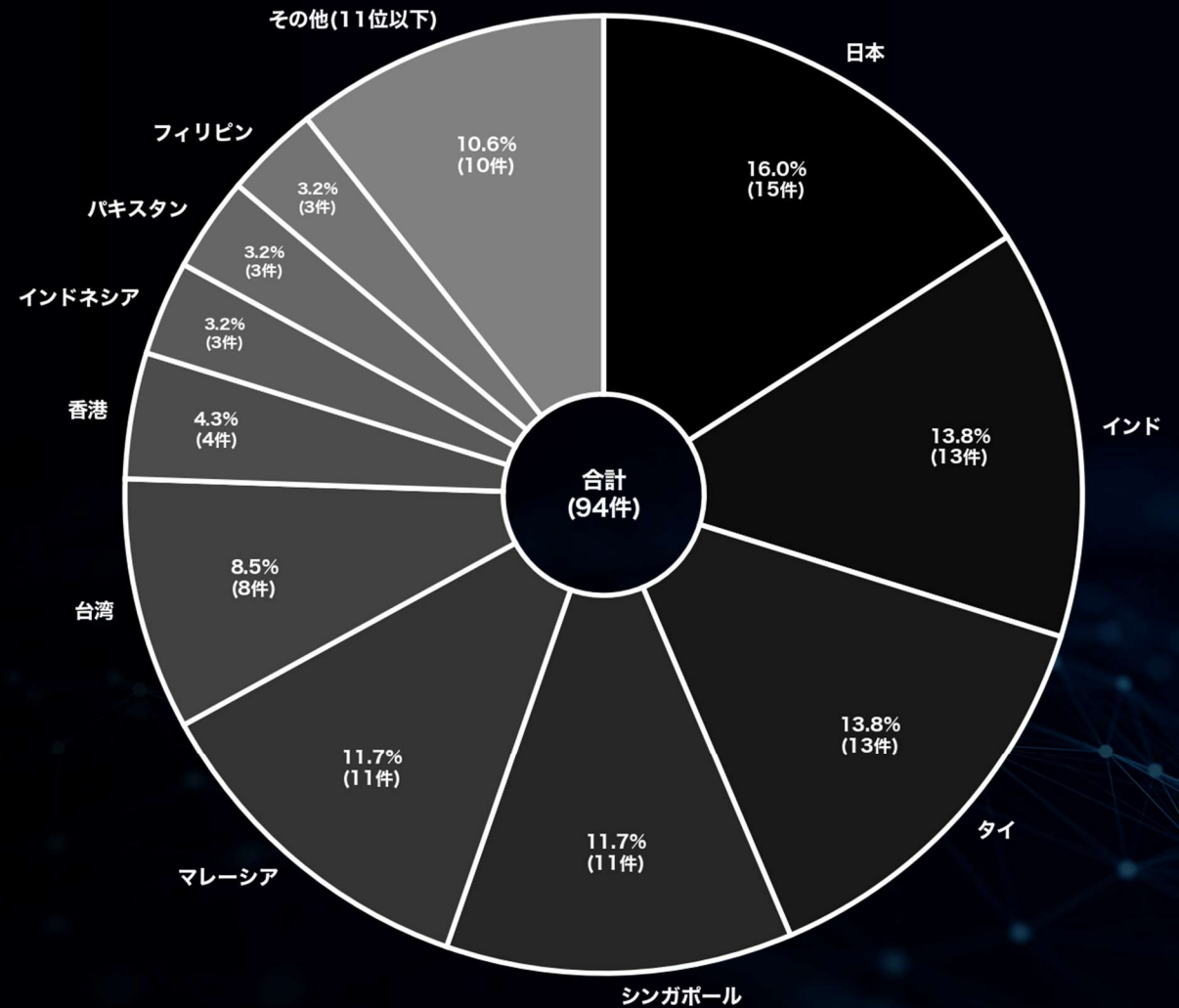
月別内訳 被害国TOP10 (アジア)

(2026年 5 月)

▼ランサムウェア攻撃を受けたアジア諸国の割合
(リークサイトの掲載数による比較)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
日本	15	16.0	+ 3
インド	13	13.8	+ 2
タイ	13	13.8	- 1
シンガポール	11	11.7	+ 8
マレーシア	11	11.7	+ 4
台湾	8	8.5	- 1
香港	4	4.3	- 3
インドネシア	3	3.2	- 7
パキスタン	3	3.2	+ 1
フィリピン	3	3.2	- 1



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

業種 月別統計

(全世界) (過去3ヶ月分)

2026
5

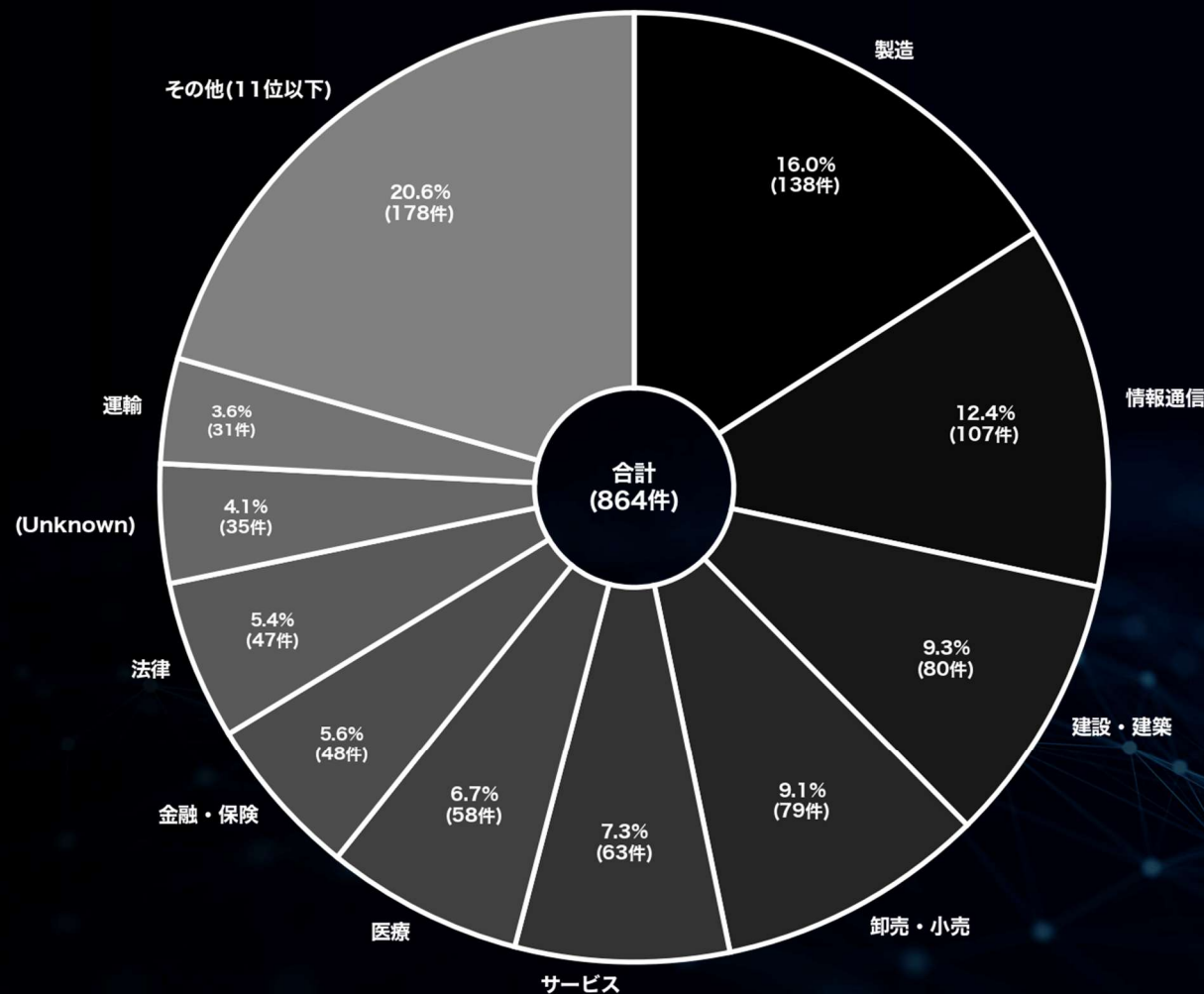
月別内訳 業種 TOP10 (全世界)

(2026年 3月)

▼ランサムウェア攻撃を受けた組織の業種割合
(リークサイトの掲載数による比較)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

業種	件数	割合(%)	前月比(件数)
製造	138	16.0	- 88
情報通信	107	12.4	- 1
建設・建築	80	9.3	+ 7
卸売・小売	79	9.1	+ 22
サービス	63	7.3	- 27
医療	58	6.7	- 53
金融・保険	48	5.6	+ 10
法律	47	5.4	+ 2
(Unknown)	35	4.1	- 113
運輸	31	3.6	- 17



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

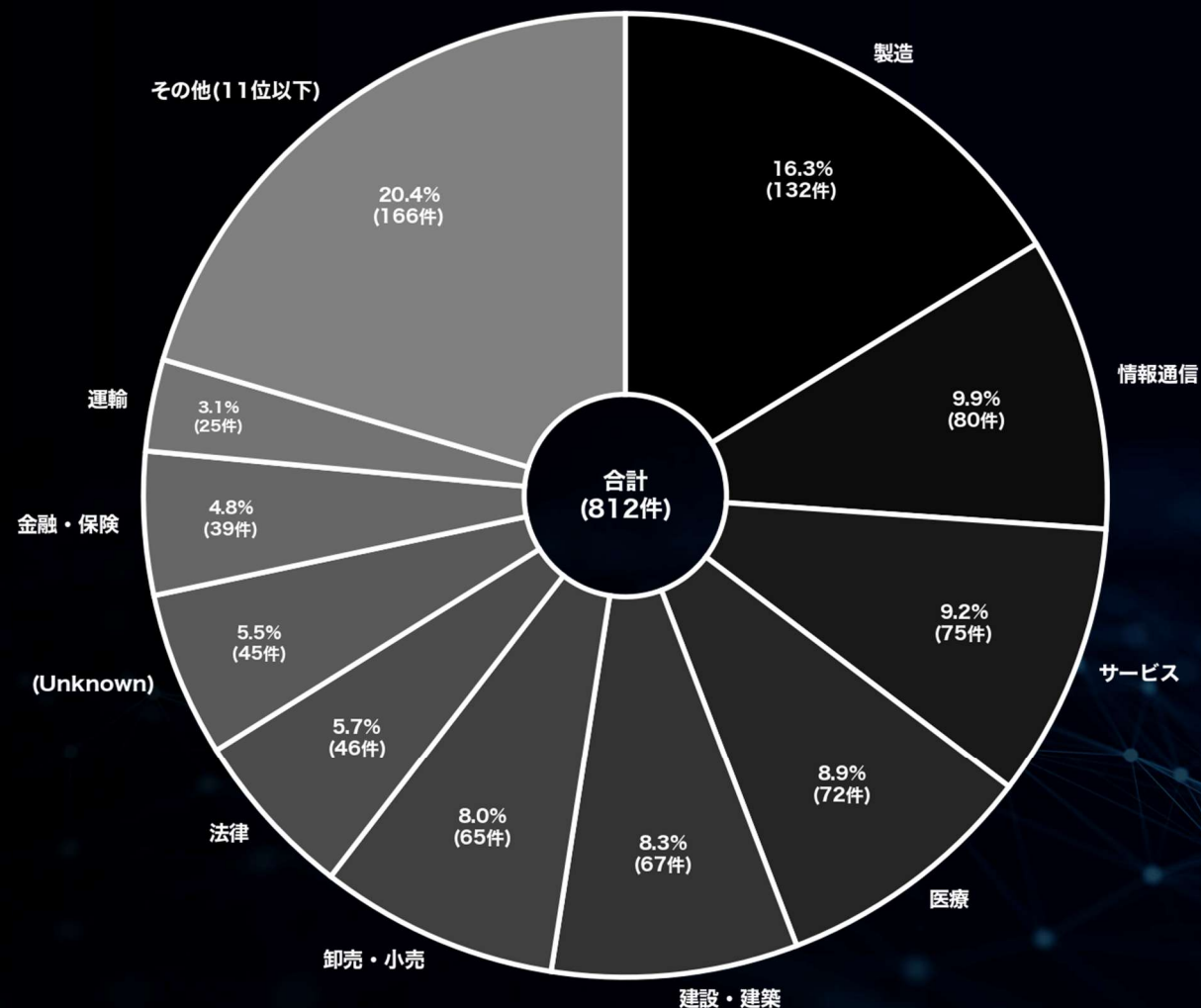
月別内訳 業種 TOP10 (全世界)

(2026年 4 月)

▼ランサムウェア攻撃を受けた組織の業種割合
(リークサイトの掲載数による比較)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

業種	件数	割合(%)	前月比(件数)
製造	132	16.3	- 6
情報通信	80	9.9	- 27
サービス	75	9.2	+ 12
医療	72	8.9	+ 14
建設・建築	67	8.3	- 13
卸売・小売	65	8.0	- 14
法律	46	5.7	- 1
(Unknown)	45	5.5	+ 10
金融・保険	39	4.8	- 9
運輸	25	3.1	- 6



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

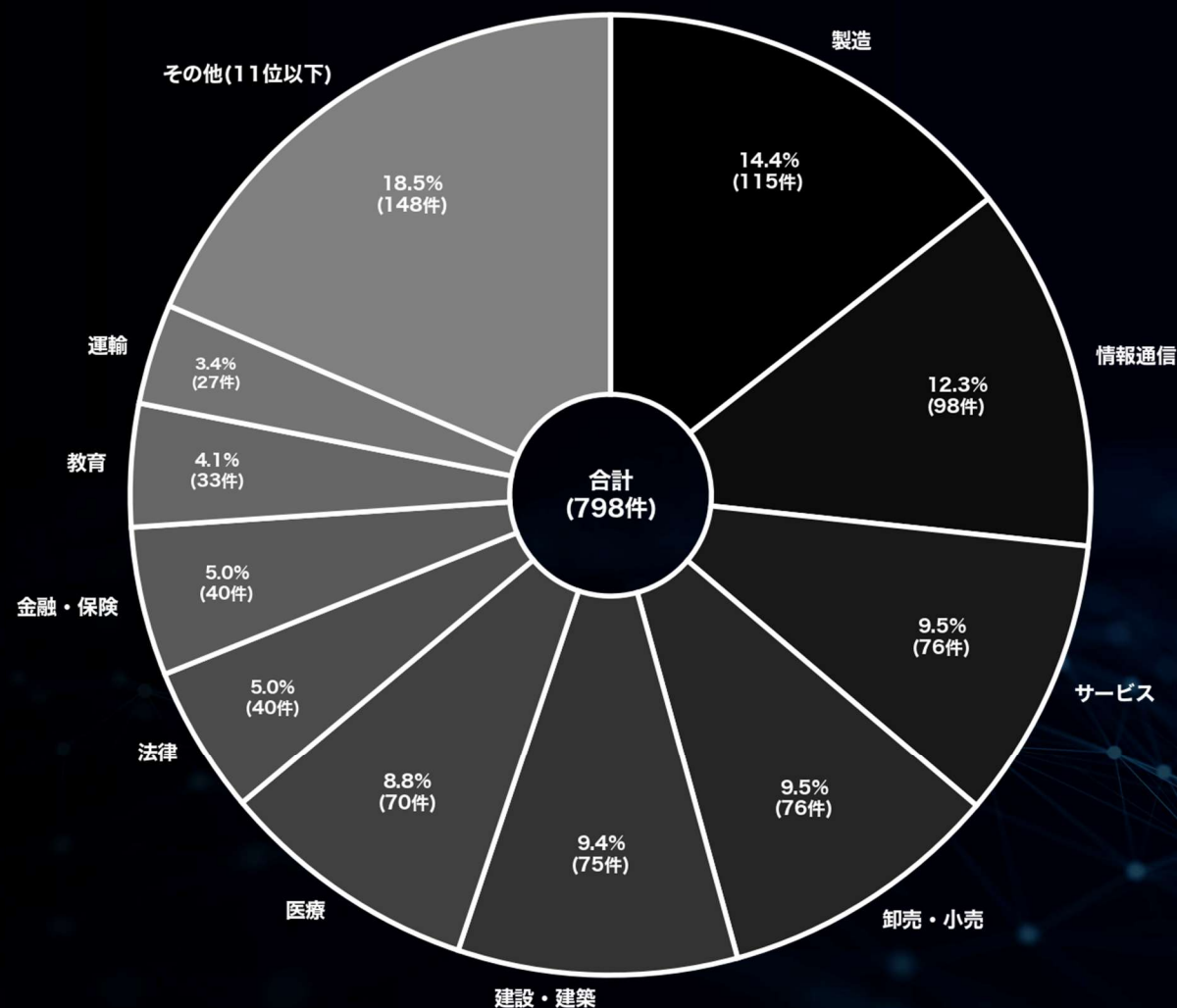
月別内訳 業種 TOP10 (全世界)

(2026年 5 月)

▼ランサムウェア攻撃を受けた組織の業種割合
(リークサイトの掲載数による比較)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

業種	件数	割合(%)	前月比(件数)
製造	115	14.4	- 17
情報通信	98	12.3	+ 18
サービス	76	9.5	+ 1
卸売・小売	76	9.5	+ 11
建設・建築	75	9.4	+ 8
医療	70	8.8	- 2
法律	40	5.0	- 6
金融・保険	40	5.0	+ 1
教育	33	4.1	+ 10
運輸	27	3.4	+ 2



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

被害数の推移に関する統計

(全世界及び国内)

2026

5

被害数の推移 (全世界及び国内)

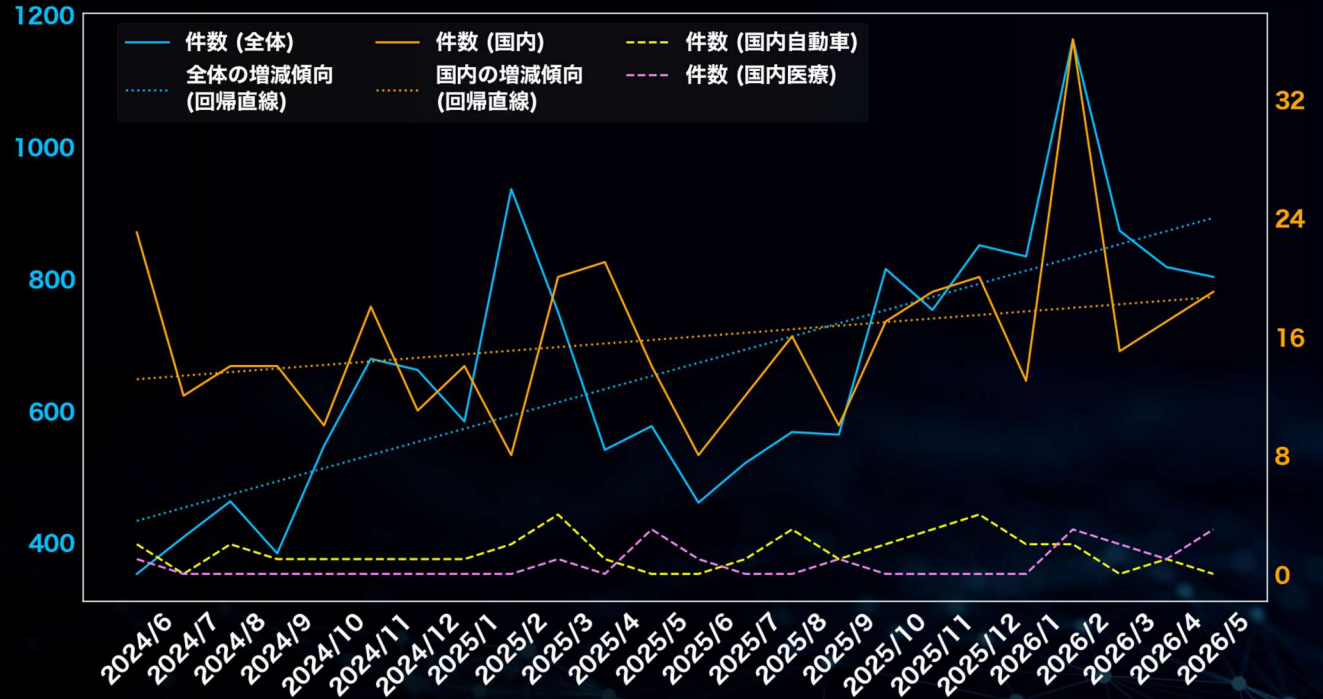
(過去2年間 / 2024年6月～2026年5月)

※件数には公表や報道から判明した数も含む

期間	件数 (全体)	件数 (国内)	件数 (国内自動車…)	件数 (国内医療)
2024/6	352	23	2	1
2024/7	408	12	0	0
2024/8	462	14	2	0
2024/9	383	14	1	0
2024/10	546	10	1	0
2024/11	678	18	1	0
2024/12	661	11	1	0
2025/1	583	14	1	0
2025/2	935	8	2	0
2025/3	749	20	4	1
2025/4	540	21	1	0
2025/5	576	14	0	3
2025/6	460	8	0	1
2025/7	520	12	1	0
2025/8	567	16	3	0
2025/9	563	10	1	1
2025/10	814	17	2	0
2025/11	752	19	3	0
2025/12	850	20	4	0
2026/1	833	13	2	0
2026/2	1162	36	2	3
2026/3	872	15	0	2
2026/4	817	17	1	1
2026/5	802	19	0	3
合計	15885	381	35	16

▼過去2年間におけるランサムウェア全体の活動推移 (全リークサイトの掲載総数の推移)

※全体統計に併せ、よく注目されがちな国内の2業種をピックアップして掲載している。



(※本ページの表/グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

資本金別の統計

(国内)

2026

5

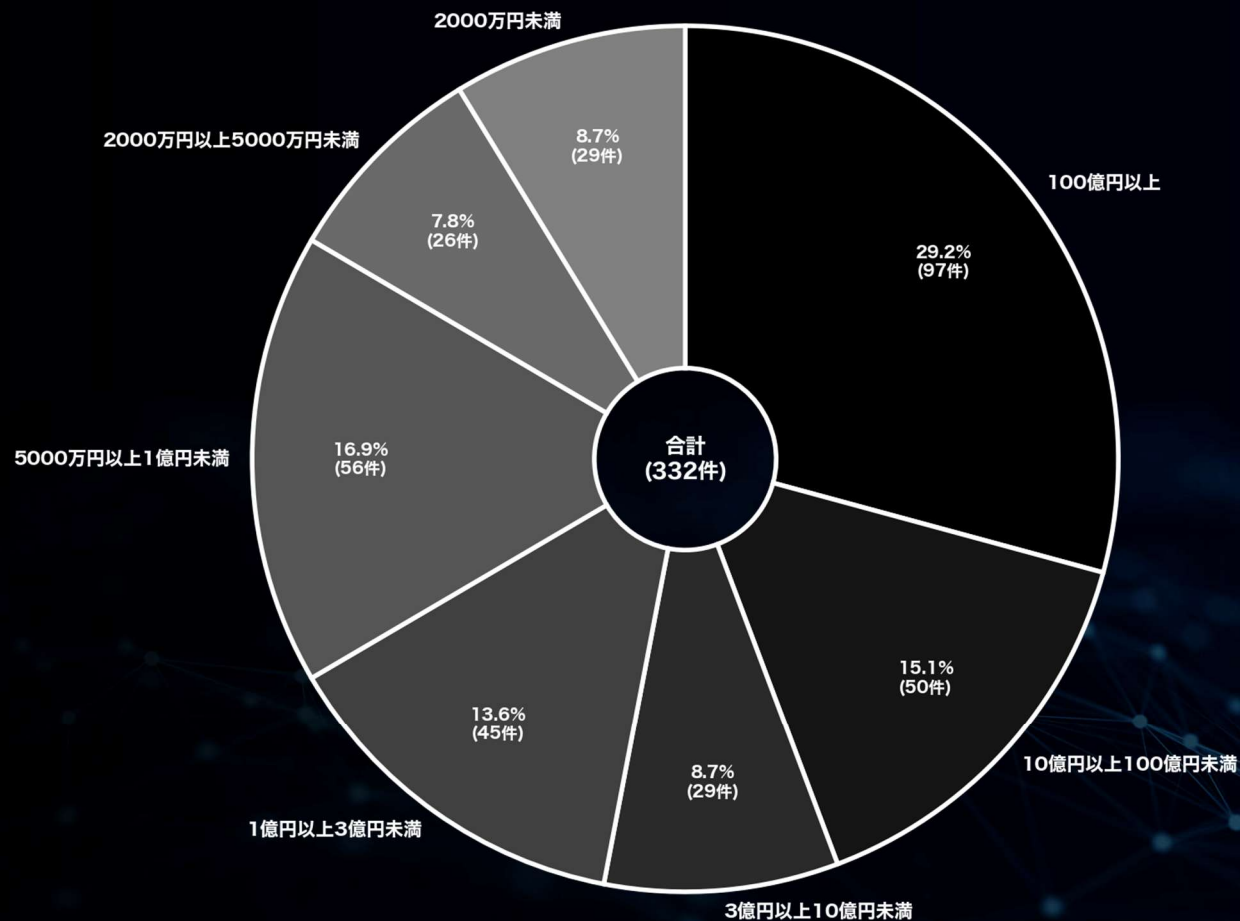
資本金別 (国内)

(過去2年間 / 2024年6月～2026年5月)

※資本金順に降順 / 資本金情報を公表していない一部の被害組織は除外

資本金	件数	割合(%)
100億円以上	97	29.2
10億円以上100億円未満	50	15.1
3億円以上10億円未満	29	8.7
1億円以上3億円未満	45	13.6
5000万円以上1億円未満	56	16.9
2000万円以上5000万円未満	26	7.8
2000万円未満	29	8.7

▼ランサムウェア攻撃を受けた日本関連組織の規模 (資本金)



中小企業に関する詳細な分析は
本レポート「中小企業における被害分析」を参照

(※本ページの表/グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

公表と暴露に関する統計 (国内)

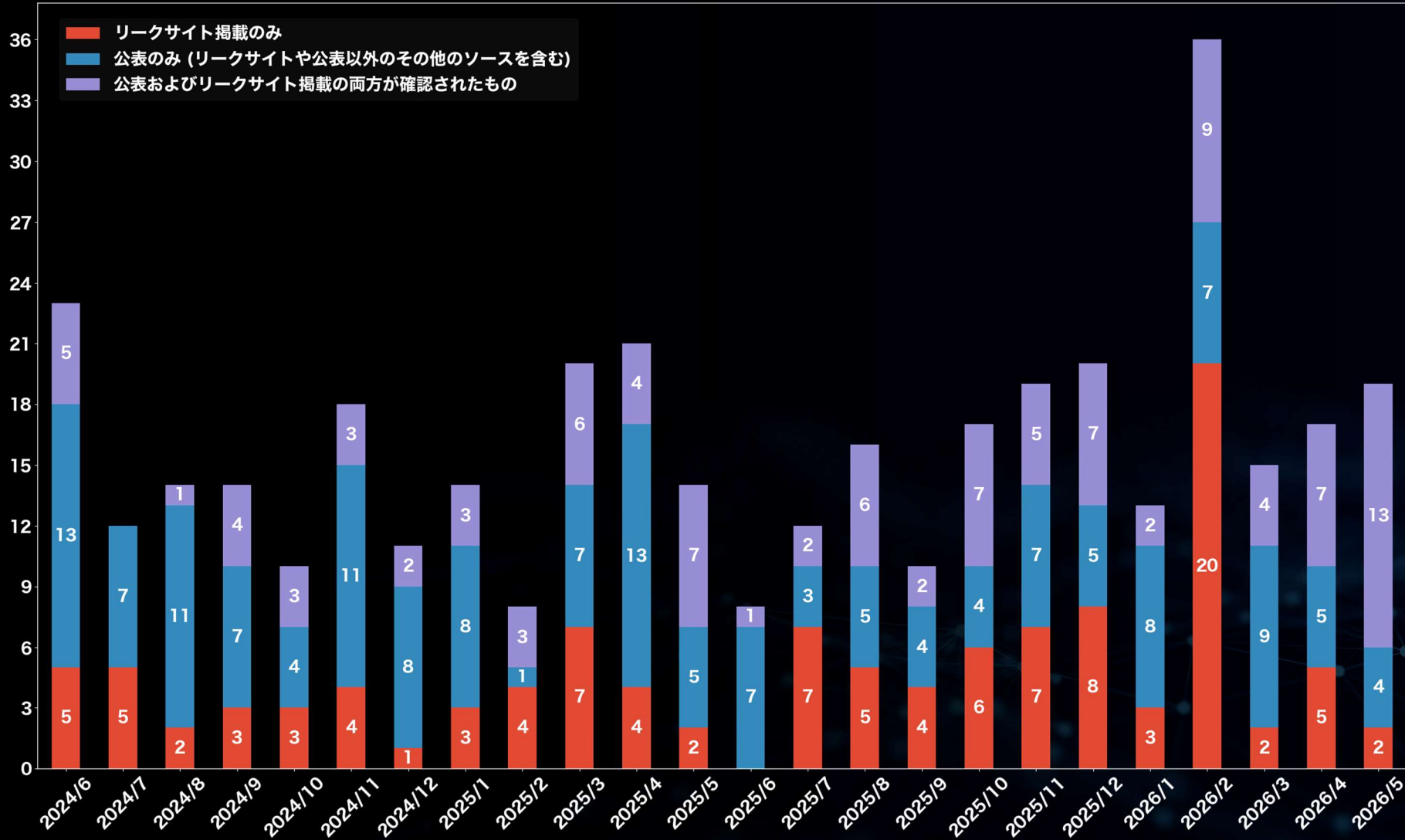
2026

5

公表割合 月別内訳 (国内)

(過去2年間 / 2024年6月～2026年5月)

▼ランサムウェア攻撃における公表数と掲載数の分析



(※本ページの表/グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

公となった国内被害組織 概要一覧

2026

5

公となった国内被害組織概要一覧 (国内)

(過去1年間/2025年6月~2026年5月)

※ (Unknown) の表記は攻撃グループ名が不明または公表されていないケースを表す。
 ※ (海外拠点) の表記は公表等により海外拠点であると判明した被害組織を表す。

被害月	攻撃グループ	業種概要
2025/6	(Unknown)	錠前・セキュリティ製品の販売
2025/6	(Unknown)	システムインテグレーター
2025/6	Qilin (Agenda)	医療機器メーカー(海外拠点)
2025/6	(Unknown)	ポンプ製造業
2025/6	(Unknown)	大手紳士服チェーン
2025/6	(Unknown)	保険事故調査サービス業
2025/6	(Unknown)	設備工事業
2025/6	(Unknown)	建材・住宅・リフォーム・不動産事業
2025/6	Kawa4096	大手保険会社
2025/7	NightSpire	ゴム製品メーカー(海外拠点)
2025/7	Kawa4096	警備サービス業
2025/7	Dire Wolf	電子デバイス製造・販売(海外拠点)
2025/7	(Unknown)	障害福祉サービス業
2025/7	(Unknown)	衛生管理製品・サービス業
2025/7	INC Ransom	高電圧電気機器メーカー(海外拠点)
2025/7	INC Ransom	ファンデーション資材メーカー
2025/7	LYNX	大手食品メーカー(海外拠点)
2025/7	DEVMAN 2.0	電子部品メーカー
2025/7	SAFEPAY	パレル用補助材料メーカー
2025/7	(Unknown)	知的財産情報提供
2025/8	(Unknown)	ソフトウェア開発
2025/8	Black Nevas	特許事務所
2025/8	D4RK4RMV	大手金融機関
2025/8	Qilin (Agenda)	プラスチック製品製造業
2025/8	Qilin (Agenda)	自動車部品メーカー(海外拠点)
2025/8	Qilin (Agenda)	業務用食品卸・加工業
2025/8	(Unknown)	農産物加工・流通
2025/8	Warlock	精密機器メーカー(海外拠点)
2025/8	RansomHouse	電池・電子部品メーカー(海外拠点)
2025/8	Qilin (Agenda)	自動車向けデザイン
2025/8	WORLD LEAKS	毛織物メーカー
2025/8	(Unknown)	業務用・産業用加湿器メーカー
2025/8	(Unknown)	医療・介護事業者向けファクタリング
2025/8	Cephalus	システムインテグレーター

被害月	攻撃グループ	業種概要
2025/8	Black Nevas	大手自動車メーカー(海外拠点)
2025/8	(Unknown)	テーマパーク運営
2025/9	AKIRA	大手精密部品メーカー(海外拠点)
2025/9	Qilin (Agenda)	医療材料メーカー
2025/9	(Unknown)	産業機械・プラントメーカー
2025/9	(Unknown)	電気機器製造業(海外拠点)
2025/9	The Gentlemen	ゴム製品メーカー(海外拠点)
2025/9	COINBASE CARTEL	大手システムインテグレーター
2025/9	(Unknown)	大手工作機械メーカー(海外拠点)
2025/9	PLAY	建設機器メーカー(海外拠点)
2025/9	(Unknown)	商工会連合会
2025/9	J GROUP	大手商社(海外拠点)
2025/10	Scattered LAPSUS\$ Hu...	大手自動車メーカー
2025/10	Scattered LAPSUS\$ Hu...	大手スポーツ用品メーカー
2025/10	Scattered LAPSUS\$ Hu...	大手総合化学メーカー
2025/10	Qilin (Agenda)	大手飲料・食品メーカー
2025/10	(Unknown)	大学法人
2025/10	Rhysida	産業機械メーカー
2025/10	WORLD LEAKS	化粧品メーカー
2025/10	(Unknown)	金融機器メーカー
2025/10	AKIRA	各種機械類・刃物メーカー(海外拠点)
2025/10	(Unknown)	私立学校
2025/10	RansomHouse	有機化学工業品メーカー
2025/10	SAFEPAY	金属加工メーカー
2025/10	(Unknown)	ケーブルテレビ
2025/10	Qilin (Agenda)	食品スーパーマーケット
2025/10	Qilin (Agenda)	総合エネルギー企業
2025/10	Qilin (Agenda)	総合スーパー
2025/10	RansomHouse	大手EC小売事業者
2025/11	(Unknown)	私立大学
2025/11	WORLD LEAKS	プラスチック製品製造業
2025/11	Warlock	サスペンションメーカー
2025/11	Qilin (Agenda)	弁理士法人
2025/11	(Unknown)	システムインテグレーター

被害月	攻撃グループ	業種概要
2025/11	Qilin (Agenda)	通信機器メーカー
2025/11	(Unknown)	雑貨・アパレル小売
2025/11	CRYPTO24	電子部品メーカー
2025/11	CLOP (CLOP)	ラベル印刷機器メーカー
2025/11	INC Ransom	自動車部品メーカー(海外拠点)
2025/11	(Unknown)	教育委員会
2025/11	(Unknown)	私立学校
2025/11	CLOP (CLOP)	大手精密機器メーカー(海外拠点)
2025/11	CLOP (CLOP)	大手自動車メーカー
2025/11	CLOP (CLOP)	大手総合化学メーカー
2025/11	Sinobi	警報装置メーカー
2025/11	Qilin (Agenda)	大手建設会社(海外拠点)
2025/11	(Unknown)	精密部品製造
2025/11	(Unknown)	国際総合検定機関
2025/12	(Unknown)	エレクトロニクス専門商社(海外拠点)
2025/12	(Unknown)	教育系ITサービス提供
2025/12	AKIRA	食用油脂メーカー(海外拠点)
2025/12	Payouts King	プラスチック精密工業部品メーカー(海外拠点)
2025/12	COINBASE CARTEL	大手半導体メーカー
2025/12	INC Ransom	ワイヤーハーネスメーカー
2025/12	LYNX	総合デベロッパー
2025/12	Qilin (Agenda)	空調・衛生設備工事(海外拠点)
2025/12	(Unknown)	総合色材・機能性化学メーカー(海外拠点)
2025/12	root	金融商品取引所
2025/12	Qilin (Agenda)	大手テクノロジー企業(海外拠点)
2025/12	Rhysida	私立学校
2025/12	Qilin (Agenda)	電気機械部品メーカー(海外拠点)
2025/12	DragonForce	自動車部品メーカー(海外拠点)
2025/12	(Unknown)	公立大学
2025/12	(Unknown)	私立大学
2025/12	LYNX	映像制作
2025/12	SAFEPAY	ECサイト運営
2025/12	Qilin (Agenda)	ソフトウェア開発
2025/12	Qilin (Agenda)	精密部品メーカー(海外拠点)

(※本ページの表の情報は、日本にフォーカスする関係上、リークサイトに掲載された情報に加えて国内被害組織からの公表や報道から判明した情報も含む)

公となった国内被害組織概要一覧 (国内)

(過去1年間/2025年6月~2026年5月)

※ (Unknown) の表記は攻撃グループ名が不明または公表されていないケースを表す。
 ※ (海外拠点) の表記は公表等により海外拠点であると判明した被害組織を表す。

被害月	攻撃グループ	業種概要
2026/1	Qilin (Agenda)	工業用計測機器メーカー
2026/1	(Unknown)	印刷サービス
2026/1	(Unknown)	ソフトウェア開発
2026/1	(Unknown)	図書整備支援
2026/1	(Unknown)	総合化学商社
2026/1	(Unknown)	生産用機械器具製造業(海外拠点)
2026/1	Everest	大手自動車メーカー
2026/1	(Unknown)	不動産管理
2026/1	Orion Leaks	タイヤメーカー(海外拠点)
2026/1	(Unknown)	飲料メーカー
2026/1	(Unknown)	スポーツ教室
2026/1	The Gentlemen	産業廃棄物処理
2026/1	Brain Cipher	システムインテグレーター
2026/2	Qilin (Agenda)	特殊金属材料・製造
2026/2	Everest	機械器具製造
2026/2	Everest	金属加工メーカー
2026/2	(Unknown)	大手化学素材メーカー(海外拠点)
2026/2	OAPT	大手電気機器メーカー
2026/2	OAPT	大手テクノロジー企業
2026/2	OAPT	自動制御機器製品メーカー
2026/2	(Unknown)	ペット関連用品製造
2026/2	OAPT	医療機器メーカー
2026/2	OAPT	医療機器メーカー
2026/2	(Unknown)	スキー場運営
2026/2	INC Ransom	国際貨物運送取扱業
2026/2	The Gentlemen	伝熱管メーカー
2026/2	OAPT	タイヤメーカー
2026/2	OAPT	総合電機メーカー
2026/2	OAPT	大手自動車メーカー
2026/2	OAPT	建設機械メーカー
2026/2	OAPT	総合電機メーカー
2026/2	(Unknown)	ソフトウェア開発
2026/2	Qilin (Agenda)	総合デベロッパー
2026/2	(Unknown)	ホテル業・飲食店業

被害月	攻撃グループ	業種概要
2026/2	OAPT	鉄道会社
2026/2	OAPT	地方自治体
2026/2	OAPT	電力会社
2026/2	OAPT	地方自治体
2026/2	Qilin (Agenda)	種苗メーカー兼商社(海外拠点)
2026/2	NightSpire	繊維・衣料関連卸売業
2026/2	(Unknown)	半導体試験装置メーカー
2026/2	NetRunner	総合病院
2026/2	LockBit	機械・工具メーカー(海外拠点)
2026/2	BLACKSHRANTAC	紳士服・婦人服販売
2026/2	NightSpire	モータースポーツチーム運営
2026/2	(Unknown)	印刷会社
2026/2	INC Ransom	石油製品・LPガス販売
2026/2	The Gentlemen	材料加工装置メーカー
2026/2	Everest	商用車メーカー
2026/3	(Unknown)	市場調査・コンサルティング
2026/3	NetRunner	療養型病院
2026/3	(Unknown)	FAX通信・BPOサービス
2026/3	(Unknown)	工業用ゴム・樹脂・配管資材商社
2026/3	(Unknown)	住宅・商業施設向けリペア
2026/3	(Unknown)	美容クリニック
2026/3	(Unknown)	シティホテル運営
2026/3	The Gentlemen	医療・看護専門出版社
2026/3	Space Bears	介護・カラオケ・飲食事業
2026/3	(Unknown)	光半導体デバイスメーカー(海外拠点)
2026/3	WORLD LEAKS	広告・制作
2026/3	The Gentlemen	繊維加工・食品加工メーカー
2026/3	(Unknown)	設備工事
2026/3	(Unknown)	美容室向け化粧品メーカー
2026/3	ALP-001	国立研究開発法人
2026/4	AKIRA	流体システム製品メーカー
2026/4	(Unknown)	非鉄金属・資源開発(海外拠点)
2026/4	(Unknown)	システムインテグレーター

被害月	攻撃グループ	業種概要
2026/4	KRYBIT	酒類製造業
2026/4	LockBit	水処理・環境設備
2026/4	DragonForce	オフィス家具メーカー(海外拠点)
2026/4	(Unknown)	診療予約システム開発
2026/4	Qilin (Agenda)	舗装・土木工事
2026/4	The Gentlemen	電気機器メーカー
2026/4	Qilin (Agenda)	建設資材・福祉用具のレンタル・販売
2026/4	(Unknown)	生活協同組合
2026/4	COINBASE CARTEL	大学研究会
2026/4	Ransom EXX	ソフトウェア開発
2026/4	LockBit	電子部品(コネクタ)製造(海外拠点)
2026/4	(Unknown)	二輪用品専門チェーン
2026/4	The Gentlemen	ソフトウェア開発
2026/4	Qilin (Agenda)	大手自動車部品メーカー(海外拠点)
2026/5	(Unknown)	百貨店業・不動産賃貸業
2026/5	(Unknown)	不動産コンサルティング・資産管理
2026/5	FulcrumSec	移植医療支援
2026/5	KILLSEC	オンライン処方箋サービス
2026/5	(Unknown)	教育サービス・学習教材
2026/5	AI Lock	半導体製造装置・精密機器メーカー(海外拠点)
2026/5	The Gentlemen	医薬品卸売業
2026/5	The Gentlemen	商業施設運営サービス
2026/5	SAFEPAY	産業資材商社
2026/5	AKIRA	家電メーカー(海外拠点)
2026/5	Lynx	水処理装置メーカー(海外拠点)
2026/5	Lynx	蓄電池・電源システム(海外拠点)
2026/5	The Gentlemen	ジュエリー輸入・企画販売
2026/5	Payload	空調設備施工
2026/5	The Gentlemen	ガラス容器メーカー
2026/5	NightSpire	医薬品・食品関連製造(海外拠点)
2026/5	(Unknown)	国立大学法人
2026/5	SAFEPAY	紙器製造
2026/5	SAFEPAY	建材リペア・再生工事

(※本ページの表の情報は、日本にフォーカスする関係上、リークサイトに掲載された情報に加えて国内被害組織からの公表や報道から判明した情報も含む)

公となった国内被害組織における拠点割合 (国内)

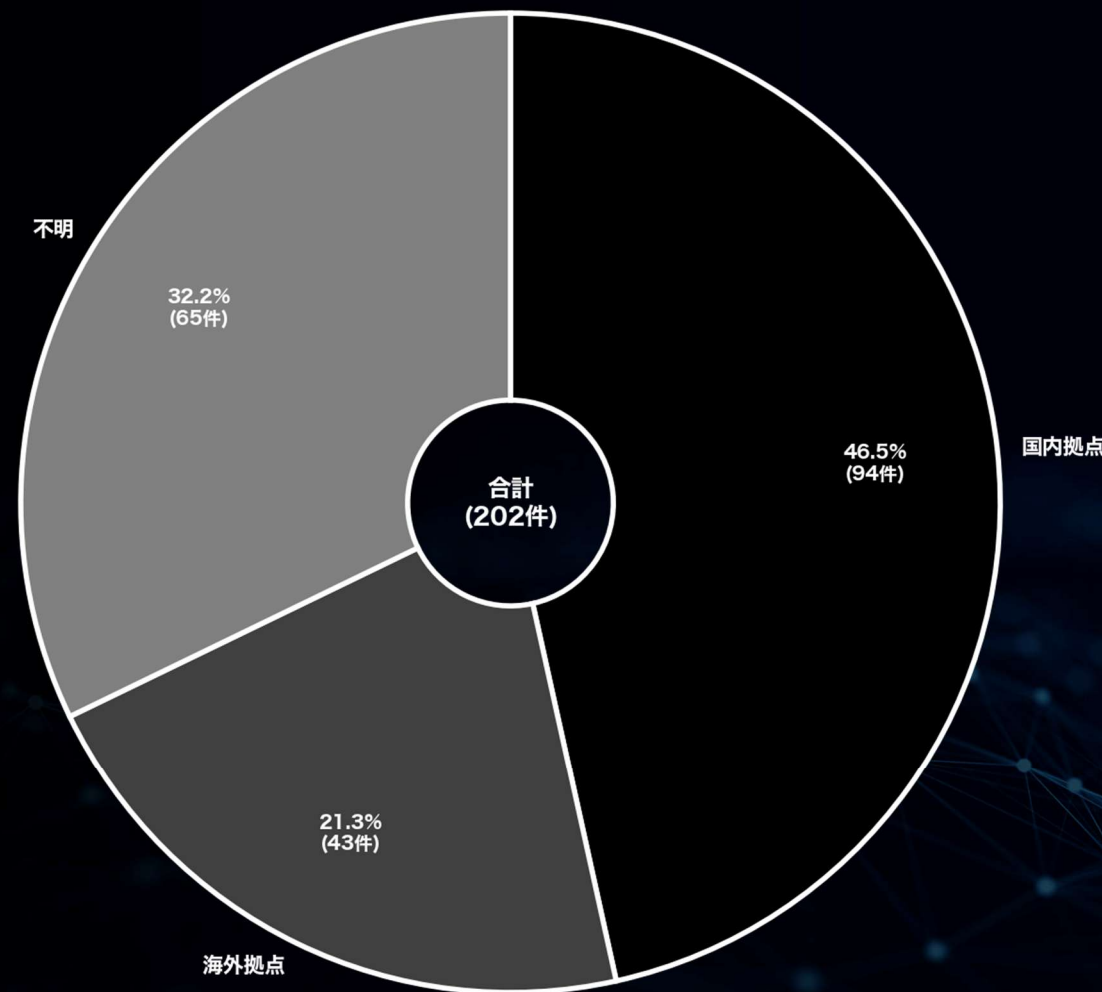
(過去1年間/2025年6月~2026年5月)

(※左下の補足記載のとおり、リークサイトへの掲載や公表から確認ができた被害組織に限定し算出された値である事にあらためて注意)

▼ランサムウェア攻撃を受けた日本関連組織の拠点別割合

※
 「国内拠点」：公表等により、国内拠点における被害事案と判断されるケース数
 「海外拠点」：公表等により、海外拠点（支社/関係会社）における被害事案と判断されるケース数
 「不明」：上記以外、被害拠点の地域的情報が得られなかったケース数

拠点	件数	割合(%)
国内拠点	94	46.5
海外拠点	43	21.3
不明	65	32.2



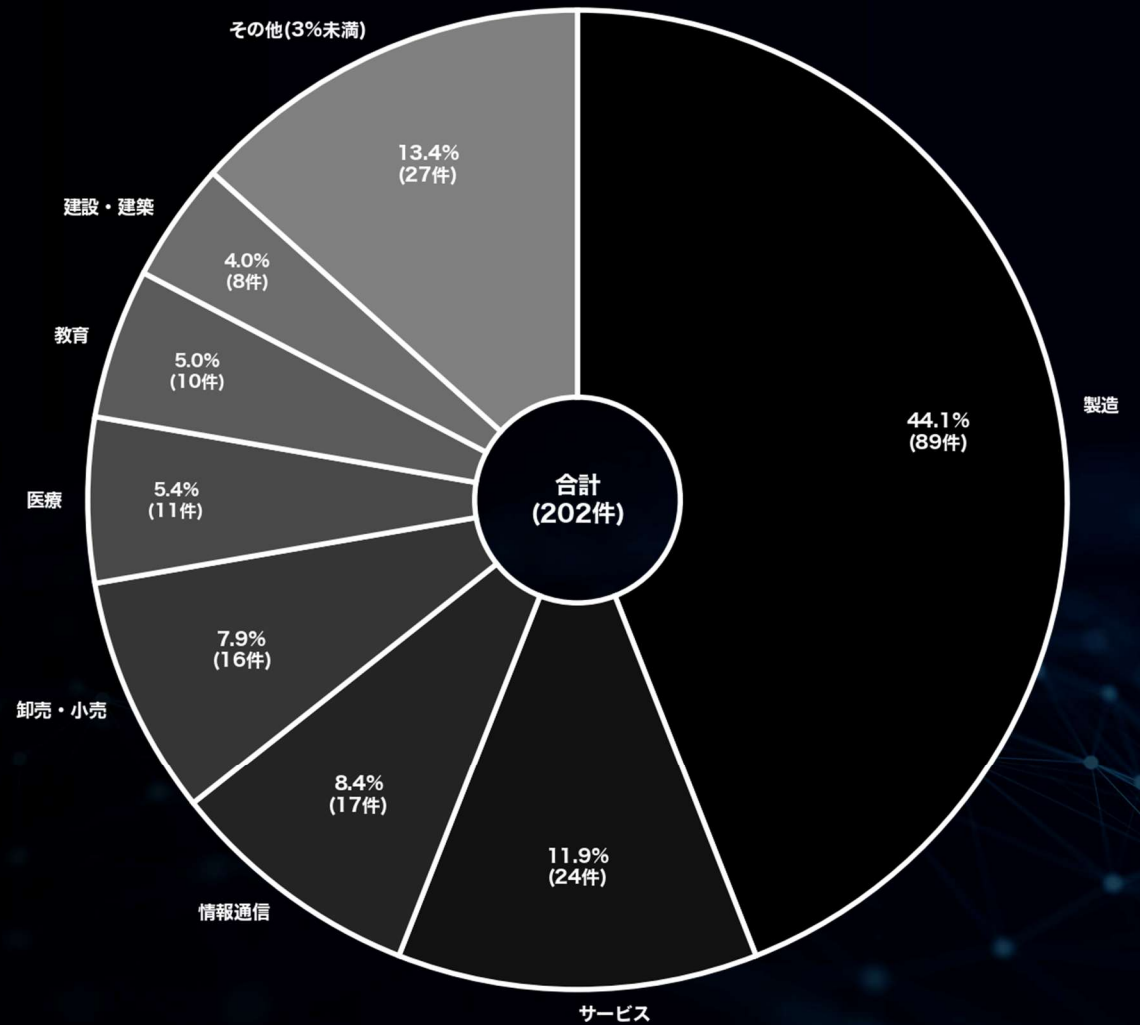
(※本ページの表/グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

公となった国内被害組織における業種割合 (国内)

(過去1年間/2025年6月~2026年5月)

▼ランサムウェア攻撃を受けた日本関連組織の業種別割合

業種	件数	割合(%)
製造	89	44.1
サービス	24	11.9
情報通信	17	8.4
卸売・小売	16	7.9
医療	11	5.4
教育	10	5.0
建設・建築	8	4.0
その他(3%未満)	27	13.4



(※本ページの表/グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

2026

5

中小企業における被害分析

(国内)

中小企業の定義^{*}は業種により法的に異なるが、本資料では中小企業を『資本金3億円未満の組織』と定義する。
※中小企業庁「中小企業・小規模企業者の定義」:<https://www.chusho.meti.go.jp/soshiki/teigj.html>

資本金別 (国内-中小企業)

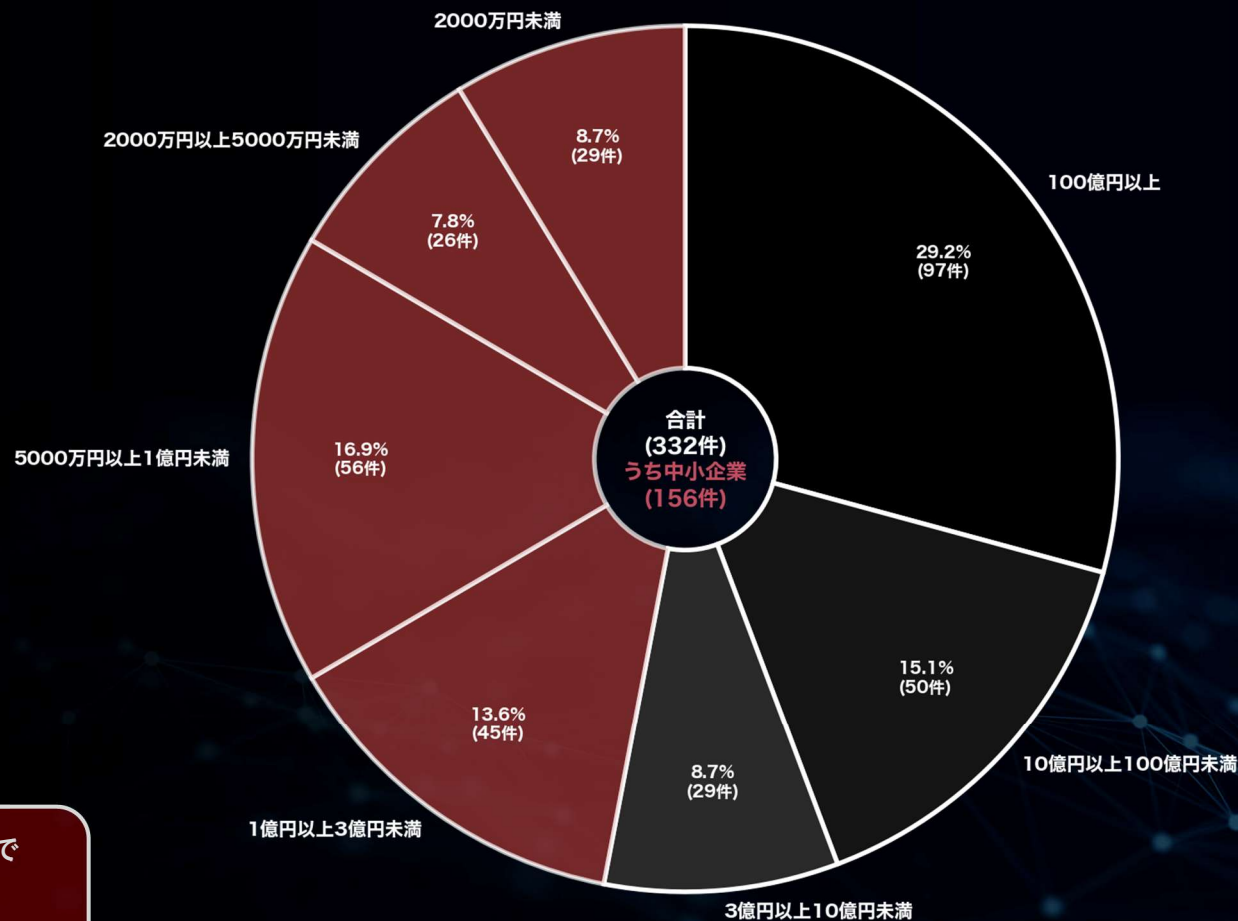
(過去2年間 / 2024年6月～2026年5月)

赤色は中小企業を示す

※資本金順に降順 / 資本金情報を公表していない一部の被害組織は除外

資本金	件数	割合(%)
100億円以上	97	29.2
10億円以上100億円未満	50	15.1
3億円以上10億円未満	29	8.7
1億円以上3億円未満	45	13.6
5000万円以上1億円未満	56	16.9
2000万円以上5000万円未満	26	7.8
2000万円未満	29	8.7

▼ランサムウェア攻撃を受けた日本関連組織の規模 (資本金)



日本関連組織の被害状況を見ると、中小企業の被害は過去2年間で156件にのぼり、全体の47.0%を占める。

これらの被害は、リークサイトへの掲載や公表から確認できたものだが、表面化していない被害も多数存在する可能性があり、実際の被害総数はさらに大きいと考えられる。

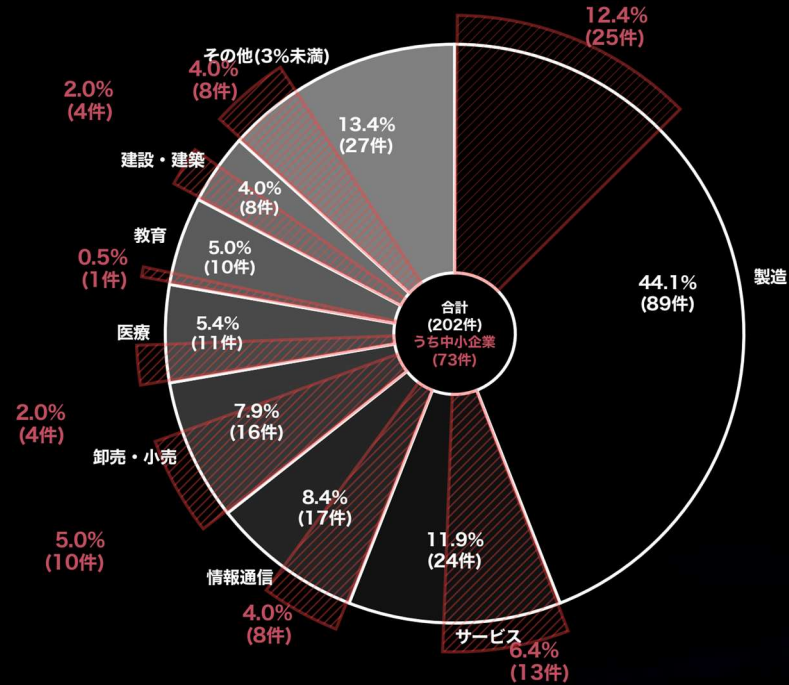
(※本ページの表/グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

公となった国内被害組織における業種割合 (国内-中小企業)

(過去1年間/2025年6月~2026年5月)

赤色は中小企業を示す

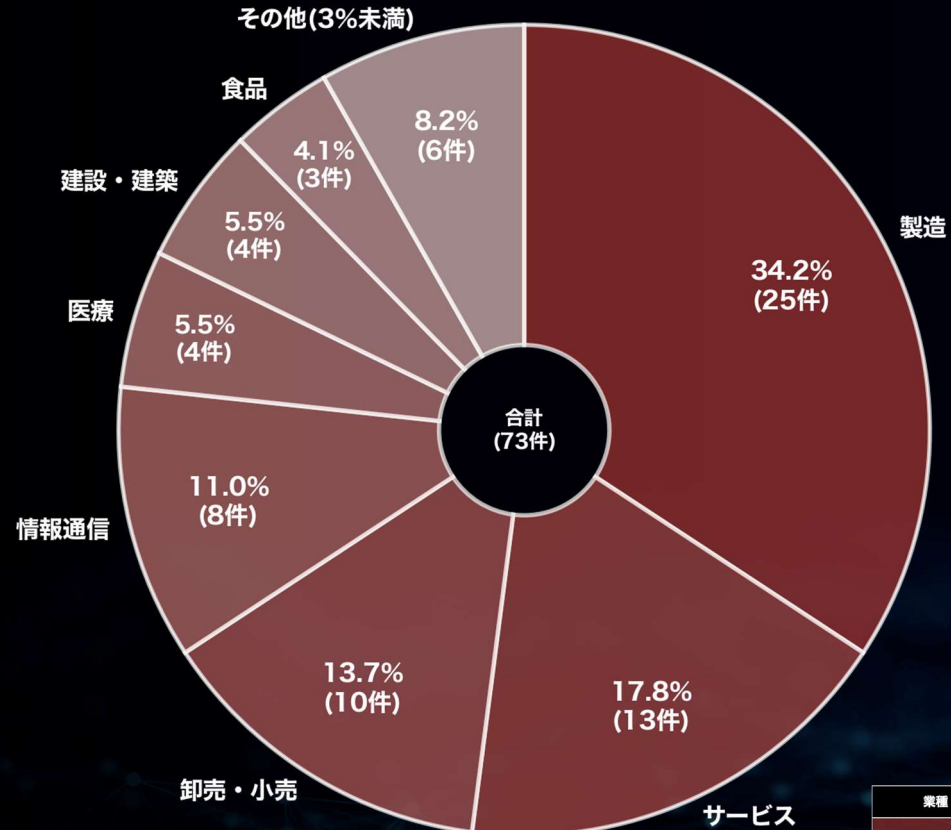
▼全体割合



※各数値の()内の数値は、資本金3億円未満の組織に対する集計結果を示す

業種	件数	割合(%)
製造	89 (25)	44.1 (12.4)
サービス	24 (13)	11.9 (6.4)
情報通信	17 (8)	8.4 (4.0)
卸売・小売	16 (10)	7.9 (5.0)
医療	11 (4)	5.4 (2.0)
教育	10 (1)	5.0 (0.5)
建設・建築	8 (4)	4.0 (2.0)
その他(3%未満)	27 (8)	13.4 (4.0)

▼中小企業のための割合



業種	件数	割合(%)
製造	25	34.2
サービス	13	17.8
卸売・小売	10	13.7
情報通信	8	11.0
医療	4	5.5
建設・建築	4	5.5
食品	3	4.1
その他(3%未満)	6	8.2

過去1年間の業種別分析においては、中小企業だけに抜粋すると、被害件数の割合は業種問わず、より全体に分散していることがわかる。

※医療や教育、行政機関など資本金が不明な一部の組織については集計から除外

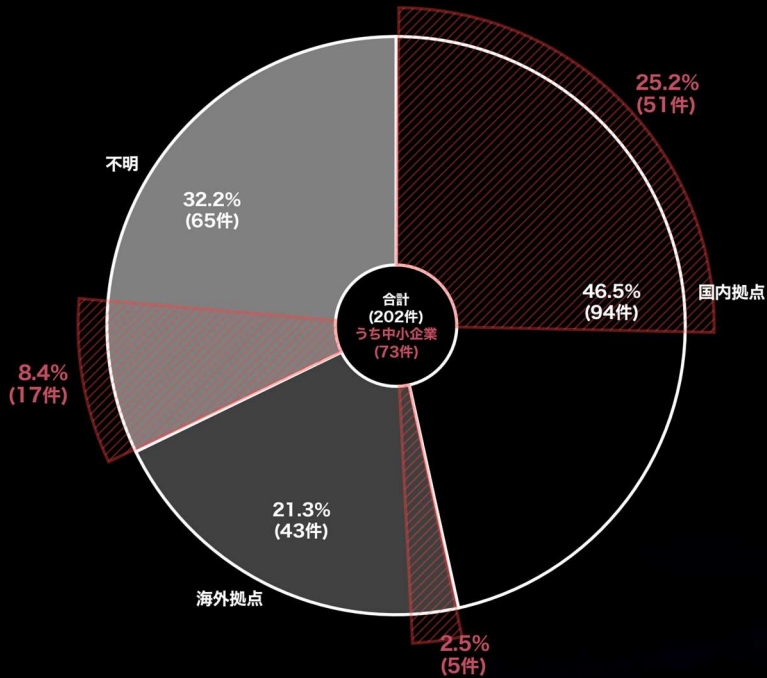
(※本ページの表/グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

公となった国内被害組織における拠点割合 (国内-中小企業)

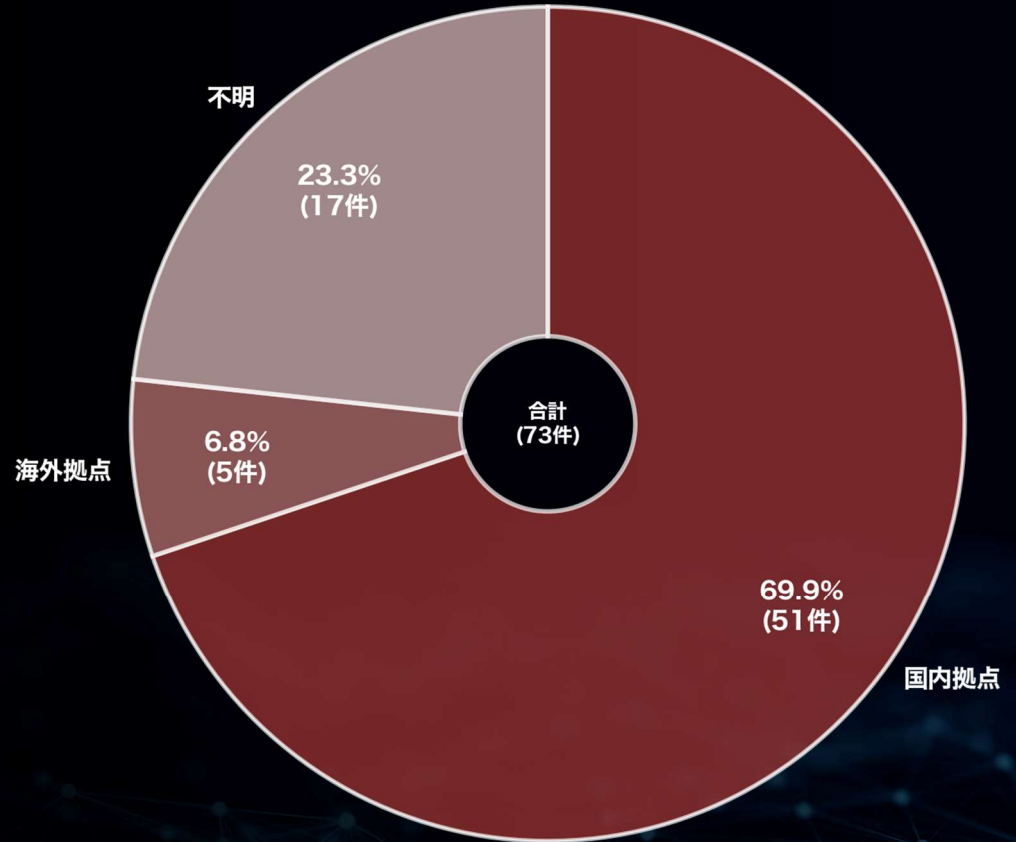
(過去1年間/2025年6月~2026年5月)

赤色は中小企業を示す

▼全体割合



▼中小企業のための割合



※ 「国内拠点」：公表等により、国内拠点における被害事案と判断されるケース数
 「海外拠点」：公表等により、海外拠点（支社/関係会社）における被害事案と判断されるケース数
 「不明」：上記以外、被害拠点の地域的情報が得られなかったケース数
 ※各数値の()内の数値は、資本金3億円未満の組織に対する集計結果を示す

拠点	件数 (中小企業)	割合 (%)
国内拠点	94 (51)	46.5 (25.2)
海外拠点	43 (5)	21.3 (2.5)
不明	65 (17)	32.2 (8.4)
合計	202 (73)	100 (36.1)

過去1年間の被害拠点の分析では、中小企業の国内拠点における被害割合が、全体と比較して高い傾向にある。

※医療や教育、行政機関など資本金が不明な一部の組織については集計から除外

拠点	件数 (中小企業)	割合 (%)
国内拠点	51	69.9
海外拠点	5	6.8
不明	17	23.3

(※本ページの表/グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

公となった国内被害組織概要一覧 (国内-中小企業)

(過去1年間/2025年6月~2026年5月)

赤色は中小企業を示す

被害月	攻撃グループ	業種概要
2025/6	(Unknown)	錠前・セキュリティ製品の販売
2025/6	(Unknown)	システムインテグレーター
2025/6	Qilin (Agenda)	医療機器メーカー(海外拠点)
2025/6	(Unknown)	ポンプ製造業
2025/6	(Unknown)	大手紳士服チェーン
2025/6	(Unknown)	保険事故調査サービス業
2025/6	(Unknown)	設備工事業
2025/6	(Unknown)	建材・住宅・リフォーム・不動産事業
2025/7	Kawa4096	大手保険会社
2025/7	NightSpire	ゴム製品メーカー(海外拠点)
2025/7	Kawa4096	警備サービス業
2025/7	Dire Wolf	電子デバイス製造・販売(海外拠点)
2025/7	(Unknown)	障害福祉サービス業
2025/7	(Unknown)	衛生管理製品・サービス業
2025/7	INC Ransom	高電圧電気機器メーカー(海外拠点)
2025/7	INC Ransom	ファンデーション資材メーカー
2025/7	LYNX	大手食品メーカー(海外拠点)
2025/7	DEVMAN 2.0	電子部品メーカー
2025/7	SAFEPAY	ハレル用補助材料メーカー
2025/7	(Unknown)	知的財産情報提供
2025/8	(Unknown)	ソフトウェア開発
2025/8	Black Nevas	特許事務所
2025/8	D4RK4RMY	大手金融機関
2025/8	Qilin (Agenda)	プラスチック製品製造業
2025/8	Qilin (Agenda)	自動車部品メーカー(海外拠点)
2025/8	Qilin (Agenda)	業務用食品卸・加工業
2025/8	(Unknown)	農産物加工・流通
2025/8	Warlock	精密機器メーカー(海外拠点)
2025/8	RansomHouse	電池・電子部品メーカー(海外拠点)
2025/8	Qilin (Agenda)	自動車向けデザイン
2025/8	WORLD LEAKS	毛織物メーカー
2025/8	(Unknown)	業務用・産業用加湿器メーカー
2025/8	(Unknown)	医療・介護事業者向けファクタリング
2025/8	Cephalus	システムインテグレーター

被害月	攻撃グループ	業種概要
2025/8	Black Nevas	大手自動車メーカー(海外拠点)
2025/8	(Unknown)	テーマパーク運営
2025/9	AKIRA	大手精密部品メーカー(海外拠点)
2025/9	Qilin (Agenda)	医療材料メーカー
2025/9	(Unknown)	産業機械・プラントメーカー
2025/9	(Unknown)	電気機器製造業(海外拠点)
2025/9	The Gentlemen	ゴム製品メーカー(海外拠点)
2025/9	COINBASE CARTEL	大手システムインテグレーター
2025/9	(Unknown)	大手工作機械メーカー(海外拠点)
2025/9	PLAY	建設機器メーカー(海外拠点)
2025/9	(Unknown)	商工会連合会
2025/9	J GROUP	大手商社(海外拠点)
2025/10	Scattered LAPSUS\$ Hu...	大手自動車メーカー
2025/10	Scattered LAPSUS\$ Hu...	大手スポーツ用品メーカー
2025/10	Scattered LAPSUS\$ Hu...	大手総合化学メーカー
2025/10	Qilin (Agenda)	大手飲料・食品メーカー
2025/10	(Unknown)	大学法人
2025/10	Rhysida	産業機械メーカー
2025/10	WORLD LEAKS	化粧品メーカー
2025/10	(Unknown)	金融機器メーカー
2025/10	AKIRA	各種機械組・刃物メーカー(海外拠点)
2025/10	(Unknown)	私立学校
2025/10	RansomHouse	有機化学工業品メーカー
2025/10	SAFEPAY	金属加工メーカー
2025/10	(Unknown)	ケーブルテレビ
2025/10	Qilin (Agenda)	食品スーパーマーケット
2025/10	Qilin (Agenda)	総合エネルギー企業
2025/10	Qilin (Agenda)	総合スーパー
2025/10	RansomHouse	大手EC小売事業者
2025/11	(Unknown)	私立大学
2025/11	WORLD LEAKS	プラスチック製品製造業
2025/11	Warlock	サスペンションメーカー
2025/11	Qilin (Agenda)	弁護士法人
2025/11	(Unknown)	システムインテグレーター

被害月	攻撃グループ	業種概要
2025/11	Qilin (Agenda)	通信機器メーカー
2025/11	(Unknown)	雑貨・アパレル小売
2025/11	CRYPTO24	電子部品メーカー
2025/11	CLOP (CLOP)	ラベル印刷機器メーカー
2025/11	INC Ransom	自動車部品メーカー(海外拠点)
2025/11	(Unknown)	教育委員会
2025/11	(Unknown)	私立学校
2025/11	CLOP (CLOP)	大手精密機器メーカー(海外拠点)
2025/11	CLOP (CLOP)	大手自動車メーカー
2025/11	CLOP (CLOP)	大手総合化学メーカー
2025/11	Sinobi	警報装置メーカー
2025/11	Qilin (Agenda)	大手建設会社(海外拠点)
2025/11	(Unknown)	精密部品製造
2025/11	(Unknown)	国際総合検定機関
2025/12	(Unknown)	エレクトロニクス専門商社(海外拠点)
2025/12	(Unknown)	教育系ITサービス提供
2025/12	AKIRA	食用油脂メーカー(海外拠点)
2025/12	Payouts King	プラスチック精密工業部品メーカー(海外拠点)
2025/12	COINBASE CARTEL	大手半導体メーカー
2025/12	INC Ransom	ワイヤーハーネスメーカー
2025/12	LYNX	総合テベロッパ
2025/12	Qilin (Agenda)	空調・衛生設備工事(海外拠点)
2025/12	(Unknown)	総合色材・機能性化学メーカー(海外拠点)
2025/12	root	金融商品取引所
2025/12	Qilin (Agenda)	大手テクノロジー企業(海外拠点)
2025/12	Rhysida	私立学校
2025/12	Qilin (Agenda)	電気機械部品メーカー(海外拠点)
2025/12	DragonForce	自動車部品メーカー(海外拠点)
2025/12	(Unknown)	公立大学
2025/12	(Unknown)	私立大学
2025/12	LYNX	映像制作
2025/12	SAFEPAY	ECサイト運営
2025/12	Qilin (Agenda)	ソフトウェア開発
2025/12	Qilin (Agenda)	精密部品メーカー(海外拠点)

※ (Unknown) の表記は攻撃グループ名が不明または公表されていないケースを表す。
 ※ (海外拠点) の表記は公表等により海外拠点であると判明した被害組織を表す。
 ※ 本ページの表の情報は、日本にフォーカスする関係上、リークサイトに掲載された情報に加えて国内被害組織からの公表や報道から判明した情報も含む

公となった国内被害組織概要一覧 (国内-中小企業)

(過去1年間/2025年6月~2026年5月)

赤色は中小企業を示す

過去1年間、中小企業でのランサムウェア被害が継続的に発生していることが分かる。特に近年の国内事例では、取引先企業にまで被害が広がるサプライチェーン攻撃が見受けられる。各企業の事業継続性を守ると同時に、サプライチェーン全体の安全性を高めるため、企業規模に関わらずセキュリティ対策を日々アップデートしていくことが望ましい。
※二次被害を受けた被害組織については本資料に記載していない

被害月	攻撃グループ	業種概要
2026/1	Qilin (Agenda)	工業用計測機器メーカー
2026/1	(Unknown)	印刷サービス
2026/1	(Unknown)	ソフトウェア開発
2026/1	(Unknown)	図書整備支援
2026/1	(Unknown)	総合化学商社
2026/1	(Unknown)	生産用機械器具製造業(海外拠点)
2026/1	Everest	大手自動車メーカー
2026/1	(Unknown)	不動産管理
2026/1	Orion Leaks	タイヤメーカー(海外拠点)
2026/1	(Unknown)	飲料メーカー
2026/1	(Unknown)	スポーツ教室
2026/1	The Gentlemen	産業廃棄物処理
2026/1	Brain Cipher	システムインテグレーター
2026/2	Qilin (Agenda)	特殊金属材料・製造
2026/2	Everest	機械器具製造
2026/2	Everest	金属加工メーカー
2026/2	(Unknown)	大手化学素材メーカー(海外拠点)
2026/2	OAPT	大手電気機器メーカー
2026/2	OAPT	大手テクノロジー企業
2026/2	OAPT	自動制御機器製品メーカー
2026/2	(Unknown)	ペット関連用品製造
2026/2	OAPT	医療機器メーカー
2026/2	OAPT	医療機器メーカー
2026/2	(Unknown)	スキー場運営
2026/2	INC Ransom	国際貨物運送取扱業
2026/2	The Gentlemen	伝熱管メーカー
2026/2	OAPT	タイヤメーカー
2026/2	OAPT	総合電機メーカー
2026/2	OAPT	大手自動車メーカー
2026/2	OAPT	建設機械メーカー
2026/2	OAPT	総合電機メーカー
2026/2	(Unknown)	ソフトウェア開発
2026/2	Qilin (Agenda)	総合テペロッパー
2026/2	(Unknown)	ホテル業・飲食店業

被害月	攻撃グループ	業種概要
2026/2	OAPT	鉄道会社
2026/2	OAPT	地方自治体
2026/2	OAPT	電力会社
2026/2	OAPT	地方自治体
2026/2	Qilin (Agenda)	種苗メーカー兼商社(海外拠点)
2026/2	NightSpire	繊維・衣料関連卸売業
2026/2	(Unknown)	半導体試験装置メーカー
2026/2	NetRunner	総合病院
2026/2	LockBit	機械・工具メーカー(海外拠点)
2026/2	BLACKSHRANTAC	紳士服・婦人服販売
2026/2	NightSpire	モータースポーツチーム運営
2026/2	(Unknown)	印刷会社
2026/2	INC Ransom	石油製品・LPガス販売
2026/2	The Gentlemen	材料加工装置メーカー
2026/2	Everest	商用車メーカー
2026/3	(Unknown)	市場調査・コンサルティング
2026/3	NetRunner	療養型病院
2026/3	(Unknown)	FAX通信・BPOサービス
2026/3	(Unknown)	工業用ゴム・樹脂・配管資材商社
2026/3	(Unknown)	住宅・商業施設向けリペア
2026/3	(Unknown)	美容クリニック
2026/3	(Unknown)	シティホテル運営
2026/3	The Gentlemen	医療・看護専門出版社
2026/3	Space Bears	介護・カラオケ・飲食事業
2026/3	(Unknown)	光半導体デバイスメーカー(海外拠点)
2026/3	WORLD LEAKS	広告・制作
2026/3	The Gentlemen	繊維加工・食品加工メーカー
2026/3	(Unknown)	設備工事
2026/3	(Unknown)	美容室向け化粧品メーカー
2026/3	ALP-001	国立研究開発法人
2026/4	AKIRA	流体システム製品メーカー
2026/4	(Unknown)	非鉄金属・資源開発(海外拠点)
2026/4	(Unknown)	システムインテグレーター

被害月	攻撃グループ	業種概要
2026/4	KRYBIT	酒類製造業
2026/4	LockBit	水処理・環境設備
2026/4	DragonForce	オフィス家具メーカー(海外拠点)
2026/4	(Unknown)	診療予約システム開発
2026/4	Qilin (Agenda)	舗装・土木工事
2026/4	The Gentlemen	電気機器メーカー
2026/4	Qilin (Agenda)	建設資材・福祉用具のレンタル・販売
2026/4	(Unknown)	生活協同組合
2026/4	COINBASE CARTEL	大学研究会
2026/4	Ransom EXX	ソフトウェア開発
2026/4	LockBit	電子部品(コネクタ)製造(海外拠点)
2026/4	(Unknown)	二輪用品専門チェーン
2026/4	The Gentlemen	ソフトウェア開発
2026/4	Qilin (Agenda)	大手自動車部品メーカー(海外拠点)
2026/5	(Unknown)	百貨店業・不動産賃貸業
2026/5	(Unknown)	不動産コンサルティング・資産管理
2026/5	FulcrumSec	移植医療支援
2026/5	KILLSEC	オンライン処方箋サービス
2026/5	(Unknown)	教育サービス・学習教材
2026/5	AIlock	半導体製造装置・精密機器メーカー(海外拠点)
2026/5	The Gentlemen	医薬品卸売業
2026/5	The Gentlemen	商業施設運営サービス
2026/5	SAFEPAY	産業資材商社
2026/5	AKIRA	家電メーカー(海外拠点)
2026/5	Lynx	水処理装置メーカー(海外拠点)
2026/5	Lynx	蓄電池・電源システム(海外拠点)
2026/5	The Gentlemen	ジュエリー輸入・企画販売
2026/5	Payload	空調設備施工
2026/5	The Gentlemen	ガラス容器メーカー
2026/5	NightSpire	医薬品・食品関連製造(海外拠点)
2026/5	(Unknown)	国立大学法人
2026/5	SAFEPAY	紙器製造
2026/5	SAFEPAY	建材リペア・再生工事

※ (Unknown) の表記は攻撃グループ名が不明または公表されていないケースを表す。
 ※ (海外拠点) の表記は公表等により海外拠点であると判明した被害組織を表す。
 ※ 本ページの表の情報は、日本にフォーカスする関係上、リークサイトに掲載された情報に加えて国内被害組織からの公表や報道から判明した情報も含む

多重被害に関する分析

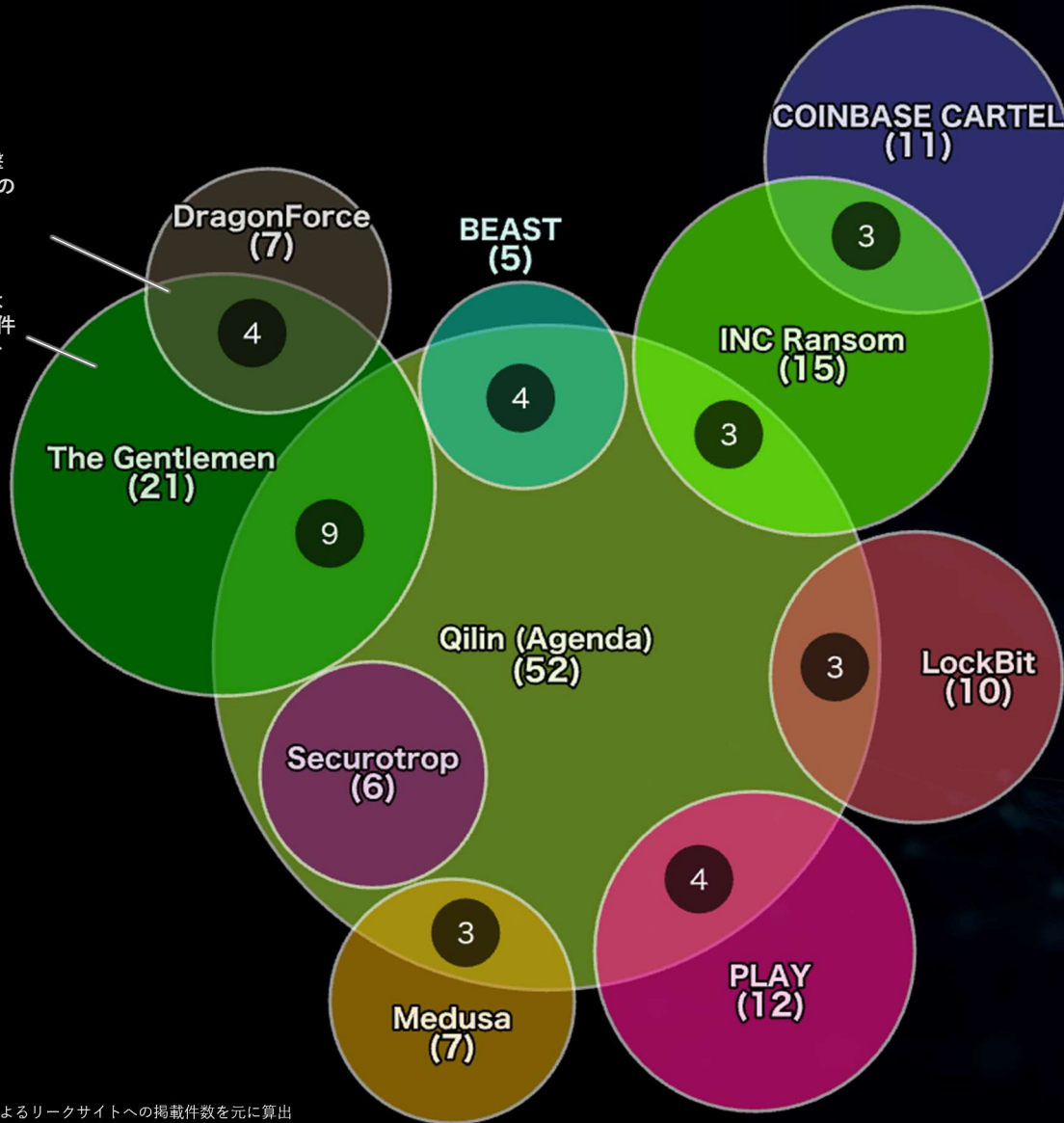
2026

5

繰り返し暴露された事案数の集計と攻撃グループ間の関係性 (全世界)

(過去1年間 / 2025年6月～2026年5月) (累計135件) ※多重被害に遭った組織数の累計

- ※ 円の重なりは他攻撃グループと3件以上の重なりを表している。
- ※ 重なりのない部分は他攻撃グループと3件未満の事案の重複を表している。



ランサムウェア攻撃の被害の中には、データを盗まれたのちにリークサイトで暴露され、さらに異なる攻撃グループのリークサイトなどから二度三度と繰り返し暴露されるケースがある。つまり言い換えると、ランサムウェア攻撃の被害組織の中には、複数回にわたってリークサイトに情報が掲載される「多重被害」に遭う組織が存在する。

有名な事例としては、AlphV (BlackCat)のアフィリエイトが被害組織のデータを他の攻撃グループに持ち込んだことで、その被害組織が異なる攻撃グループから連続して脅迫されてしまったというケースが挙げられる。これは攻撃グループの内部で起きた報酬支払いに関する内輪揉めが原因であるが、多重被害の原因は多岐にわたる。

例えば

- ・ 被害後の対策不足による再侵入
- ・ 攻撃グループ間の連携によるデータの横流し
- ・ 攻撃グループによる他グループのリークサイトやハッカーフォーラムからのデータ盗用
- ・ 攻撃グループメンバーやアフィリエイトによるデータの持ち出しなどが理由の一部として挙げられる。

一度盗まれたデータの流用を完全に防ぐことは困難だが、複数回の侵入による多重被害は、インシデント発生時の適切な対応とその後の対策により、防御の可能性を大幅に高めることができる。

ランサムウェア被害発生を想定し、有事の際に冷静な対応ができるよう、対策のための情報の一つとして多重被害の実態を把握しておくことも重要である。

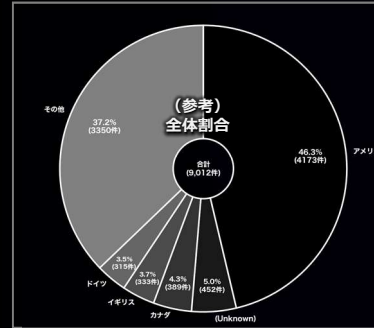
※異なる攻撃グループによるリークサイトへの掲載件数を元に算出

多重被害に遭った被害組織の傾向と分析 (全世界)

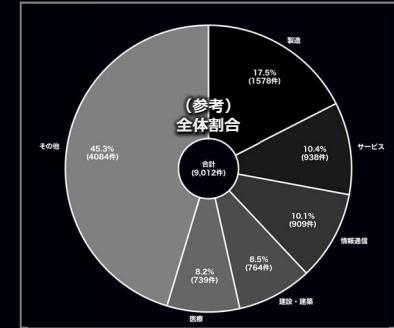
(過去1年間 / 2025年6月～2026年5月)

※多重被害：一度ランサムウェア攻撃の被害を受けた組織が異なる時期に異なる攻撃グループのリークサイトに再び掲載されるケース

(参考比較) 同期間の全データにおける割合

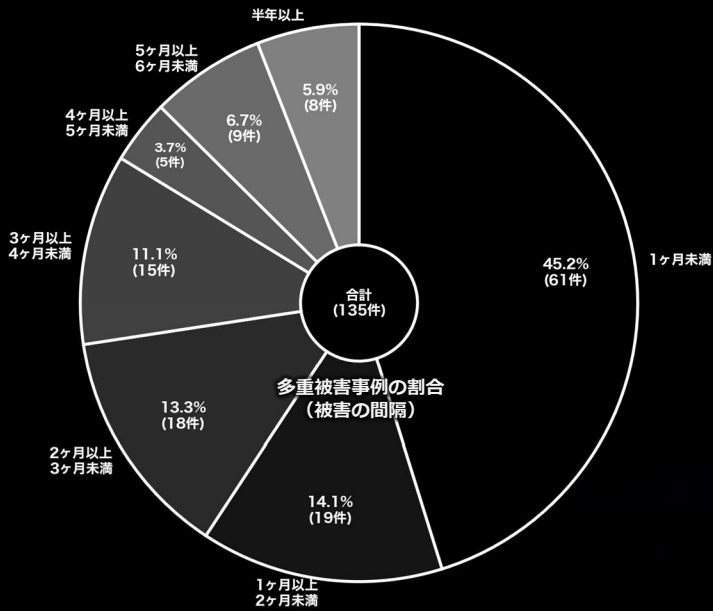


(参考比較) 同期間の全データにおける割合

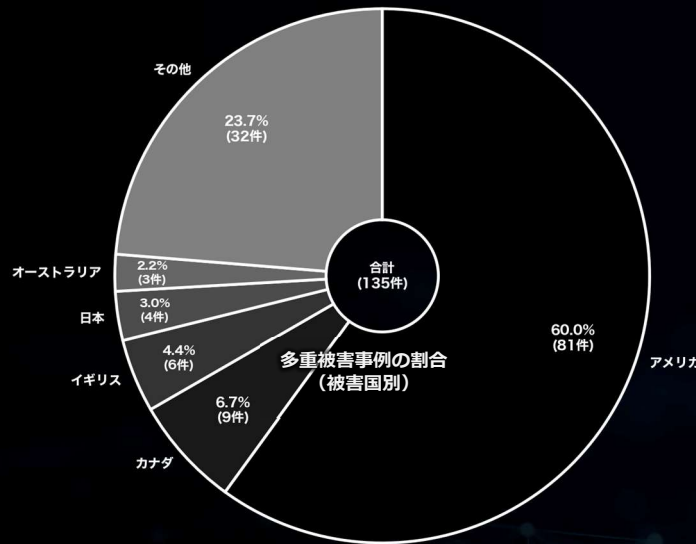


▼被害の間隔

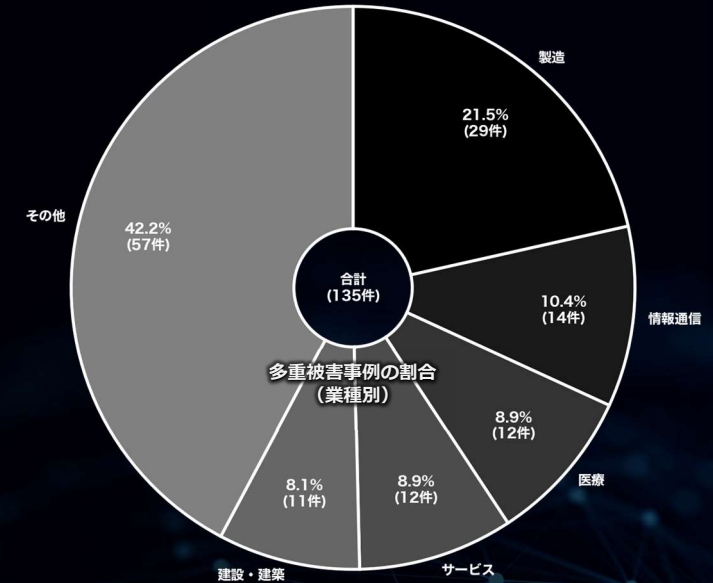
(一度目の被害から二度目の被害までの間隔)



▼被害国別



▼業種別



▶多重被害に遭った組織数の累計：135件 (全体9012件中)

※異なる攻撃グループによるリークサイトへの掲載件数を元に算出

全体母数からの割合は少ないものの、一度ランサムウェア攻撃を受けた被害組織は、異なる時期に異なる攻撃グループによって再びリークサイトへ掲載される被害を繰り返す場合があり、中には3回以上被害に遭うケースもある。これは事後対応が不十分で再び侵入されるケースや、流出した暴露データが裏で共有・拡散され繰り返し脅されるケースなどの背景があると考えられる。被害国や業種の観点ではほぼ全体割合の縮図となっているものの、最も注目すべきは繰り返される「被害の間隔」であり、実に70%以上が一度目の掲載から2ヶ月以内に再び発生していることが判明した。これら多重被害の事例には日本関連の組織も含まれており、一度侵入されデータ窃取されれば、いかなる組織でも多重被害に遭う可能性がある事を示す。こうした被害を防ぐためには、日頃からの対策に加え万が一ランサムウェアの被害に遭っても身代金を支払わない(脅せば支払う組織であると認知されてしまう)ことや、繰り返しの侵入を防ぐために侵入経路の徹底的な洗い出し等の事後対応・再発防止策の実施が不可欠である。

業種に関する分析

(過去2年間のリークサイト掲載上位10業種)

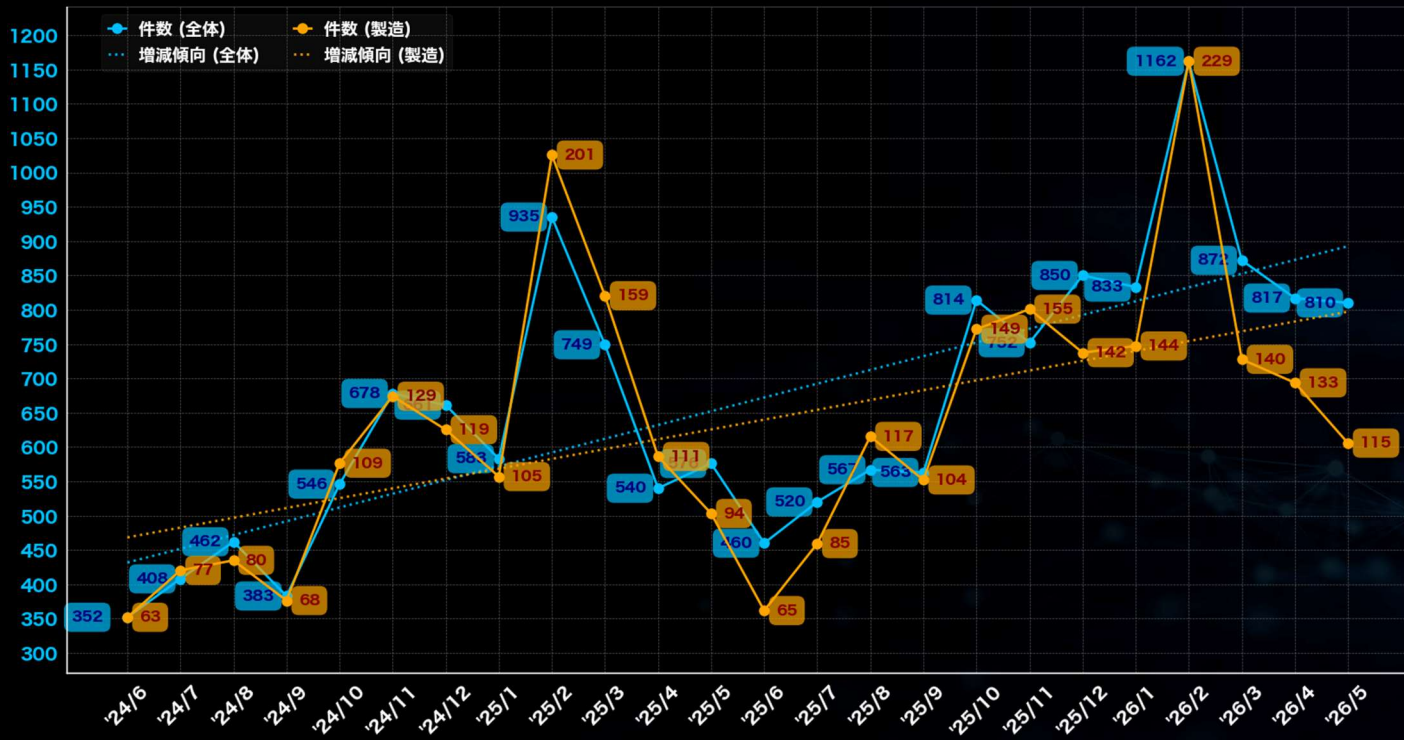
2026
5

業種に関する分析 (全世界)

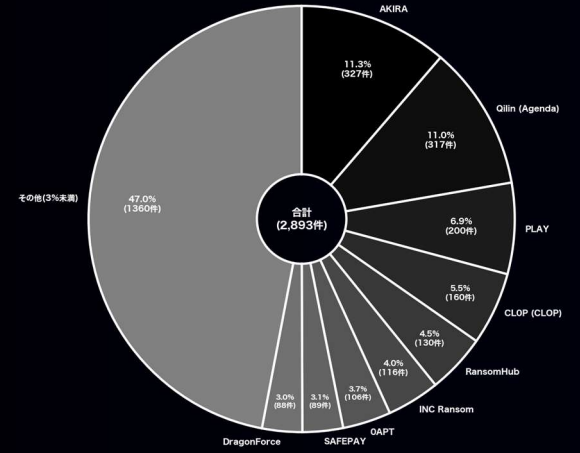
(過去2年間 / 2024年6月～2026年5月)

製造

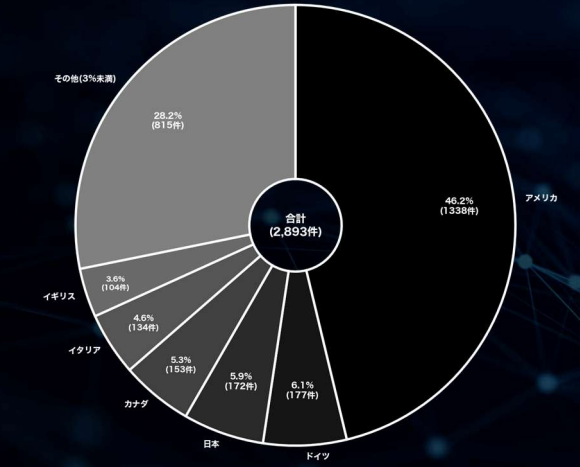
「製造」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年2月で、229件の掲載があった。一方、最も少なかった月は2024年6月で、63件であった。被害組織の所在国の割合では、アメリカが約46%と最も多く、次いでドイツと日本がそれぞれ約6%である。攻撃グループについては、少なくとも146のグループが関与しており、特に「AKIRA」が327件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「PLAY」がそれぞれ317件と200件の掲載を行っている。製造関連の件数は全体件数に対して高い割合で推移しており、全体件数を引き上げている。全世界的に被害が多い業種であるが、日本関連組織においても多くの被害が出ている状況や、長期にわたり増加傾向にあることから、今後も国内外問わず被害が増加する可能性がある。



▼攻撃グループ別



▼国別



(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

業種に関する分析 (全世界)

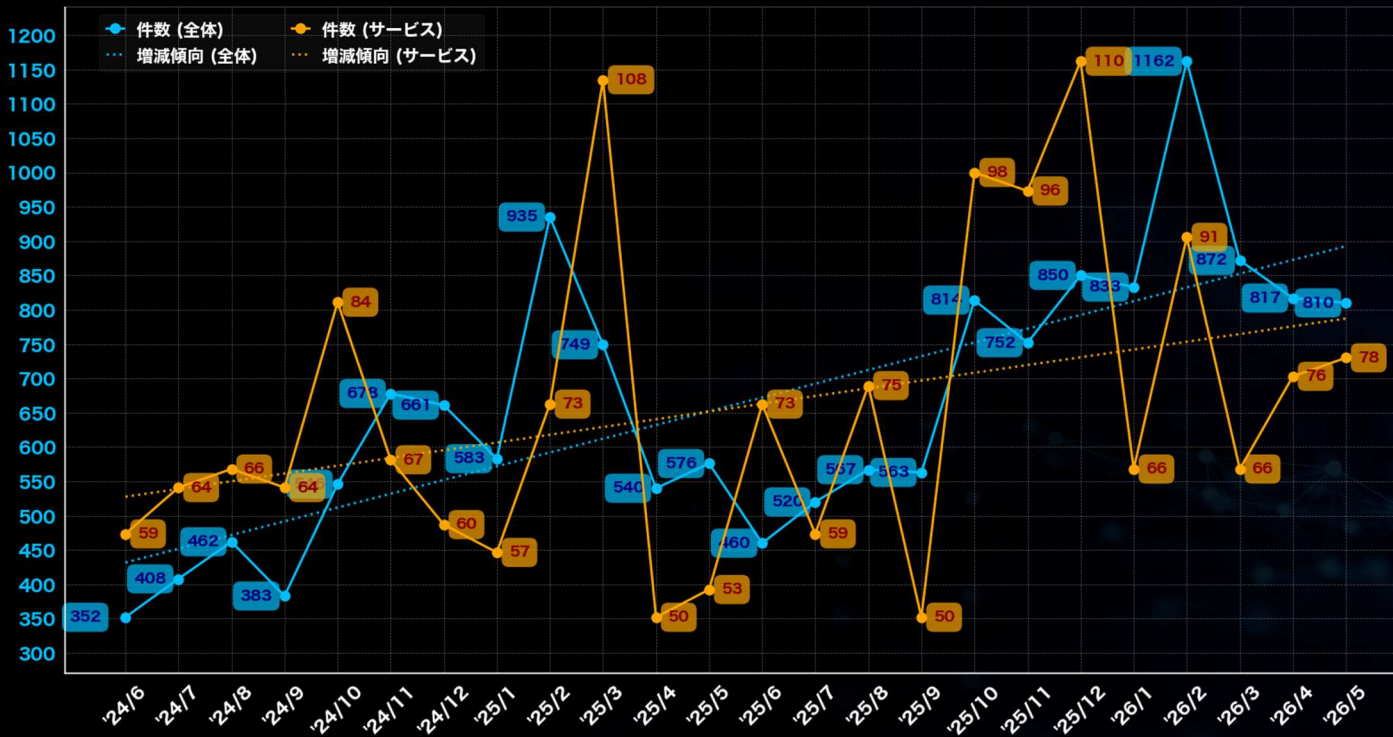
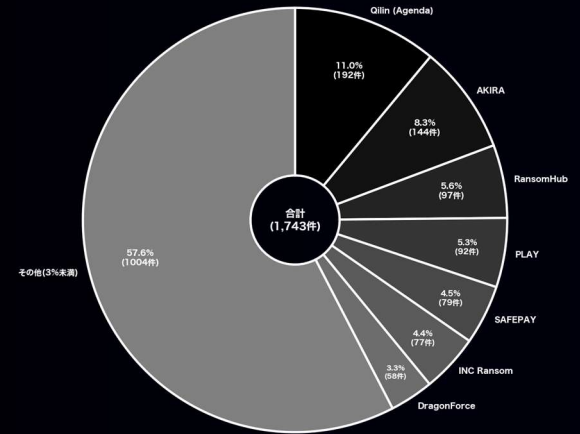
(過去2年間 / 2024年6月～2026年5月)



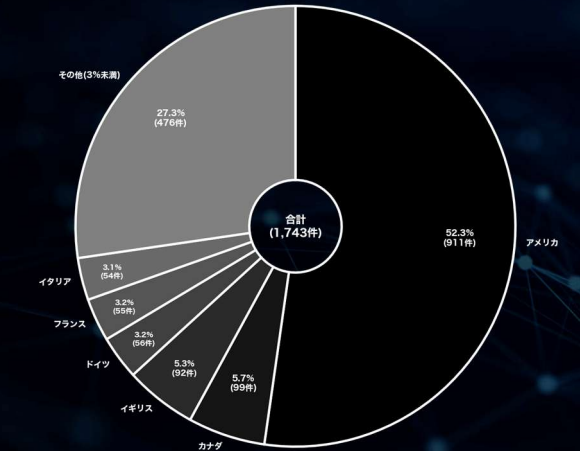
サービス

「サービス」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年12月で、110件の掲載があった。一方、最も少なかった月は2025年4月および2025年9月で、50件であった。被害組織の所在国の割合では、アメリカが約52%と最も多く、次いでカナダとイギリスがそれぞれ約6%と約5%である。攻撃グループについては、少なくとも140のグループが関与しており、特に「Qilin (Agenda)」が192件のリークサイト掲載を実施している。次いで「AKIRA」と「RansomHub」がそれぞれ144件と97件の掲載を行っている。サービス関連の件数は製造関連と同じく全体件数に対し、高い割合をキープしており、年々その割合は高まっている。

▼攻撃グループ別



▼国別



(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照



業種に関する分析 (全世界)

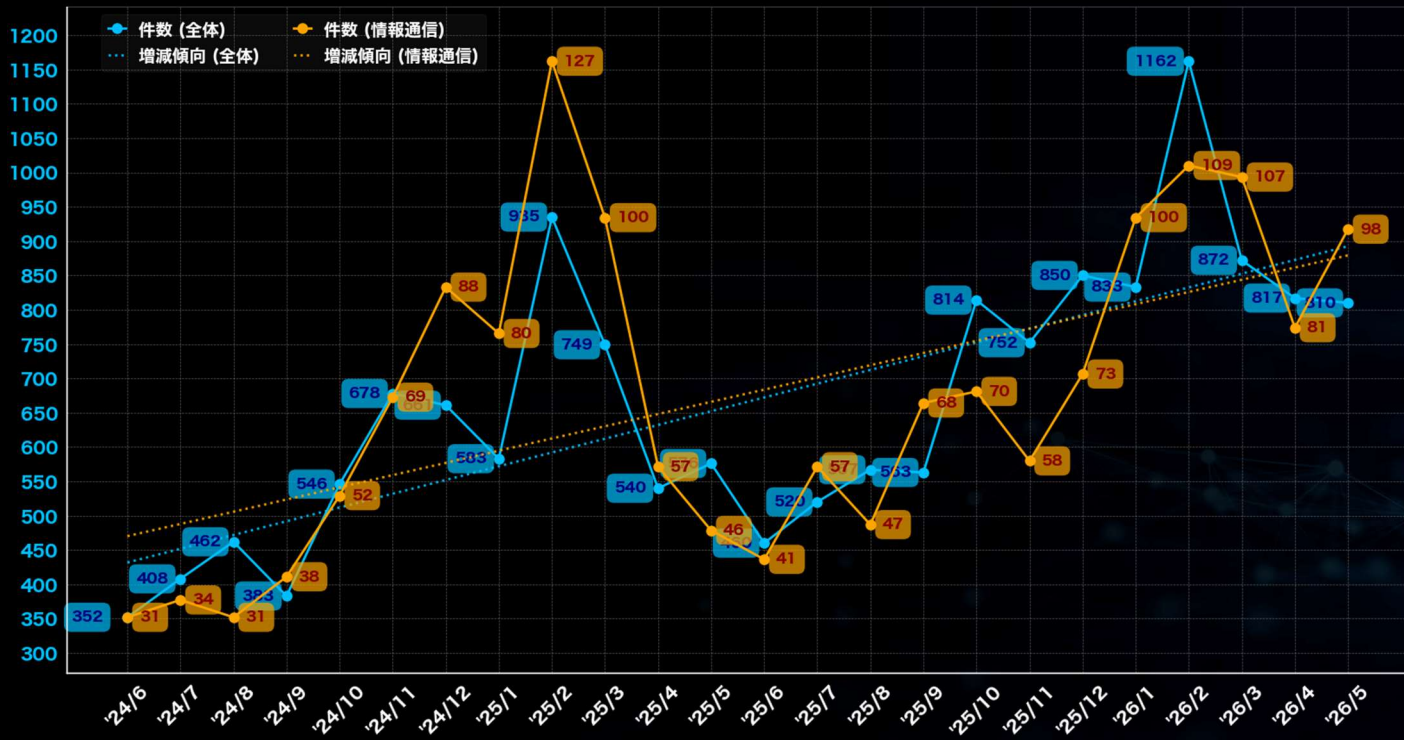
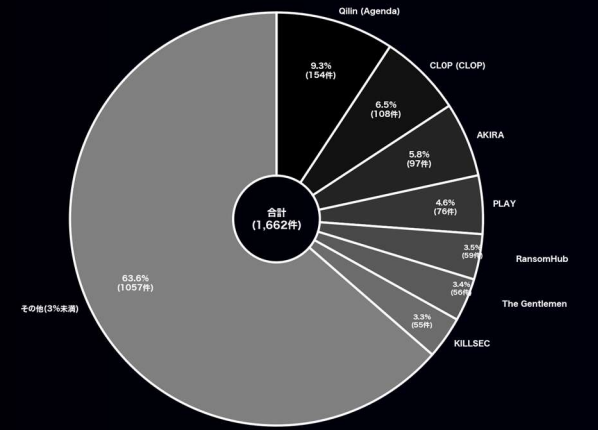
(過去2年間 / 2024年6月 ~ 2026年5月)



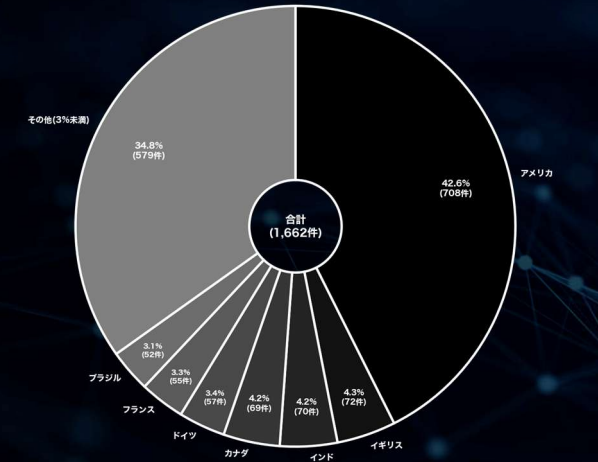
情報通信

「情報通信」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、127件の掲載があった。一方、最も少なかった月は2024年6月および2024年8月で、31件であった。被害組織の所在国の割合では、アメリカが約43%と最も多く、次いでイギリスとインドがそれぞれ約4%である。攻撃グループについては、少なくとも147のグループが関与しており、特に「Qilin (Agenda)」が154件のリークサイト掲載を実施している。次いで「CLOP (CLOP)」と「AKIRA」がそれぞれ108件と97件の掲載を行っている。情報通信業界は技術情報や顧客データを多く保有することから、引き続きランサムウェア攻撃の主要な標的となっており、関与グループ数も製造業と並ぶ規模となっている。

▼攻撃グループ別



▼国別



(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

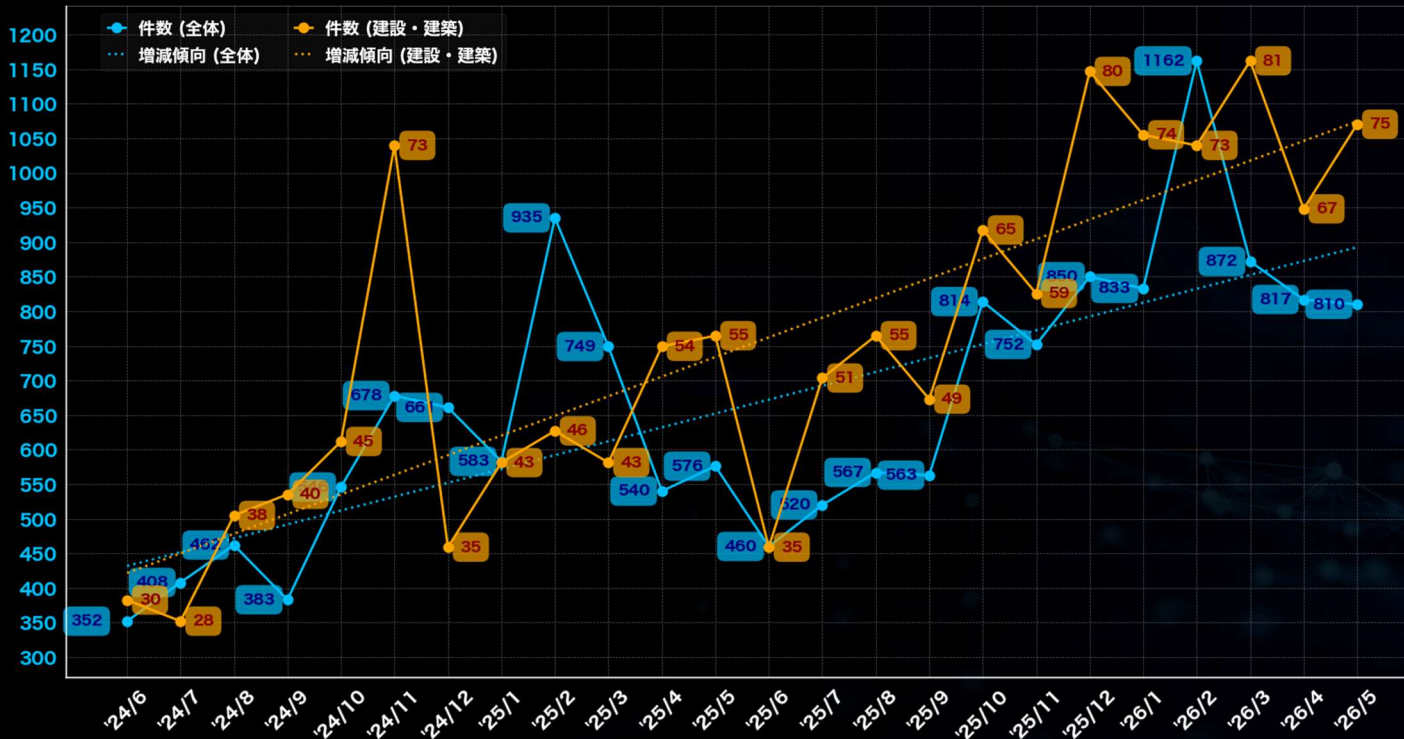


業種に関する分析 (全世界)

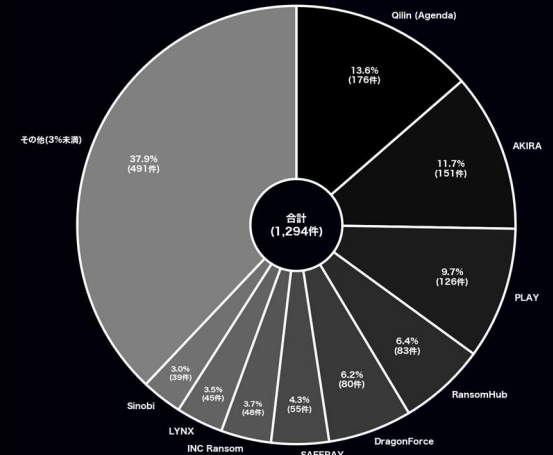
(過去2年間 / 2024年6月～2026年5月)

建設・建築

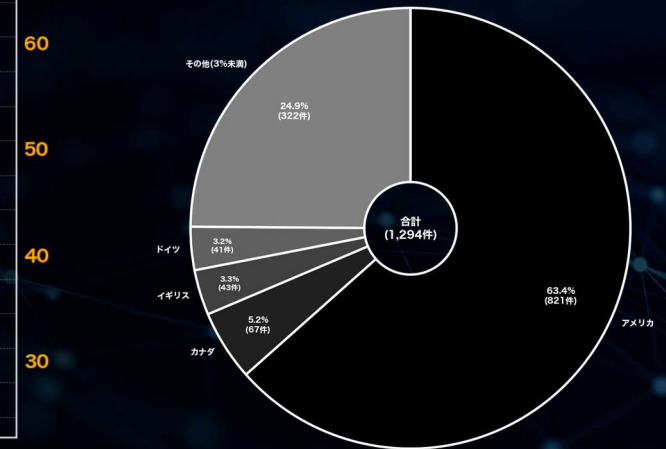
「建設・建築」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年3月で、81件の掲載があった。一方、最も少なかった月は2024年7月で、28件であった。被害組織の所在国の割合では、アメリカが約63%と最も多く、次いでカナダとイギリスがそれぞれ約5%と約3%である。攻撃グループについては、少なくとも112のグループが関与しており、特に「Qilin (Agenda)」が176件のリークサイト掲載を実施している。次いで「AKIRA」と「PLAY」がそれぞれ151件と126件の掲載を行っている。建設・建築業界はアメリカに被害が集中しており、攻撃対象としての偏りが顕著に表れている。



▼攻撃グループ別



▼国別



(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

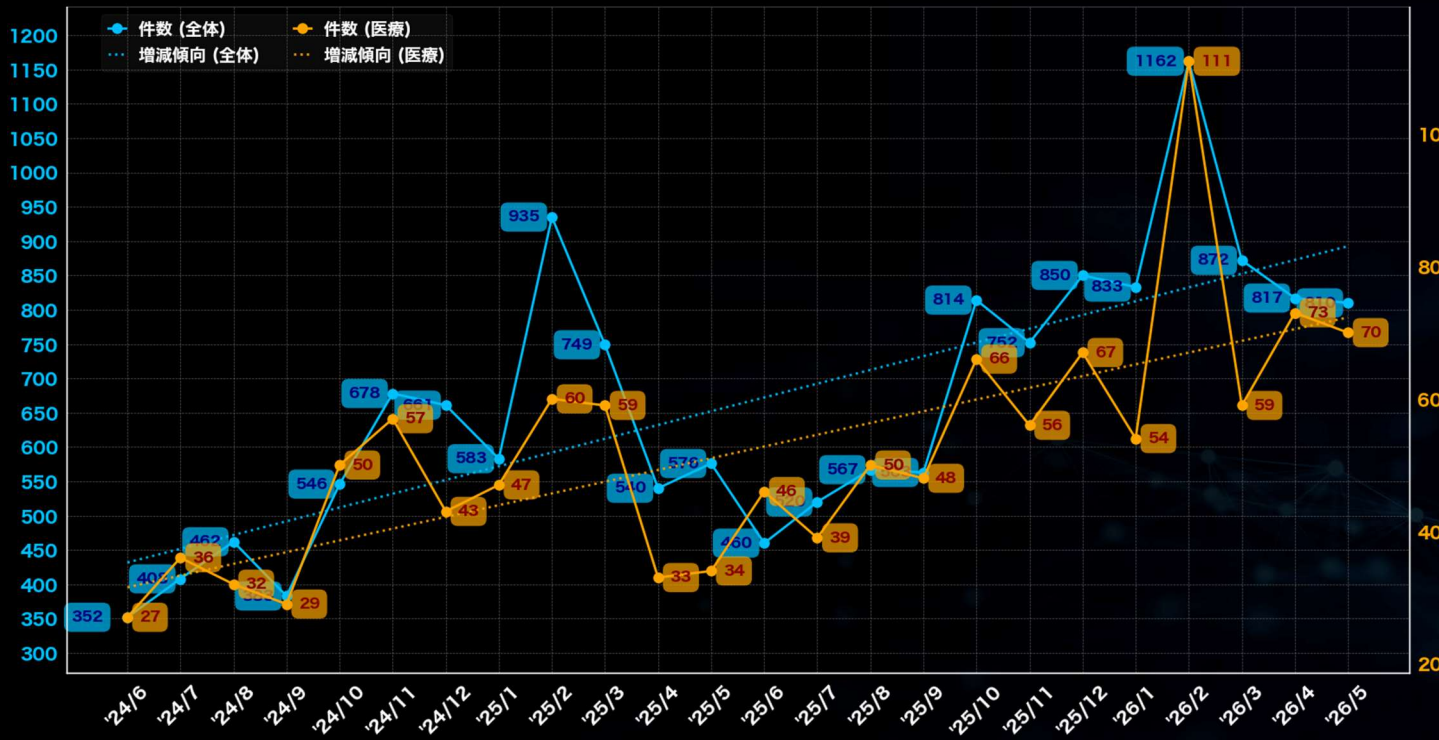
業種に関する分析 (全世界)

(過去2年間 / 2024年6月～2026年5月)

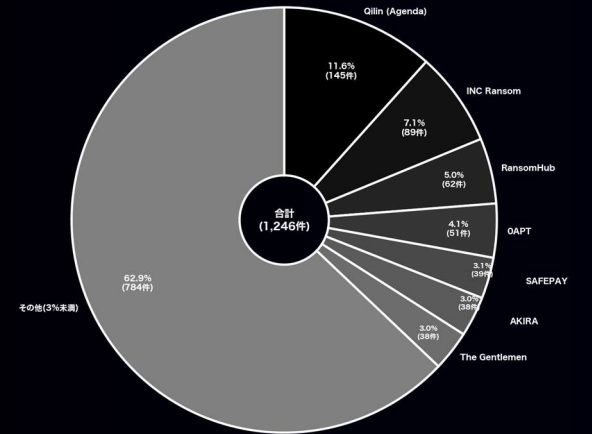


医療

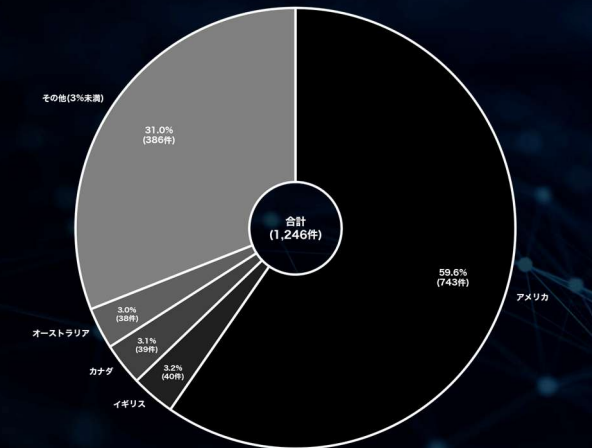
「医療」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年2月で、111件の掲載があった。一方、最も少なかった月は2024年6月で、27件であった。被害組織の所在国の割合では、アメリカが約60%と最も多く、次いでイギリスとカナダがそれぞれ約3%である。攻撃グループについては、少なくとも125のグループが関与しており、特に「Qilin (Agenda)」が145件のリークサイト掲載を実施している。次いで「INC Ransom」と「RansomHub」がそれぞれ89件と62件の掲載を行っている。医療業界は患者情報など機微なデータを保有することから、依然として攻撃者の標的となっている。



▼攻撃グループ別



▼国別



(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

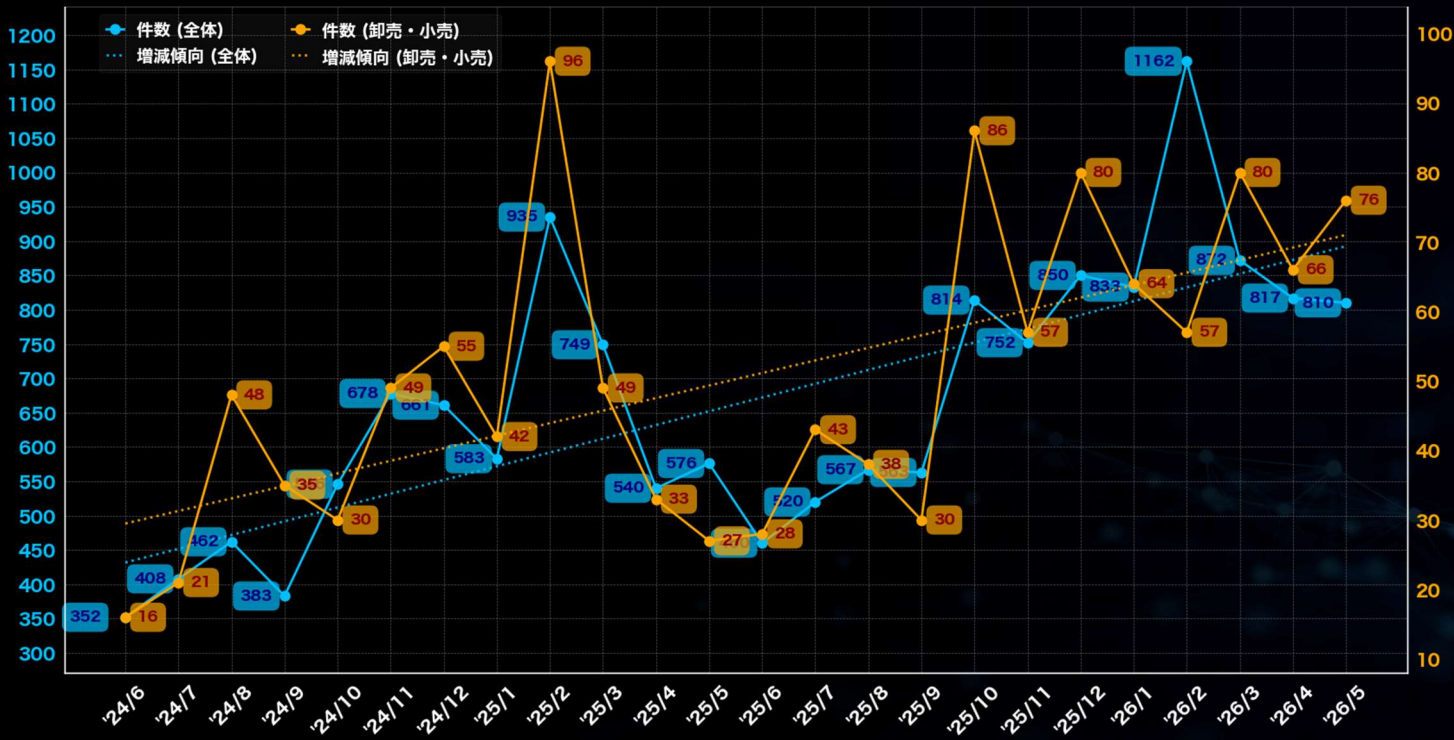


業種に関する分析 (全世界)

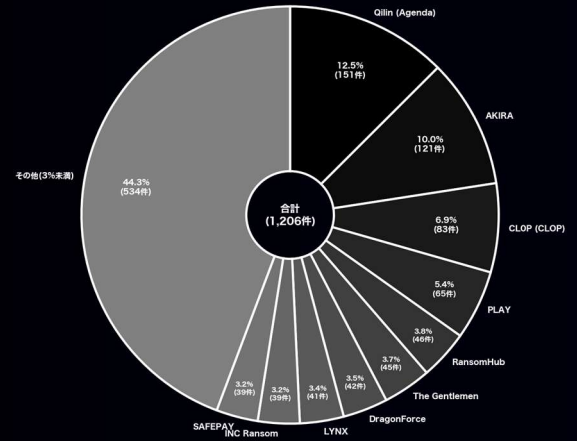
(過去2年間 / 2024年6月 ~ 2026年5月)

卸売・小売

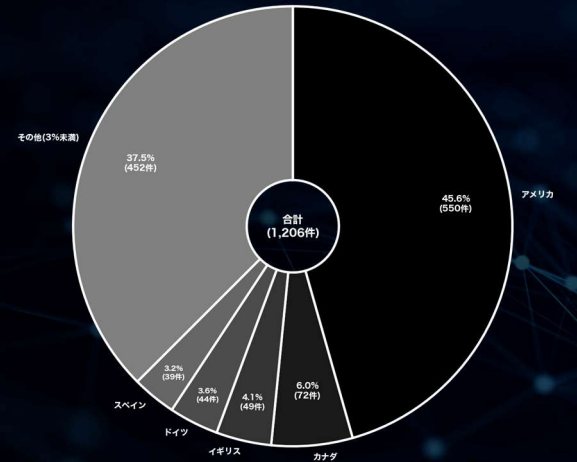
「卸売・小売」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、96件の掲載があった。一方、最も少なかった月は2024年6月で、16件であった。被害組織の所在国の割合では、アメリカが約46%と最も多く、次いでカナダとイギリスがそれぞれ約6%と約4%である。攻撃グループについては、少なくとも114のグループが関与しており、特に「Oilin (Agenda)」が151件のリークサイト掲載を実施している。次いで「AKIRA」と「CLOP (CLOP)」がそれぞれ121件と83件の掲載を行っている。卸売・小売業界は最大月と最小月の差が大きく月次変動の激しい業種でありながら、全体としては増加傾向が続いている。



▼攻撃グループ別



▼国別



(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

業種に関する分析 (全世界)

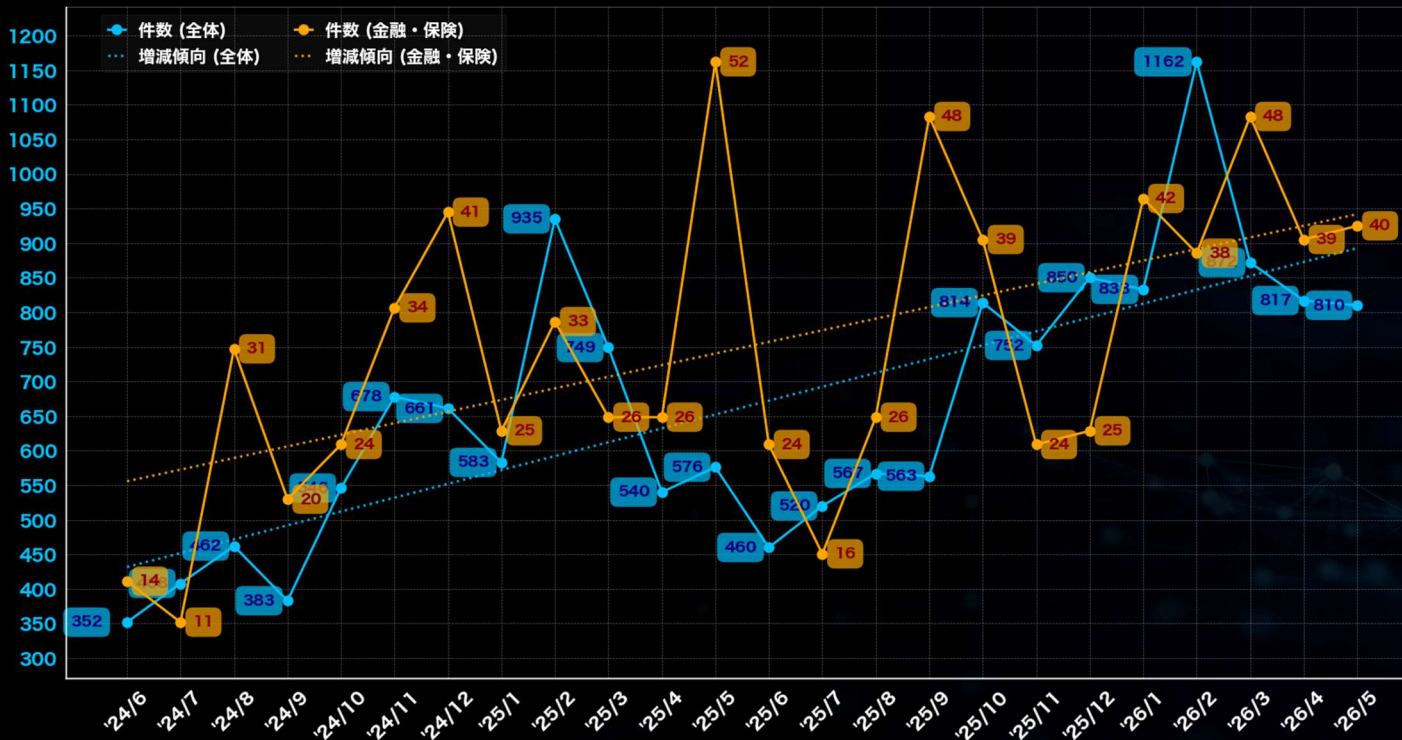
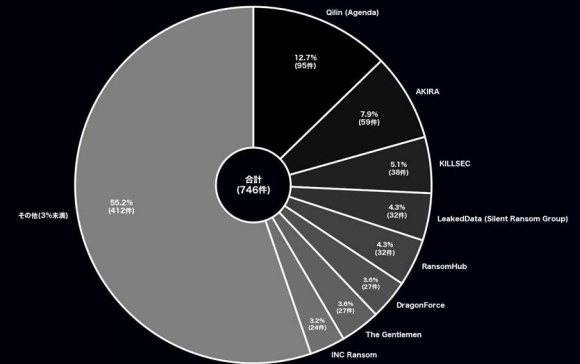
(過去2年間 / 2024年6月～2026年5月)



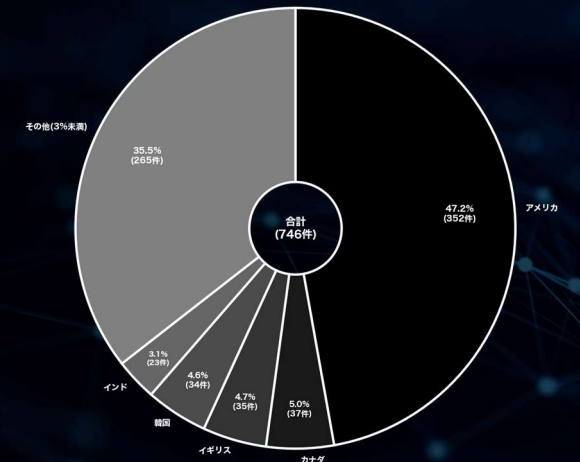
金融・保険

「金融・保険」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年5月で、52件の掲載があった。一方、最も少なかった月は2024年7月で、11件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いでカナダとイギリスがそれぞれ約5%である。攻撃グループについては、少なくとも114のグループが関与しており、特に「Qilin (Agenda)」が95件のリークサイト掲載を実施している。次いで「AKIRA」と「KILLSEC」がそれぞれ59件と38件の掲載を行っている。金融・保険業界は被害件数こそ他業界に比べ少ないものの、関与する攻撃グループは114と多岐にわたっており、引き続き警戒が必要である。

▼攻撃グループ別



▼国別



(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照



業種に関する分析 (全世界)

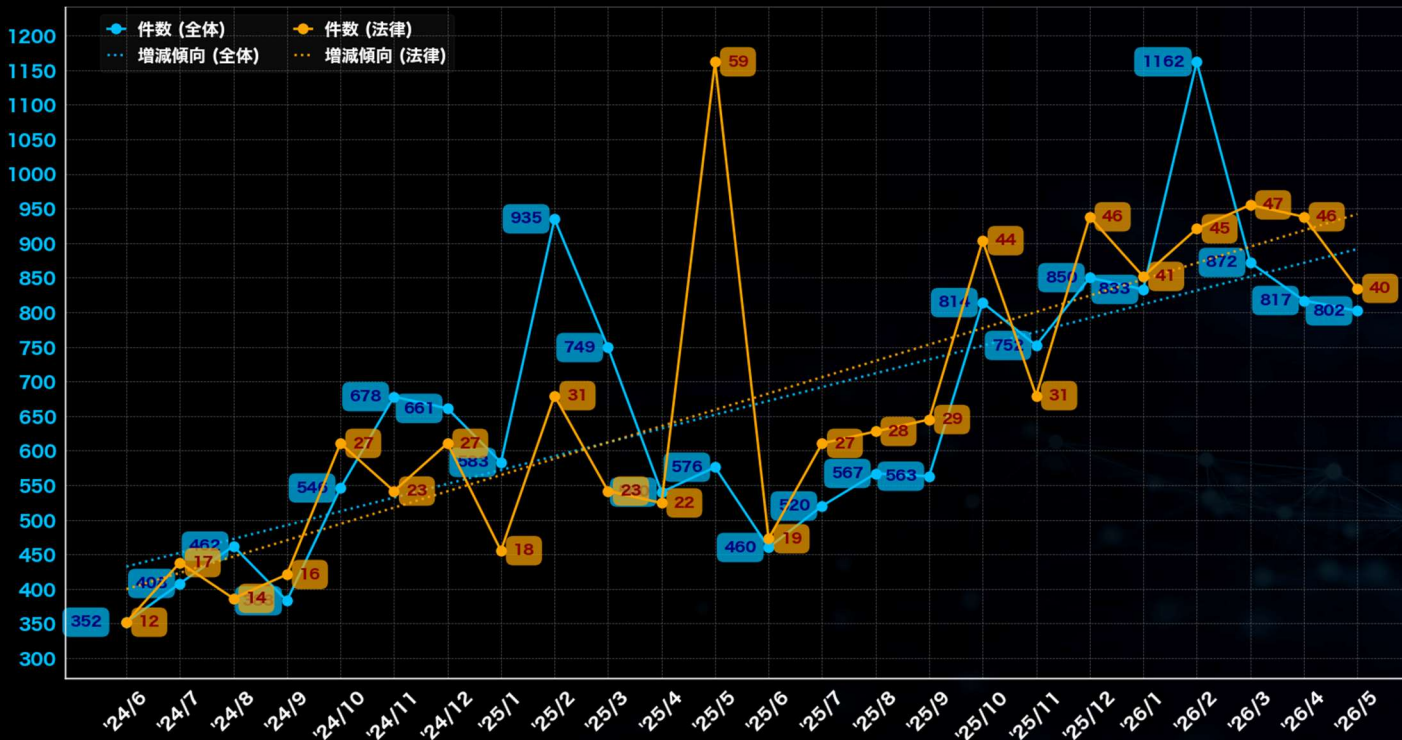
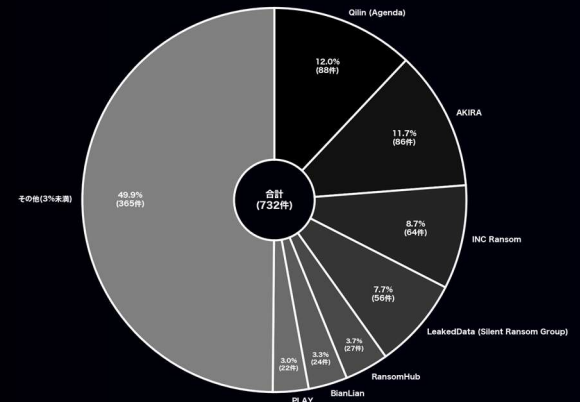
(過去2年間 / 2024年6月～2026年5月)



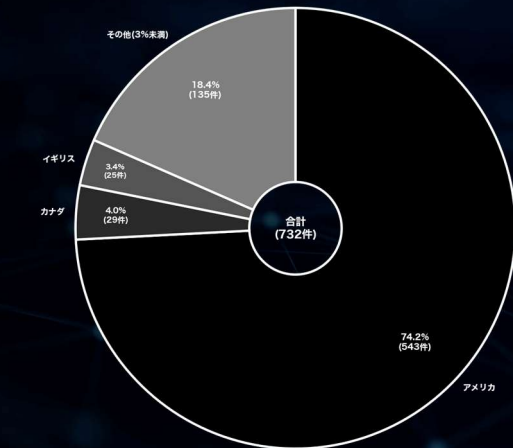
法律

「法律」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年5月で、59件の掲載があった。一方、最も少なかった月は2024年6月で、12件であった。被害組織の所在国の割合では、アメリカが約74%と最も多く、次いでカナダとイギリスがそれぞれ約4%と約3%である。攻撃グループについては、少なくとも92のグループが関与しており、特に「Qilin (Agenda)」が88件のリークサイト掲載を実施している。次いで「AKIRA」と「INC Ransom」がそれぞれ86件と64件の掲載を行っている。法律業界はアメリカの被害が極端に集中している点も特徴である。

▼攻撃グループ別



▼国別



(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

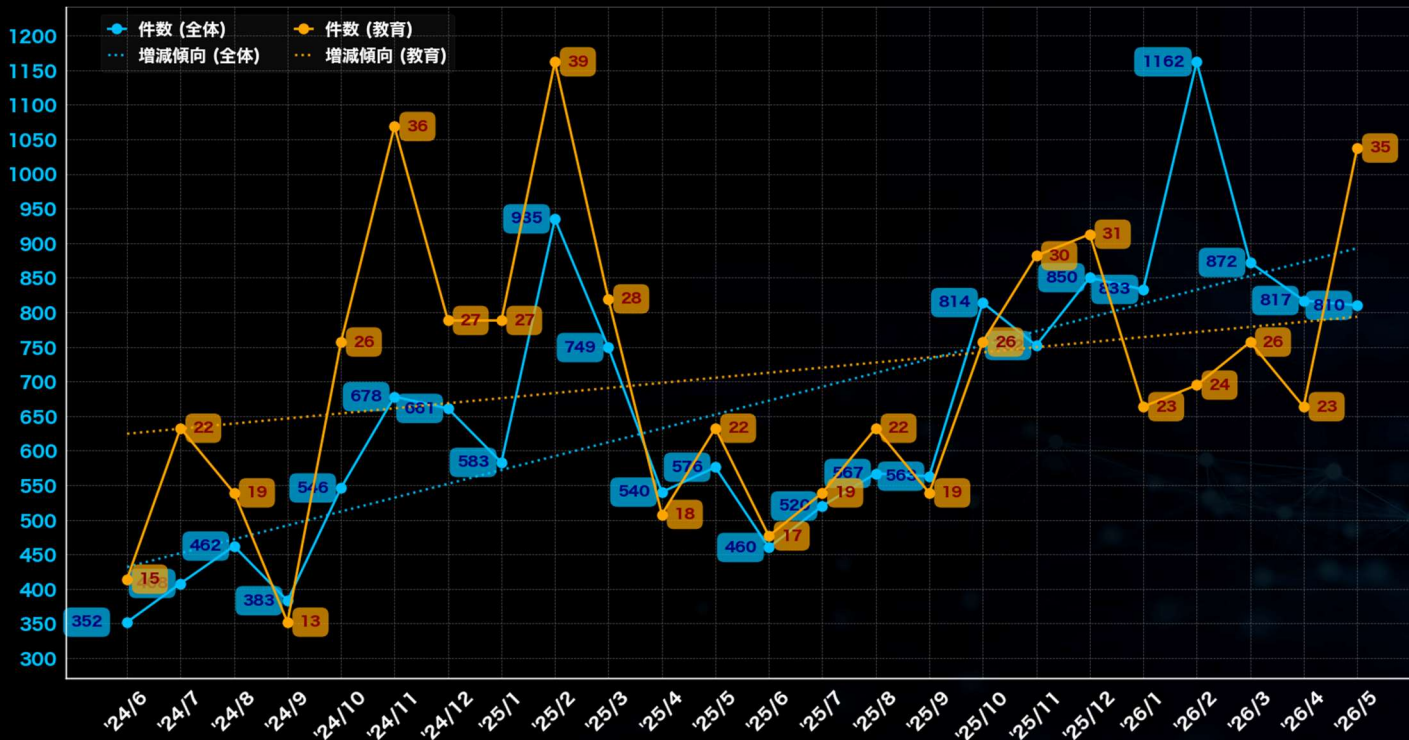


業種に関する分析 (全世界)

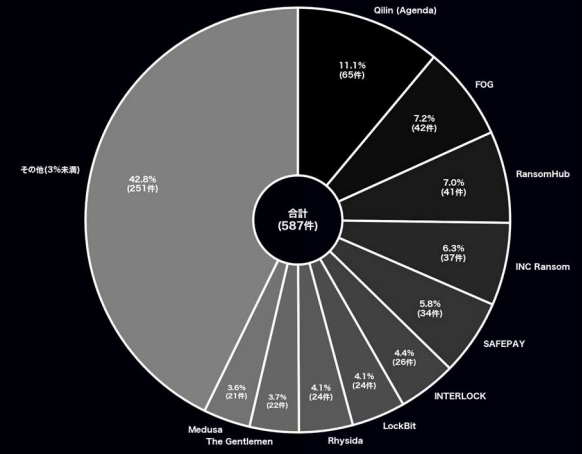
(過去2年間 / 2024年6月 ~ 2026年5月)

教育

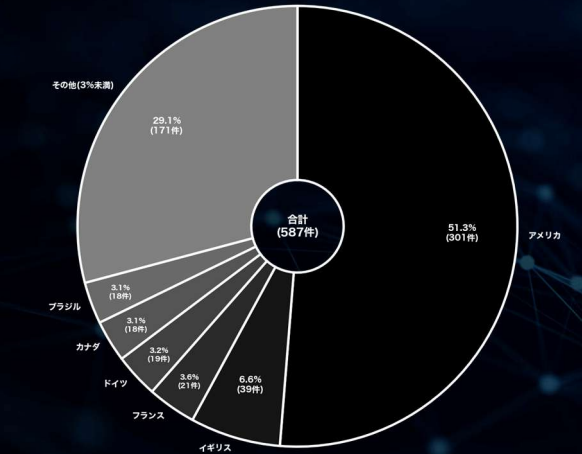
「教育」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、39件の掲載があった。一方、最も少なかった月は2024年9月で、13件であった。被害組織の所在国の割合では、アメリカが約51%と最も多く、次いでイギリスとフランスがそれぞれ約7%と約4%である。攻撃グループについては、少なくとも93のグループが関与しており、特に「Qilin (Agenda)」が65件のリークサイト掲載を実施している。次いで「FOG」と「RansomHub」がそれぞれ42件と41件の掲載を行っている。教育業界は他業界に比べ被害件数は限定的であるものの、関与する攻撃グループは93と多く、依然として注意が必要である。



▼攻撃グループ別



▼国別



(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

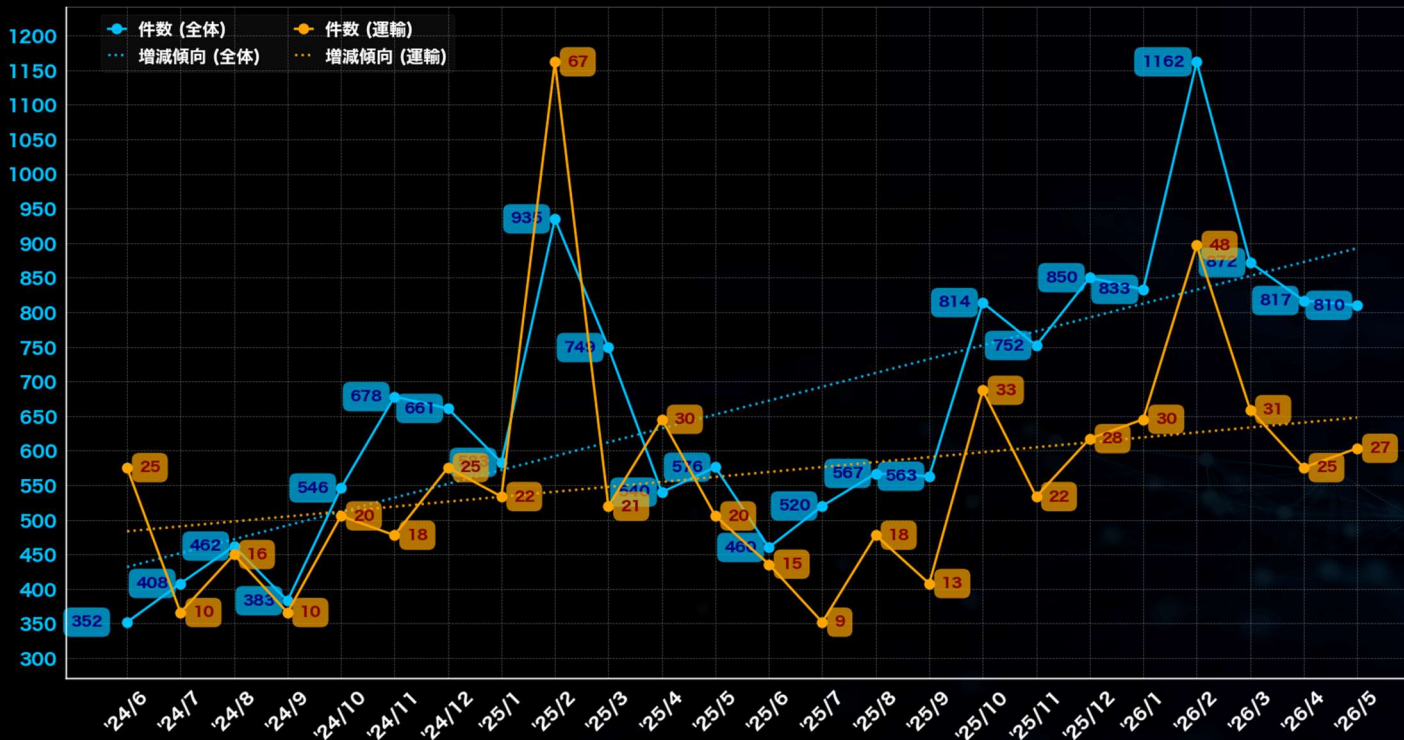
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

業種に関する分析 (全世界)

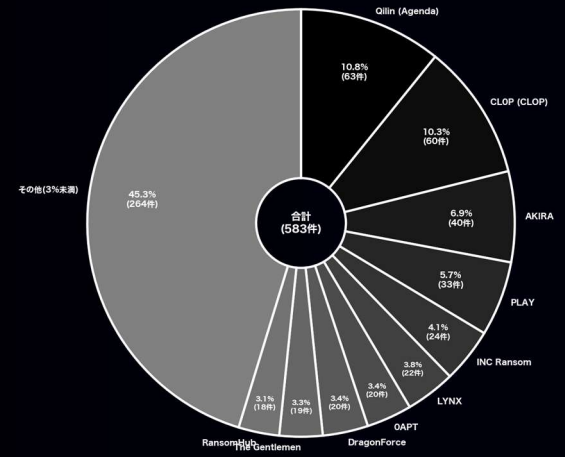
(過去2年間 / 2024年6月 ~ 2026年5月)

運輸

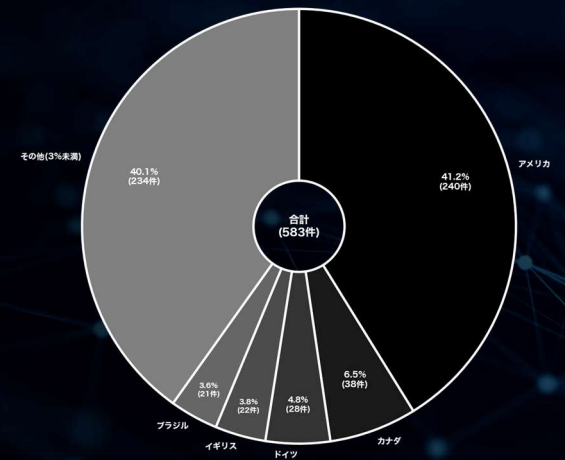
「運輸」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、67件の掲載があった。一方、最も少なかった月は2025年7月で、9件であった。被害組織の所在国の割合では、アメリカが約41%と最も多く、次いでカナダとドイツがそれぞれ約7%と約5%である。攻撃グループについては、少なくとも99のグループが関与しており、特に「Qilin (Agenda)」が63件のリークサイト掲載を実施している。次いで「CLOP (CLOP)」と「AKIRA」がそれぞれ60件と40件の掲載を行っている。運輸関係は全体件数に対する割合こそ低いものの、サプライチェーンへの影響を考慮すると引き続き注視が必要である。



▼攻撃グループ別



▼国別



(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

CIGのコンテンツ紹介

Cyber Intelligence Group (CIG) では、ランサムウェアに関する様々な観点からの分析結果を情報発信しています。ぜひとも皆様の脅威情報の把握にご活用ください。

- CIG Ransomware Information Portal (WEBアプリケーション) :

<https://www.mbsd.jp/cig-ransomware-portal/>

- CIGランサム統計だより :

<https://www.mbsd.jp/research/20231023/blog/>

- 技術ブログ :

<https://www.mbsd.jp/research/cig/>

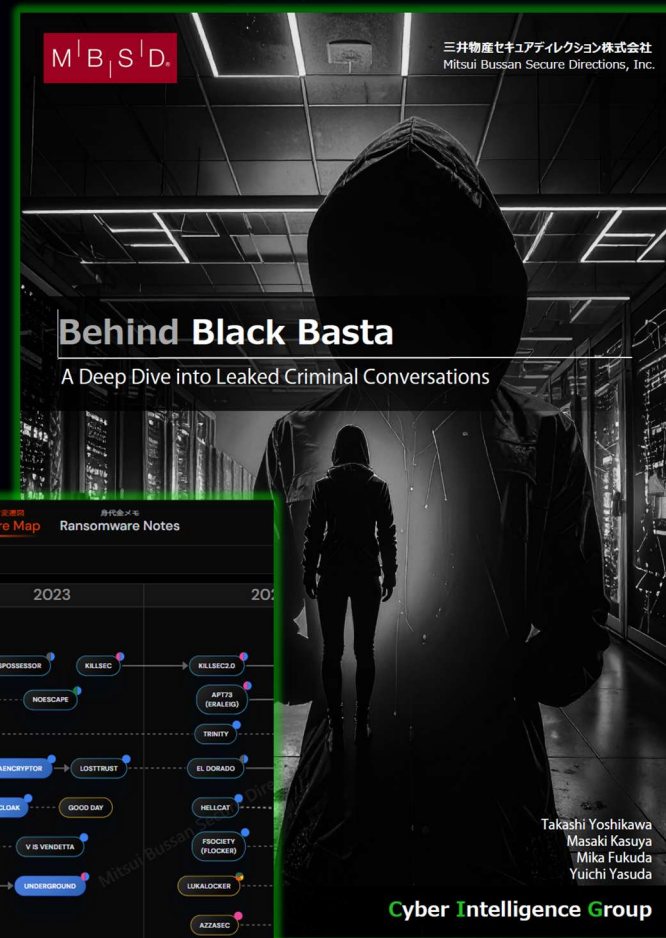
<https://www.mbsd.jp/research/t.yoshikawa/>

<https://www.mbsd.jp/research/m.kasuya/>

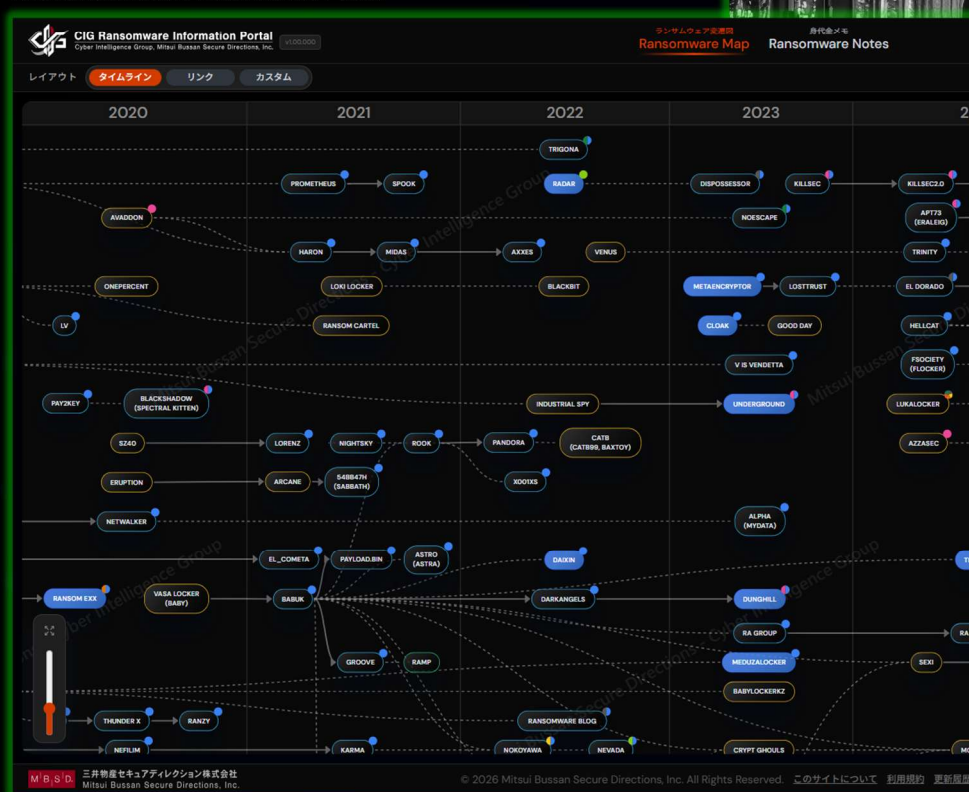
- 分析レポート :

<https://www.mbsd.jp/report>

Black Basta 内部チャット分析レポート



CIG Ransomware Information Portal



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

本資料に関する留意事項及び二次利用について

留意事項

- ・ 攻撃グループや被害組織などについて、正確な情報が公開されていない項目は「(Unknown)」として集計しています。
- ・ 各分析における掲載数は、特に注釈がない限り、公表や報道を含めず、リークサイトに掲載された数のみを基にしています。
(日本にフォーカスした一部の表／グラフのみ、公表や報道から判明した数を加味し集計)
- ・ 本レポートにおける「国」データは、被害組織の本社所在地情報を元に集計しています。
ただし、本社所在地情報が確認できない場合は、「攻撃された拠点の所在国」もしくは「(Unknown)」として集計しています。
- ・ 国内被害組織に関する各種データについては、海外拠点（支社／関連会社）を含みます。
- ・ 業種分類や集計方法を含む本レポートの各データ（値）はMBSD Cyber Intelligence Group (CIG) 独自の観測および集計結果となります。
- ・ 件数については、攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を基に集計しています。
- ・ ごく一部の、ランサムウェアの使用が明確に確認されていない暴露&恐喝グループの値も含まれています。
- ・ これらはいくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定されます。
- ・ 集計方法の変更や、時間が長期経過し公開／公表されるケースを再集計する場合もあるため、常に最新月のレポートを参照してください。

二次利用等に関して

本レポートはご自由に二次利用いただけます。様々な用途にぜひご活用ください。

ご利用・転載・引用の際には、出典として「MBSD Cyber Intelligence Group (CIG)」と明記くださいますようお願いいたします。

(※本レポートそのものの販売など直接的な営利目的でのご利用はご遠慮ください。有料セミナーや出版物、メディア記事など、利用者側の収益が発生する活動においても、参考情報として一部を引用・掲載いただくことに問題はございません。その際は大変お手数ですが、状況把握のため、ご利用前に下記連絡先まで簡単にご一報いただけますと幸いです)

お問い合わせ窓口：<https://www.mbsd.jp/contact-list/>

Mitsui Bussan Secure Directions

M|B|S|D.



Cyber Intelligence Group

三井物産セキュアディレクション株式会社
Mitsui Bussan Secure Directions, Inc.

<https://www.mbsd.jp/> | @mbsdnews | Tokyo Japan