

# 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3月号 Rev 1.00  
(2026年2月分)

2026

2

# 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

2

# 今月のハイライト

## ● 新興グループ The Gentlemen の掲載数が倍増

2026年2月はランサムウェア攻撃グループ「The Gentlemen」が日本企業を含む88件の被害組織をリークサイトへ掲載し、Qilin (Agenda) の108件<sup>※1</sup>に次ぐ活動量を記録した。The Gentlemen は2025年7月頃に Qilin の主要なパートナーが独立して立ち上げた攻撃グループとされ<sup>※2</sup>、多重脅迫を行う RaaS (Ransomware-as-a-Service) として運営されている。盗み取った認証情報を大量にストック<sup>※3</sup>し、常に攻撃に備えるなど技術的、戦術的な成熟度からも重大な脅威といえる。また、アフィリエイトへの収益分配の高さや交渉権の全権委任<sup>※4</sup>による他攻撃グループとの差別化により、今後のさらなる活発化も予想される。

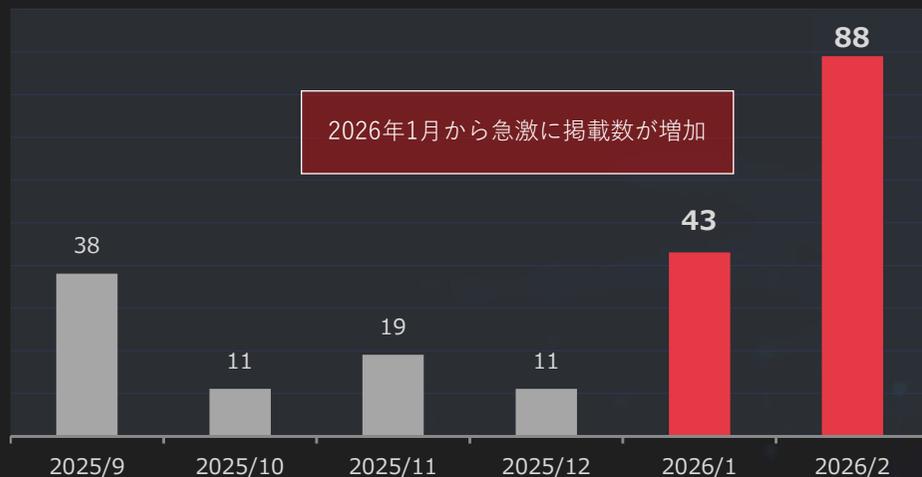
### The Gentlemen リークサイト統計情報

#### ● リークサイト掲載数概要

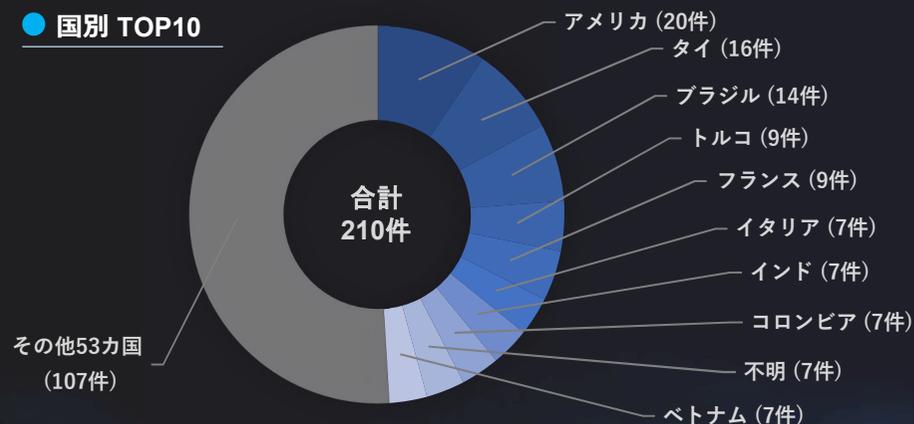


※ リークサイトに掲載された被害組織数であり、交渉などによりリークサイトへ未掲載の被害組織数を除く

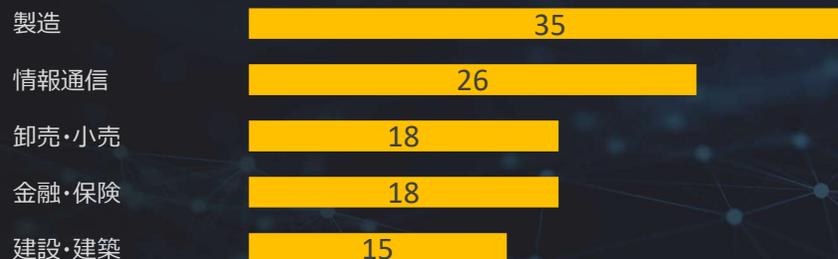
#### ● リークサイト掲載件数推移 (月別)



#### ● 国別 TOP10



#### ● 業種別 Top5 ※合計210件のうち TOP 5 (112件) を集計



集計期間はいずれも2025年9月 ~ 2026年2月

The Gentlemenのリークサイト掲載動向をみると、2025年後半は増減を繰り返していたが、2026年1月以降は件数が急増している。被害組織は国別・業種別ともに特定の傾向がなく、あらゆる組織が標的となりうる状況といえる。こうした脅威グループの動向を継続的に注視し、自組織も標的となりうるという前提で警戒を維持することが重要である。

※1: 掲載数としては「0APT」が一番多いが、0APTの掲載情報が実際の攻撃に基づく情報ではない可能性もあるため、本項では次点で掲載数の多い「Qilin」と比較。

※2: (参考情報) <https://www.securitylab.lat/news/570609.php>

※3: (参考情報) <https://www.group-ib.com/blog/hastalamuerte-gentlemen-raas-ttps/>

※4: (参考情報) <https://socradar.io/blog/dark-web-profile-the-gentlemen-ransomware/>

## 【BeyondTrustの脆弱性がランサムウェア攻撃で悪用される】(SecurityWeek：2026/2/20)

BeyondTrust製品のRCE脆弱性 CVE-2026-1731 が公開 PoC 後24時間以内から悪用され、CISA が KEV を更新してランサムウェア攻撃での悪用を警告、複数業種・国で偵察やデータ窃取などが確認されている。  
<https://www.securityweek.com/beyondtrust-vulnerability-exploited-in-ransomware-attacks/>

## 【北朝鮮のLazarus GroupがMedusaランサムウェアを利用】(SECURITY.COM (Broadcom/Symantec)：2026/2/24)

サイバー攻撃グループ Lazarus の下部グループが Medusa ランサムウェアを利用し、中東や米国の医療機関・非営利団体などを標的に金銭目的のランサムウェア攻撃を行なっている。  
<https://www.security.com/threat-intelligence/lazarus-medusa-ransomware>

## 【ポストRAMP時代：疑惑、分断、そして再構築されるランサムウェア地下経済】(Rapid7：2026/2/25)

2026年1月のRAMP押収後もランサムウェアを含む地下経済圏は存続しているが、管理人の詐欺疑惑やリーク・ハニーポット説を巡る混乱で攻撃者間の信頼が崩壊し、複数フォーラムへと分散・再編されている。  
<https://www.rapid7.com/blog/post/tr-post-ramp-allegations-fragmentation-ransomware-underground-rebuild/>

## 【ランサムウェア被害における身代金支払い率が過去最低水準に低下、攻撃件数は増加】(Bleeping Computer：2026/2/26)

Chainalysisによると2025年はランサムウェア攻撃の件数が大幅に増えた一方で、実際に身代金を払った被害者は28%と過去最低水準にとどまった。少数から多くを搾り取る戦略にシフトしている可能性がある。  
<https://www.bleepingcomputer.com/news/security/ransomware-payment-rate-drops-to-record-low-as-attacks-surge/>

## 【ロシア人ランサムウェア運営関係者が電信詐欺共謀で有罪答弁】(米司法省 (U.S. Attorney's Office, District of Maryland)：2026/3/4)

1,000超の組織に被害を与え、3,900万ドル超を脅し取ったとされるPhobosランサムウェア運営に関与した被告が有罪を認めた。  
<https://www.justice.gov/usao-md/pr/russian-ransomware-administrator-pleads-guilty-wire-fraud-conspiracy>

## 【INC Ransomのアフィリエイトモデルが重要ネットワーク標的化を可能にしている】(New Zealand National Cyber Security Centre：2026/3/6)

ニュージーランドの国家サイバーセキュリティセンターなどが、INC Ransomに関する共同アドバイザリーを公開。豪州・ニュージーランド・太平洋島嶼国の組織に対し、警戒と対策強化を呼びかけた。  
<https://www.ncsc.govt.nz/alerts/inc-ransom-affiliate-model-enabling-targeting-of-critical-networks/>

## 【Termiteランサムウェア侵害、ClickFixとCastleRAT攻撃に関連】(BleepingComputer：2026/3/7)

MalBeaconは、Termiteを含む複数ランサムウェア攻撃に関与してきた Velvet Tempest が ClickFix と Windows 正規ツールを悪用して侵入した事例(本件で暗号化なし)を報告。  
<https://www.bleepingcomputer.com/news/security/termite-ransomware-breaches-linked-to-clickfix-castlerat-attacks/>

## 【令和7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】(警察庁 (サイバー警察局)：2026/3/12)

警察庁が毎年公表している「サイバー空間をめぐる脅威の情勢等」レポートの最新版(令和7年版)が発表。令和7年、ランサムウェア被害報告は226件、サイバー犯罪検挙数は過去最高の15,108件。  
[https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07\\_cyber\\_jousei.pdf](https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf)

## 【AI生成の可能性があるSlopolymalware、Interlockランサムウェア攻撃で使用】(BleepingComputer：2026/3/12)

生成AIで作られたとみられるmalware Slopoly がランサムウェア攻撃に悪用され、攻撃者は1週間以上潜伏して情報を窃取した。AIがmalware開発の迅速化と検知回避を後押ししている実態が浮き彫りになった。  
<https://www.bleepingcomputer.com/news/security/ai-generated-slopoly-malware-used-in-interlock-ransomware-attack/>

## 【LeakNetランサムウェア、ClickFixとDenoランタイムを用いたステルス攻撃を実施】(BleepingComputer：2026/3/17)

ランサムウェアグループ LeakNet が ClickFix と Deno ランタイム (JavaScript 実行環境) を悪用。偽の認証画面でユーザーを騙し悪意あるコマンドを実行させ、malwareをメモリ上で動かす手口を採用している。  
<https://www.bleepingcomputer.com/news/security/leaknet-ransomware-uses-clickfix-and-deno-runtime-for-stealthy-attacks/>

※ 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：<sup>(※1)</sup> <sup>(※2)</sup> **309**

→ 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：**59**

● 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

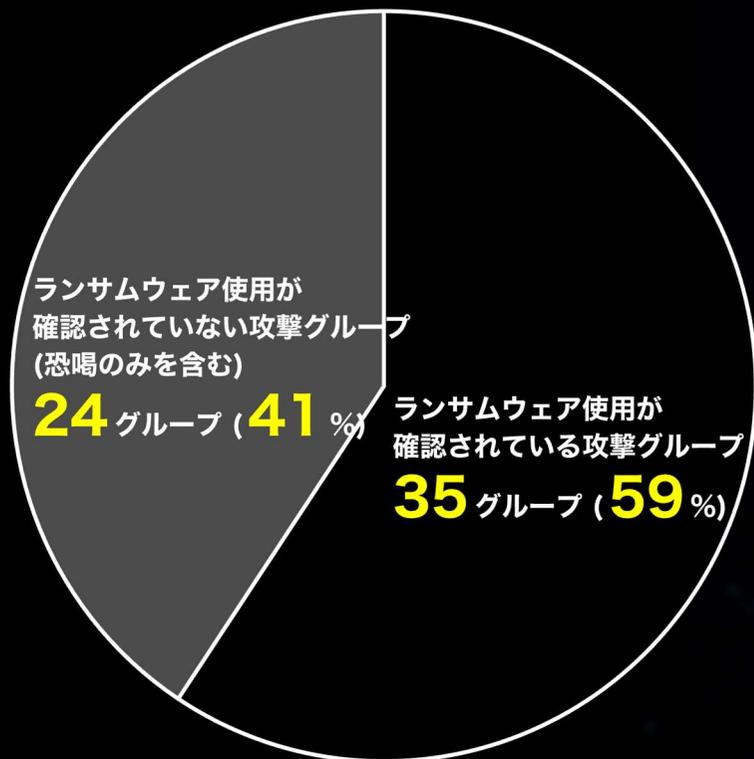
- |   |   |  |  |   |  |   |
|---|---|--|--|---|--|---|
| OAPT<br>Omega (Omega)<br>8BASE<br>Abyss<br>AKIRA<br>AKO<br>Alpha (MYDATA)<br>AlphV (BlackCat)<br>Anubis<br>Apos Security<br>APT73 (Eraleig)<br>ARACHNA<br>ARCUS MEDIA<br>Argonauts<br>Arkana<br>ArvinClub<br>Astro (Astra)<br>Cloak<br>Atomsilo<br>Avaddon<br>AvosLocker<br>AWARE<br>Axxes<br>AzzaSec<br>Babuk<br>Babuk (2025)<br>BASHE<br>BEAST<br>Benzona<br>BERT<br>BianLian<br>BLOODY (BLOODY)<br>Bl4ck0r (BlackTor)<br>Black Basta<br>BlackByte<br>BlackDolphin<br>● BlackField<br>BlackLock<br>BlackMatter<br>Black Nevas<br>Blackout<br>BLACKSHIRANTAC<br>BlackSuit<br>BLUEBOX<br>BLUESKY<br>BOTLOCK | Brain Cipher<br>BRAVOX<br>Brotherhood<br>BULLY<br>Business Data Leaks<br>CACTUS<br>Cephalus<br>CHAOS (2025)<br>CHEERS<br>ChileLocker (Arcrypter)<br>CHORT<br>Cicada3301<br>CiphBit<br>● CipherForce<br>CipherLocker<br>CLOP (CLOP)<br>Cloak<br>COINBASE CARTEL<br>Conti<br>Cooming Project<br>Crazy Hunter Team<br>CROSSLOCK<br>CRYO<br>CryptBB<br>CRYPTNET<br>CRYPTO24<br>CryptOn<br>Cuba<br>Cyclops<br>D4RK4RMY<br>DAGON<br>DAIXIN<br>dAn0n (danon)<br>Dark Angels<br>DARKBIT<br>DARKPOWER<br>DarkRace<br>DarkRypt<br>Dark Shinigamis<br>Darkside<br>Dark Vault<br>DataCarry<br>Datakeeper<br>Desolator | DEVMAN<br>DEVMAN 2.0<br>Dire Wolf<br>Dispossessor[Databroker]<br>Donex<br>Donut Leaks<br>DoppelPaymer<br>dotAdmin<br>DragonForce<br>DragonRansomware<br>DUNGHILL<br>eCh0raix (eChoraix)<br>EL Cometa<br>EL DORADO<br>EMBARGO<br>Endurance<br>Entropy<br>Everest<br>FOG<br>Frag<br>FSOCIETY / FLOCKER<br>FSTeam<br>FulcrumSec<br>Funksec<br>GD LockerSec<br>Genesis<br>GLOBAL<br>Grief<br>Groove<br>Gunra / Fresh Gunra<br>HANDARA [Hacktivist]<br>Haron<br>HELLCAT<br>Helldown<br>HelloGookie<br>Hitler (AGLOBGVYCG)<br>Hive<br>HolyGhost<br>Hotarus<br>Hunters International<br>ICEFIRE<br>IMN Crew<br>INC Ransom<br>Insane | ● INSONMIA<br>INTERLOCK<br>J GROUP<br>KAIVOS<br>Karakurt<br>Karma<br>Kawa4096<br>Kazu<br>KILLSEC<br>● Kittykatkrew<br>Knight<br>Kraken (HelloKitty)<br>Kryptos<br>Kyber<br>LAMBDA<br>La Plovra<br>LAPSUS\$<br>LAPSUS\$ Group<br>LeakedData (Silent Ransom Group)<br>LEAKNET<br>LILLITH<br>Link<br>LookBit<br>Lorenz<br>LostTrust<br>LunaLock<br>LV<br>LYNX<br>MADCAT<br>MAD LIBERATOR<br>MALAS<br>MalekTeam<br>Mallox<br>Mamona RIP<br>MBC<br>Medusa<br>● MEDUZA LOCKER<br>MEOU<br>Metaencryptor<br>Midas<br>MIGA<br>Mindware<br>Minteye<br>Mogilevich [fraud] | MOISHA<br>Money Message<br>Monti<br>Morpheus<br>Mount Locker<br>MST3-089<br>N3tw0rm (NetWorm)<br>N4UGHTYSEC (NAUGHTYSEC)<br>NASIR SECUTRIY<br>Nefilim<br>● NetRunner<br>Nevada<br>NightSky<br>NightSpire<br>NITROGEN<br>NoEscape<br>Nokoyawa<br>NONAME (VFOKX)<br>NONAME [2023年確認]<br>Nova<br>NULLBULGE<br>Obscura<br>Obscura 2.0<br>Onyx<br>Orca<br>Orion Leaks<br>OSIRIS PROJECT<br>Pandora<br>Pay2Key<br>● Payload<br>Payload.bin<br>Payouts King<br>PEAR<br>PLAY<br>PLAYBOY<br>Prometheus<br>PRYX<br>PUTIN TEAM<br>Pysa / Mespinoza<br>Qilin (Agenda)<br>QIULONG<br>Quantum<br>RABBIT HOLE<br>RADAR | RADIANT<br>Ragnar Locker<br>Ragnarok<br>RA GROUP<br>RALord<br>Rancoz<br>RansomBay<br>Ransom Cartel<br>Ransom Corp<br>RANSOMCORTEX<br>Ransomed.vc<br>Ransom EXX<br>RansomHouse<br>RansomHub<br>Ransomware Blog<br>Ranzy<br>RA WORLD<br>Raznatovic<br>RedAlert (N13V)<br>Red Ransomware Group (Red CryptoApp)<br>Relic<br>Revil (Sodinokibi)<br>● Reynolds<br>Rhysida<br>Risen<br>ROOK<br>root<br>Royal<br>Ransom<br>RunSomeWares<br>Rusty Locker<br>Sabbath (54bb47h)<br>PEAR<br>SARCOMA<br>SATAN LOCK<br>SATAN LOCK V2<br>Scattered LAPSUS\$ Hunters<br>Secp0<br>Securotrop<br>SenSay0<br>● SHADOWBYT3\$<br>shaoleaks<br>SHINYHUNTERS<br>Sicarii | SIEGEDSEC<br>Silent<br>Simobi<br>SKIRA TEAM<br>SLUG<br>Snatch<br>Solidbit<br>Space Bears<br>Sparta<br>Spook<br>STORMOUS<br>Sugar<br>Suncrypt<br>SynACK<br>TeamXXX<br>TENGU<br>Termite<br>The Gentlemen<br>THE GREEN BLOOD GROUP<br>ThreeAM (3AM)<br>TridentLocker<br>TRIGONA<br>TRINITY<br>TRISEC<br>Underground<br>UnSafe<br>Valencia<br>VanHelsing<br>VanirGroup<br>Vect<br>Vice Society<br>V IS VENDETTA<br>VSOP<br>WALocker<br>Warlock<br>WEREWOLVES<br>Weyhro<br>WORLD LEAKS<br>x001xs<br>XING Team<br>Yanluowang<br>Yurei<br>Zeon<br>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 **2**月)

(※当月にリークサイト掲載を確認した攻撃グループ全**59**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2月に活動中である事が確認された全59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。

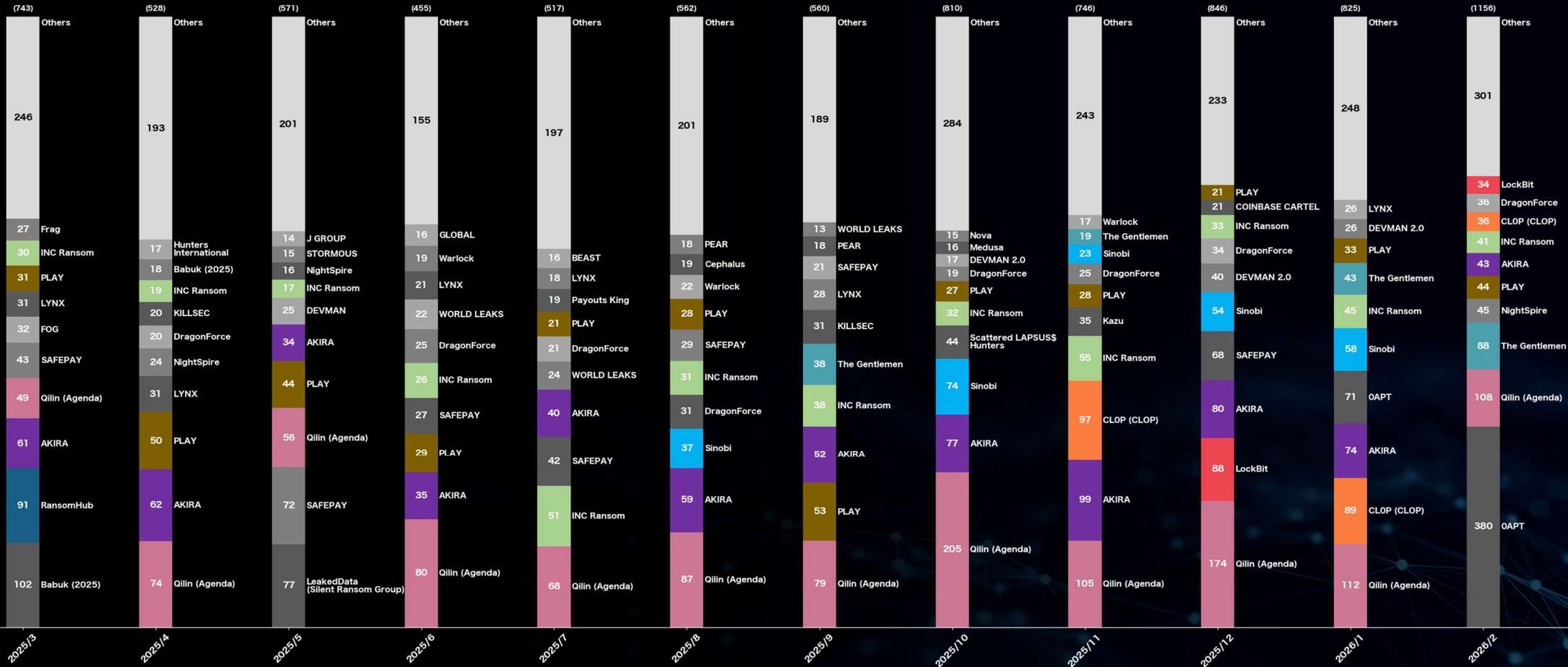
# 年間統計

(全世界)

2026  
2

# 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3月～2026年2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3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  
2

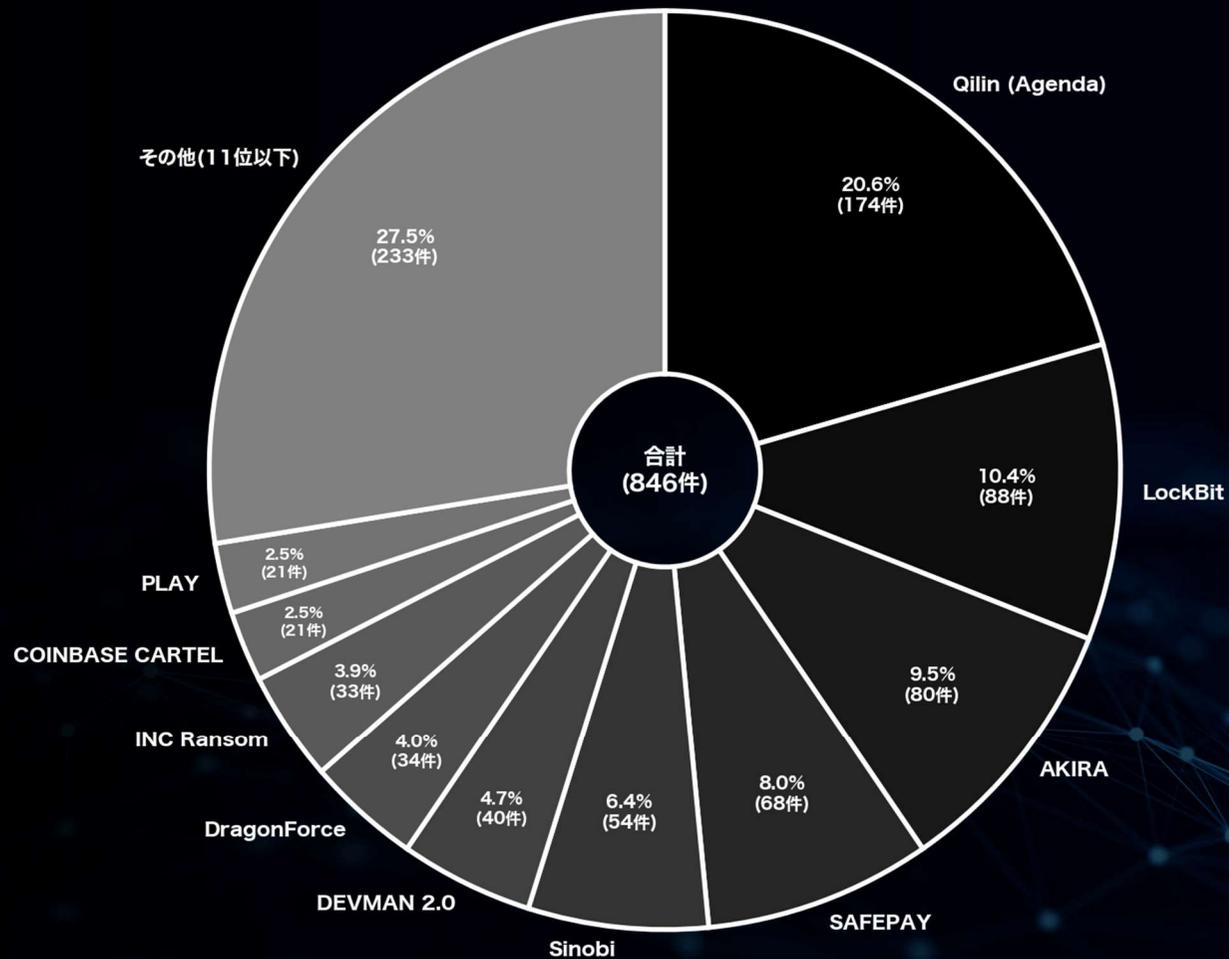
# 月別内訳 攻撃グループ TOP10 (全世界)

(2025年 12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)	174	20.6	+ 69
LockBit	88	10.4	+ 88
AKIRA	80	9.5	- 19
SAFEPAY	68	8.0	+ 54
Sinobi	54	6.4	+ 31
DEVMAN 2.0	40	4.7	+ 30
DragonForce	34	4.0	+ 9
INC Ransom	33	3.9	- 22
COINBASE CARTEL	21	2.5	+ 10
PLAY	21	2.5	- 7



※ 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

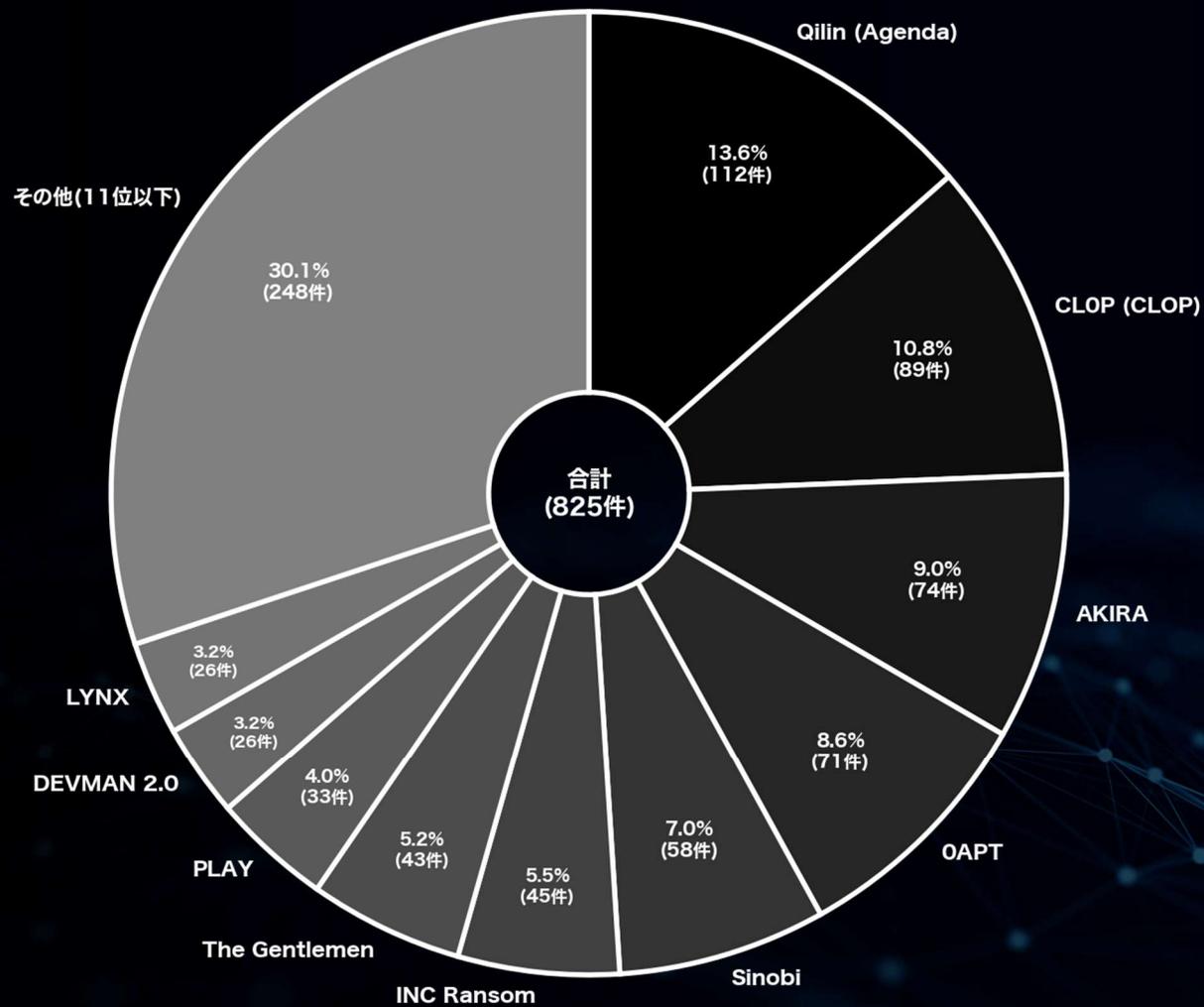
# 月別内訳 攻撃グループ TOP10 (全世界)

(2026年 1 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)	112	13.6	- 62
CLOP (CLOP)	89	10.8	+ 88
AKIRA	74	9.0	- 6
OAPT	71	8.6	+ 71
Sinobi	58	7.0	+ 4
INC Ransom	45	5.5	+ 12
The Gentlemen	43	5.2	+ 32
PLAY	33	4.0	+ 12
DEVMAN 2.0	26	3.2	- 14
LYNX	26	3.2	+ 12



※ 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

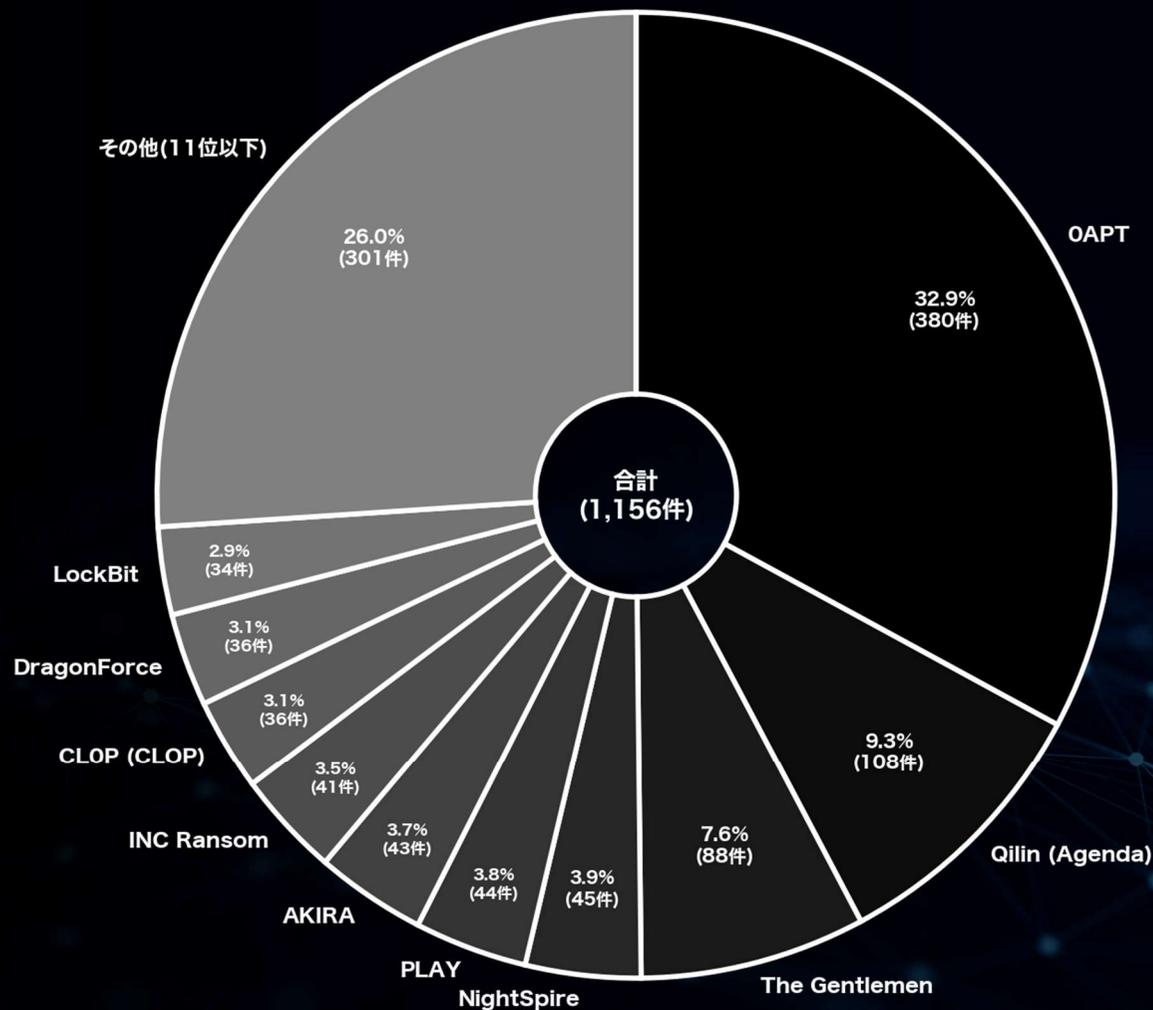
# 月別内訳 攻撃グループ TOP10 (全世界)

(2026年 2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)
OAPT	380	32.9	+ 309
Qilin (Agenda)	108	9.3	- 4
The Gentlemen	88	7.6	+ 45
NightSpire	45	3.9	+ 24
PLAY	44	3.8	+ 11
AKIRA	43	3.7	- 31
INC Ransom	41	3.5	- 4
CLOP (CLOP)	36	3.1	- 53
DragonForce	36	3.1	+ 27
LockBit	34	2.9	+ 23



※ 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  
2

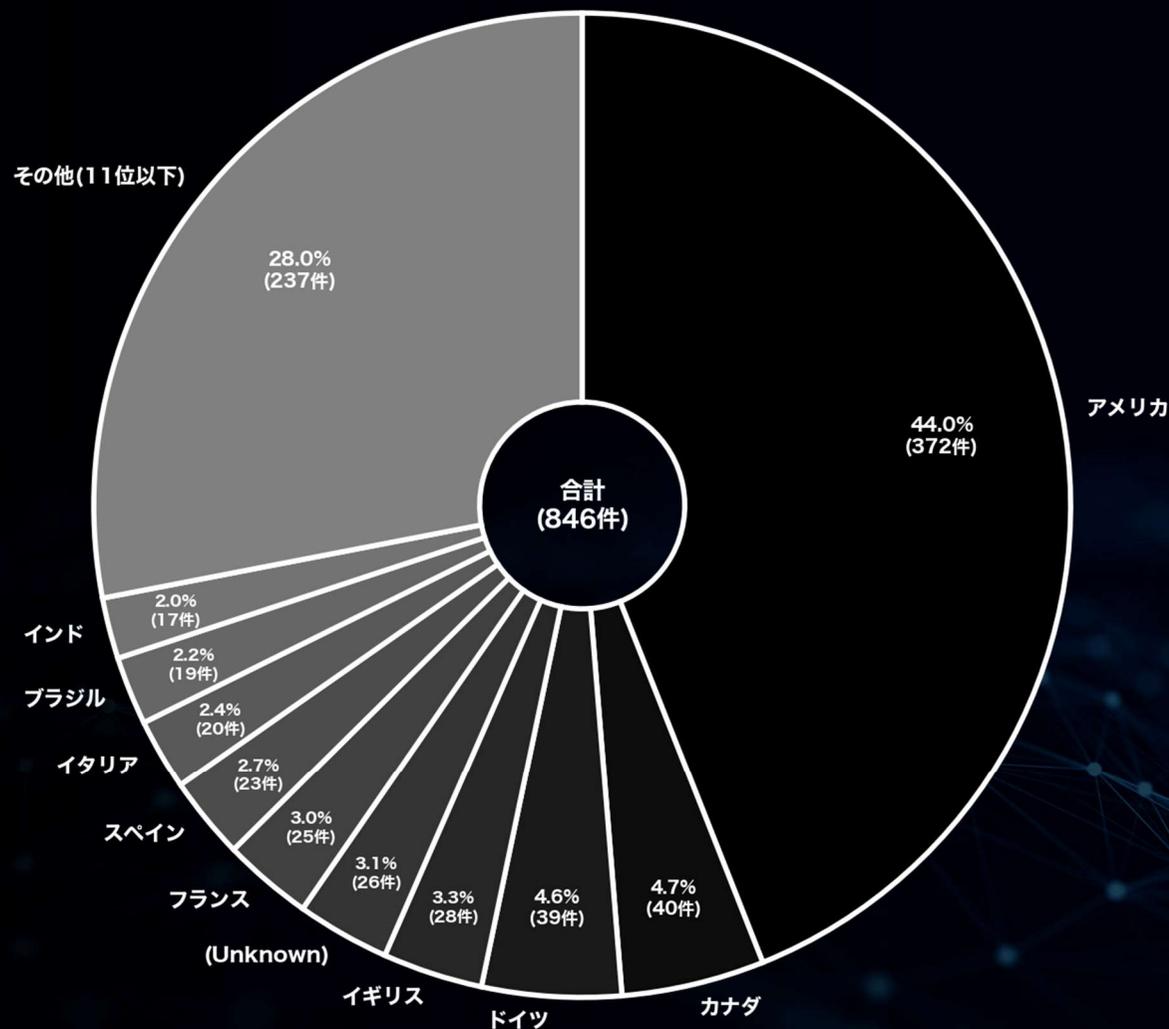
# 月別内訳 被害国TOP10 (全世界)

(2025年 12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	372	44.0	+ 6
カナダ	40	4.7	+ 3
ドイツ	39	4.6	+ 26
イギリス	28	3.3	+ 11
(Unknown)	26	3.1	- 4
フランス	25	3.0	+ 17
スペイン	23	2.7	+ 9
イタリア	20	2.4	+ 9
ブラジル	19	2.2	+ 8
インド	17	2.0	+ 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

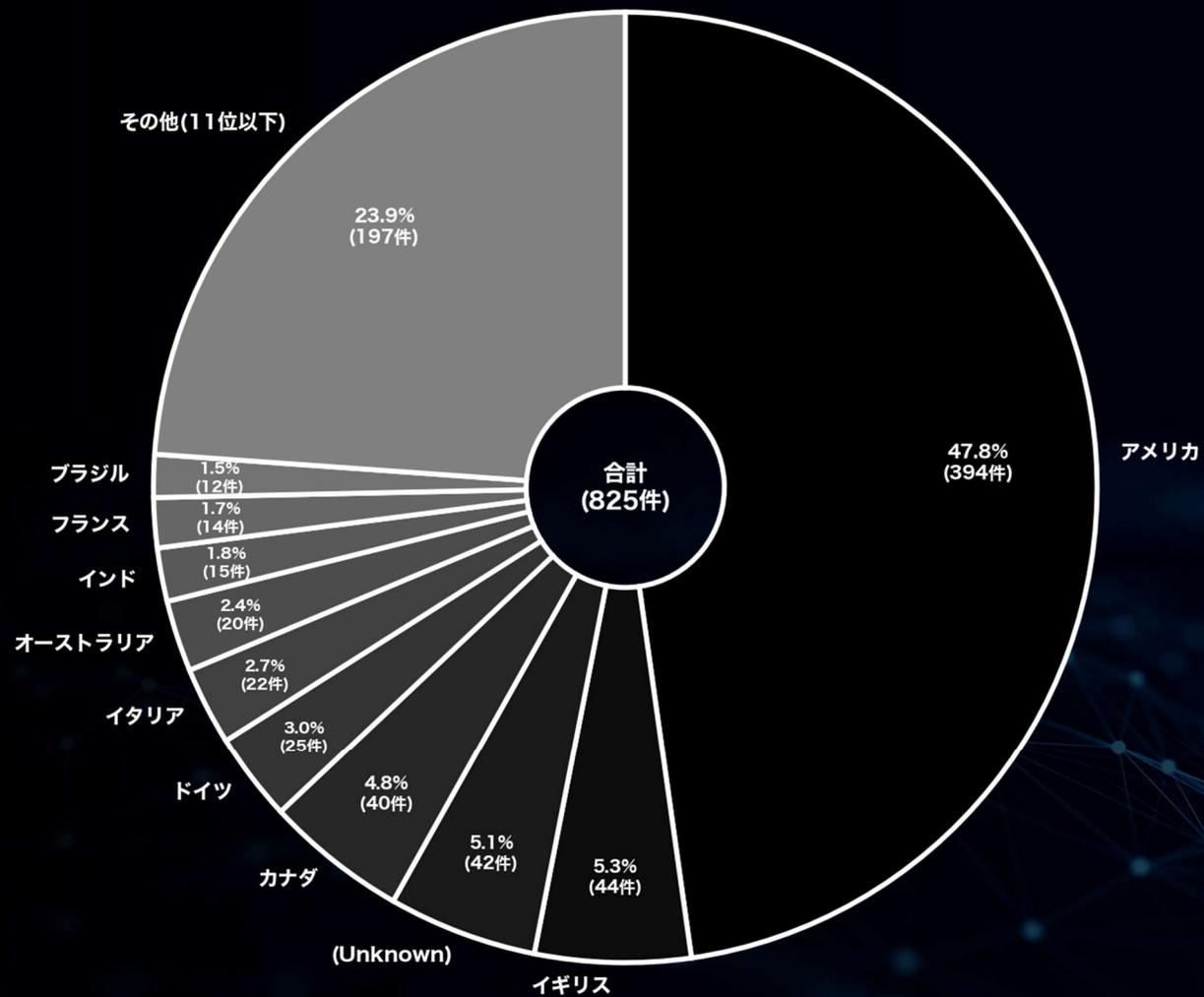
# 月別内訳 被害国TOP10 (全世界)

(2026年 1 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	394	47.8	+ 22
イギリス	44	5.3	+ 16
(Unknown)	42	5.1	+ 16
カナダ	40	4.8	± 0
ドイツ	25	3.0	- 14
イタリア	22	2.7	+ 2
オーストラリア	20	2.4	+ 9
インド	15	1.8	- 2
フランス	14	1.7	- 11
ブラジル	12	1.5	- 7



※ 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

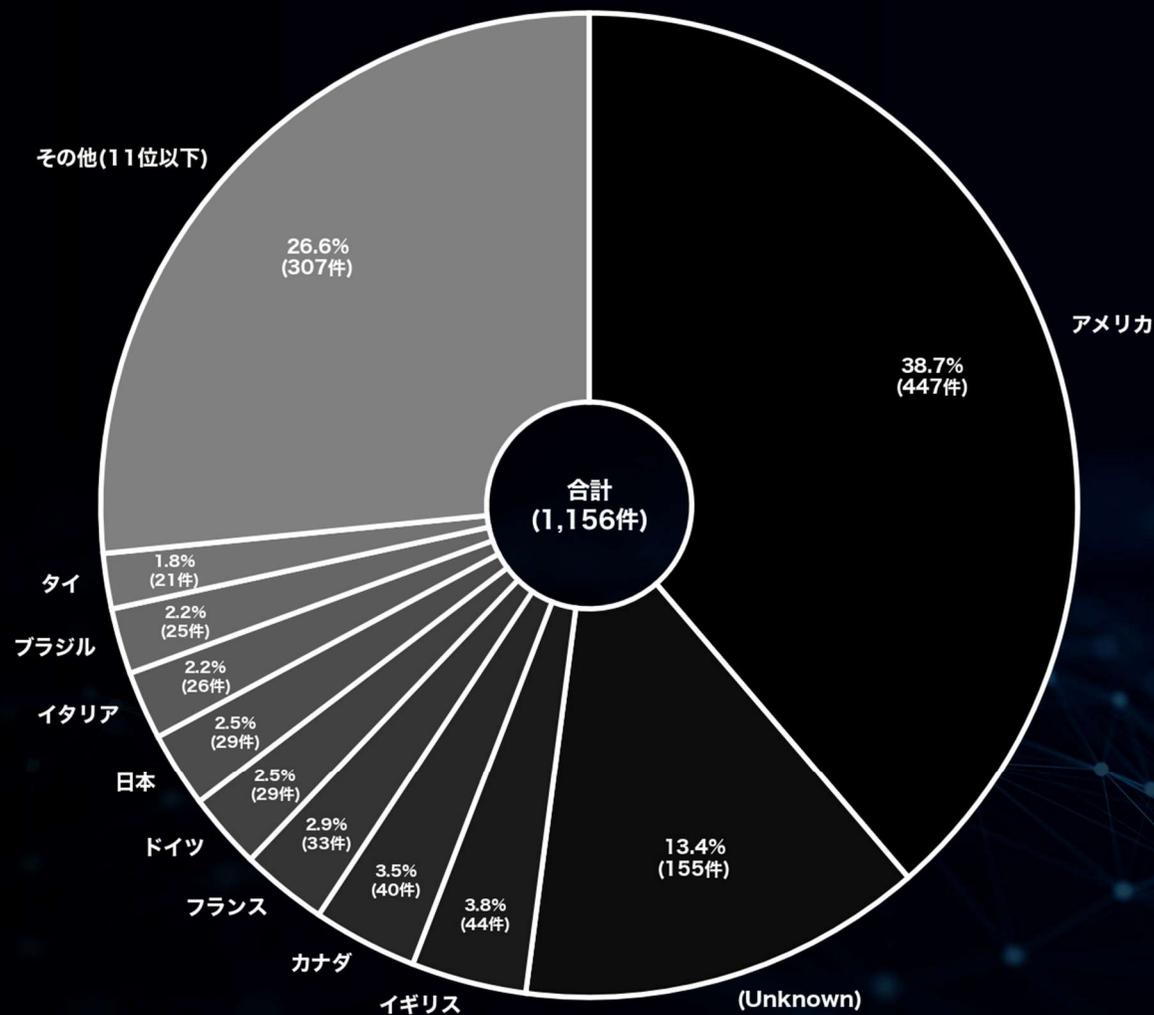
# 月別内訳 被害国TOP10 (全世界)

(2026年 2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	447	38.7	+ 53
(Unknown)	155	13.4	+ 113
イギリス	44	3.8	± 0
カナダ	40	3.5	± 0
フランス	33	2.9	+ 19
ドイツ	29	2.5	+ 4
日本	29	2.5	+ 24
イタリア	26	2.2	+ 4
ブラジル	25	2.2	+ 13
タイ	21	1.8	+ 11



※ 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  
2

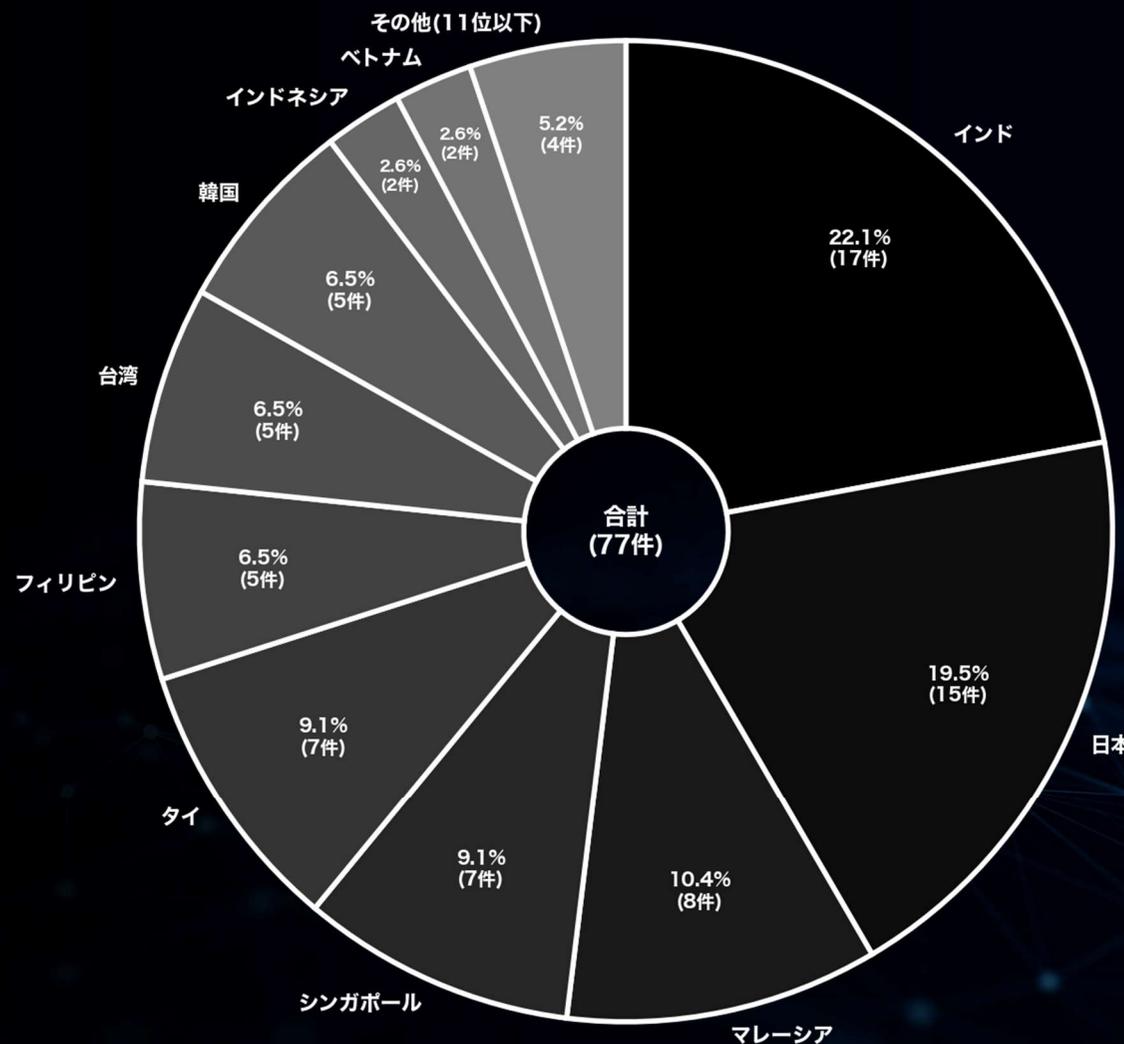
# 月別内訳 被害国TOP10 (アジア)

(2025年 12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	17	22.1	+ 3
日本	15	19.5	+ 3
マレーシア	8	10.4	+ 2
シンガポール	7	9.1	+ 1
タイ	7	9.1	- 4
フィリピン	5	6.5	+ 4
台湾	5	6.5	+ 3
韓国	5	6.5	+ 1
インドネシア	2	2.6	- 3
ベトナム	2	2.6	- 5



※ 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

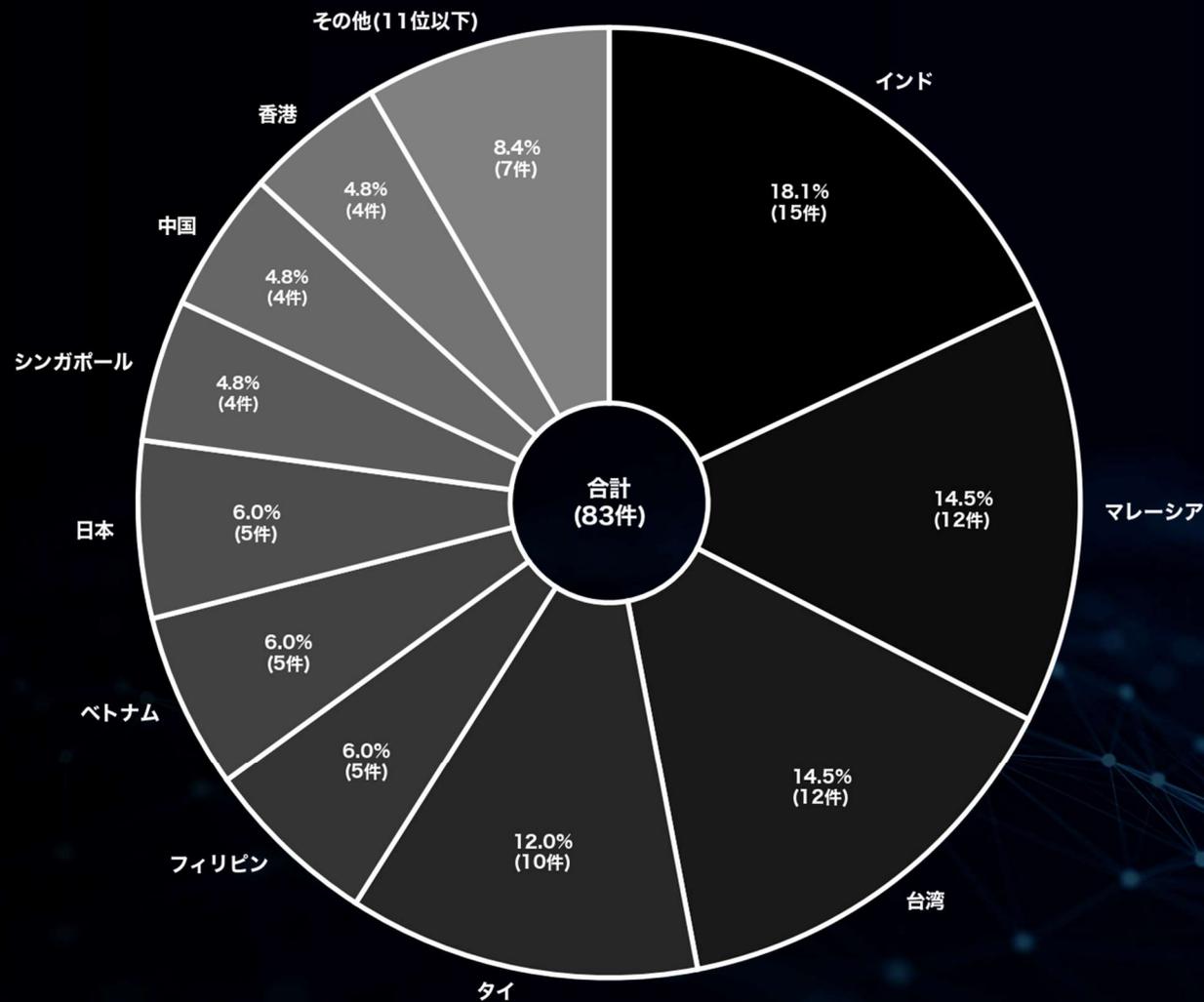
# 月別内訳 被害国TOP10 (アジア)

(2026年 1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	15	18.1	- 2
マレーシア	12	14.5	+ 4
台湾	12	14.5	+ 7
タイ	10	12.0	+ 3
フィリピン	5	6.0	± 0
ベトナム	5	6.0	+ 3
日本	5	6.0	- 10
シンガポール	4	4.8	- 3
中国	4	4.8	+ 3
香港	4	4.8	+ 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

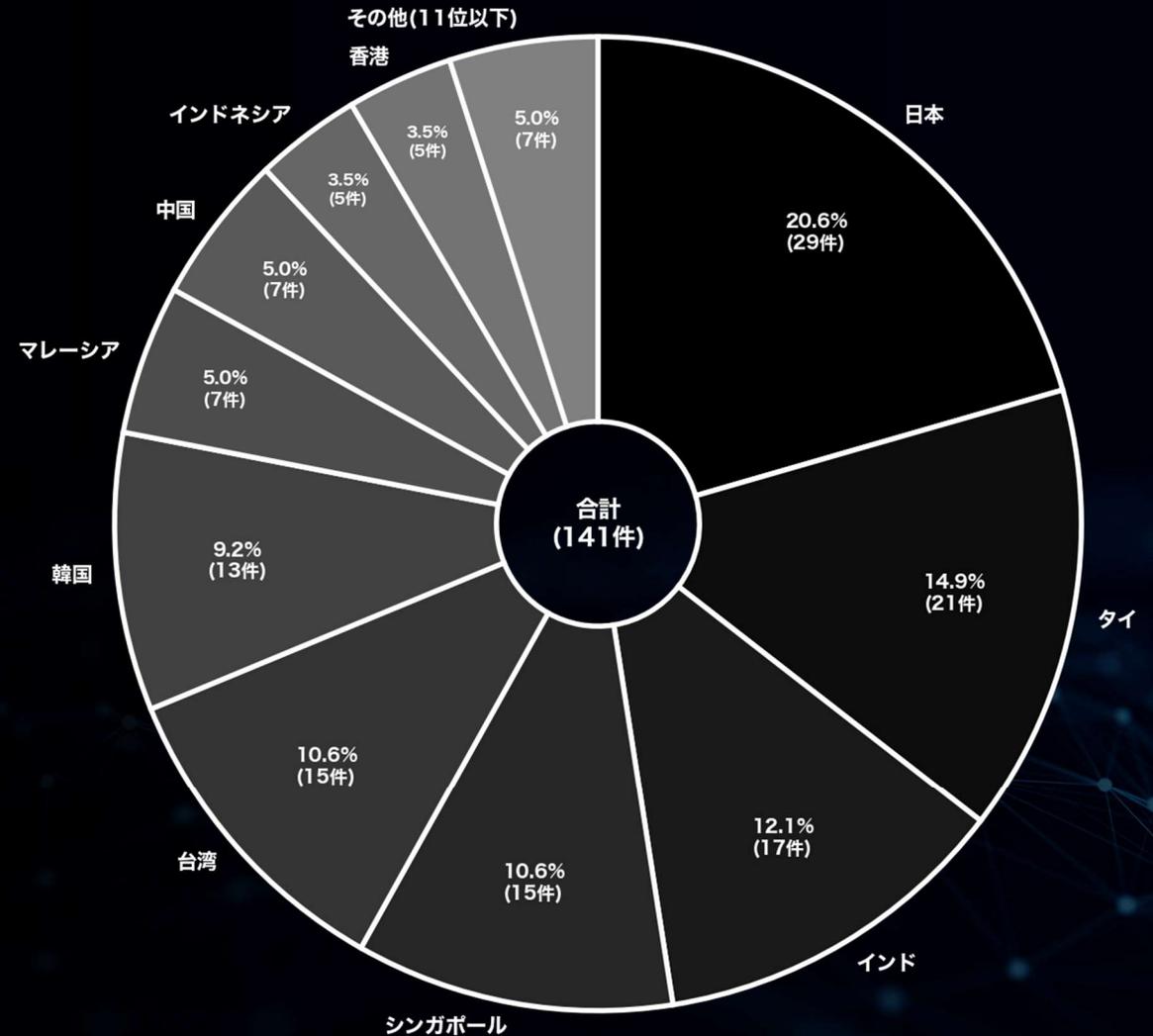
# 月別内訳 被害国TOP10 (アジア)

(2026年 2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	29	20.6	+ 24
タイ	21	14.9	+ 11
インド	17	12.1	+ 2
シンガポール	15	10.6	+ 11
台湾	15	10.6	+ 3
韓国	13	9.2	+ 11
マレーシア	7	5.0	- 5
中国	7	5.0	+ 3
インドネシア	5	3.5	+ 3
香港	5	3.5	+ 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  
2

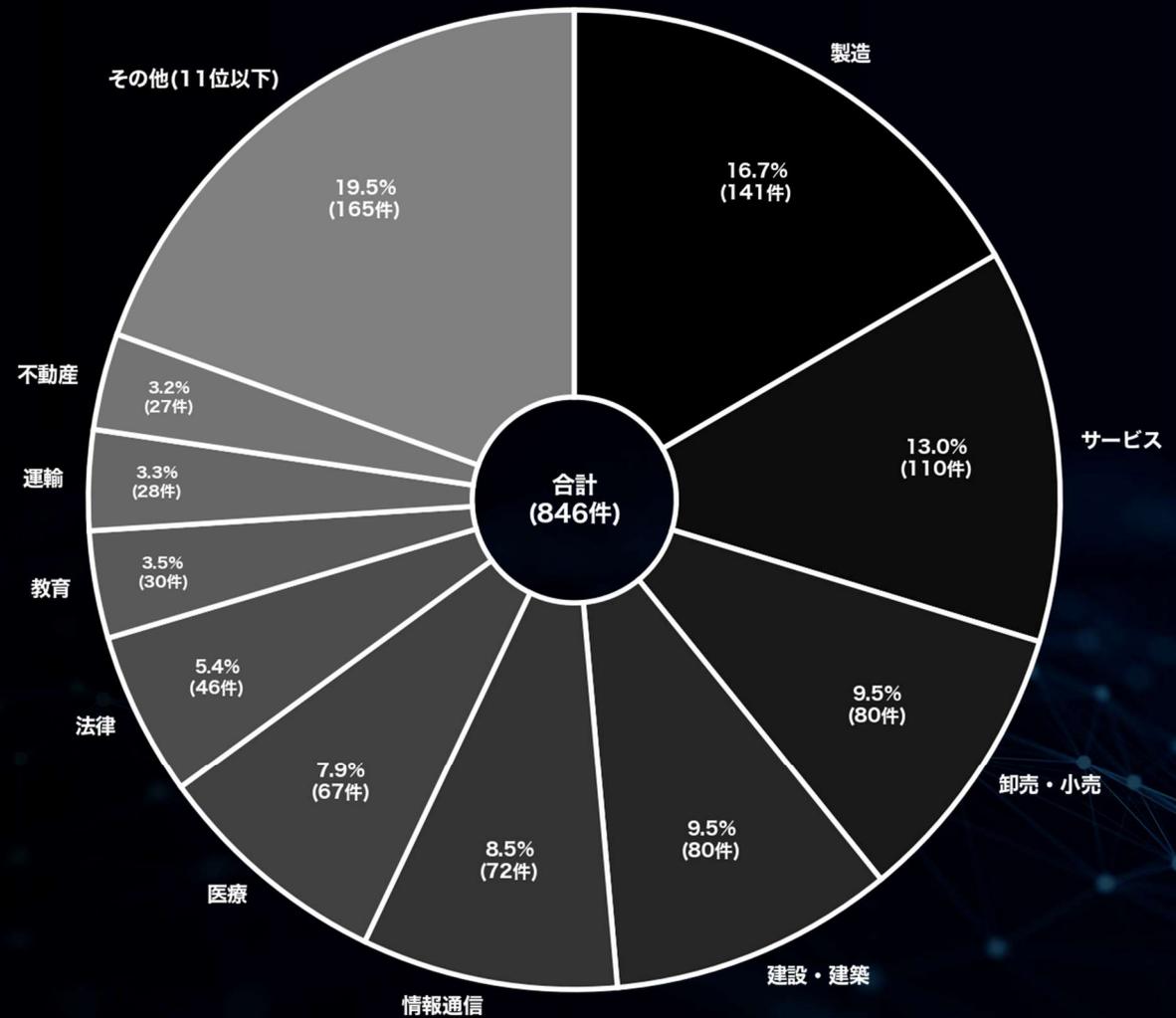
# 月別内訳 業種 TOP10 (全世界)

(2025年 12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	141	16.7	- 13
サービス	110	13.0	+ 15
卸売・小売	80	9.5	+ 23
建設・建築	80	9.5	+ 21
情報通信	72	8.5	+ 15
医療	67	7.9	+ 11
法律	46	5.4	+ 15
教育	30	3.5	+ 2
運輸	28	3.3	+ 6
不動産	27	3.2	+ 7



※ 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

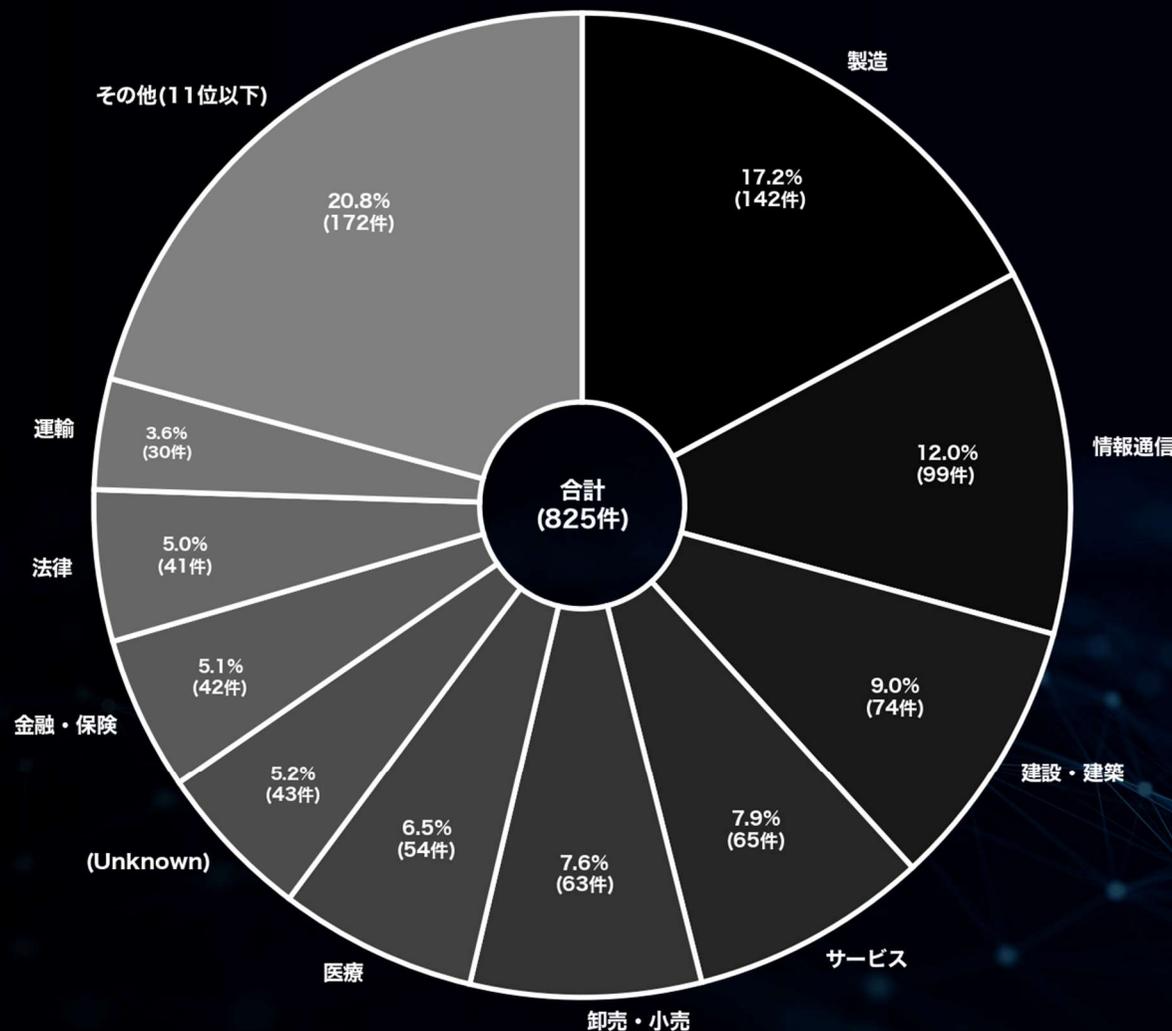
# 月別内訳 業種 TOP10 (全世界)

(2026年 1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	142	17.2	+ 1
情報通信	99	12.0	+ 27
建設・建築	74	9.0	- 6
サービス	65	7.9	- 45
卸売・小売	63	7.6	- 17
医療	54	6.5	- 13
(Unknown)	43	5.2	+ 17
金融・保険	42	5.1	+ 17
法律	41	5.0	- 5
運輸	30	3.6	+ 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

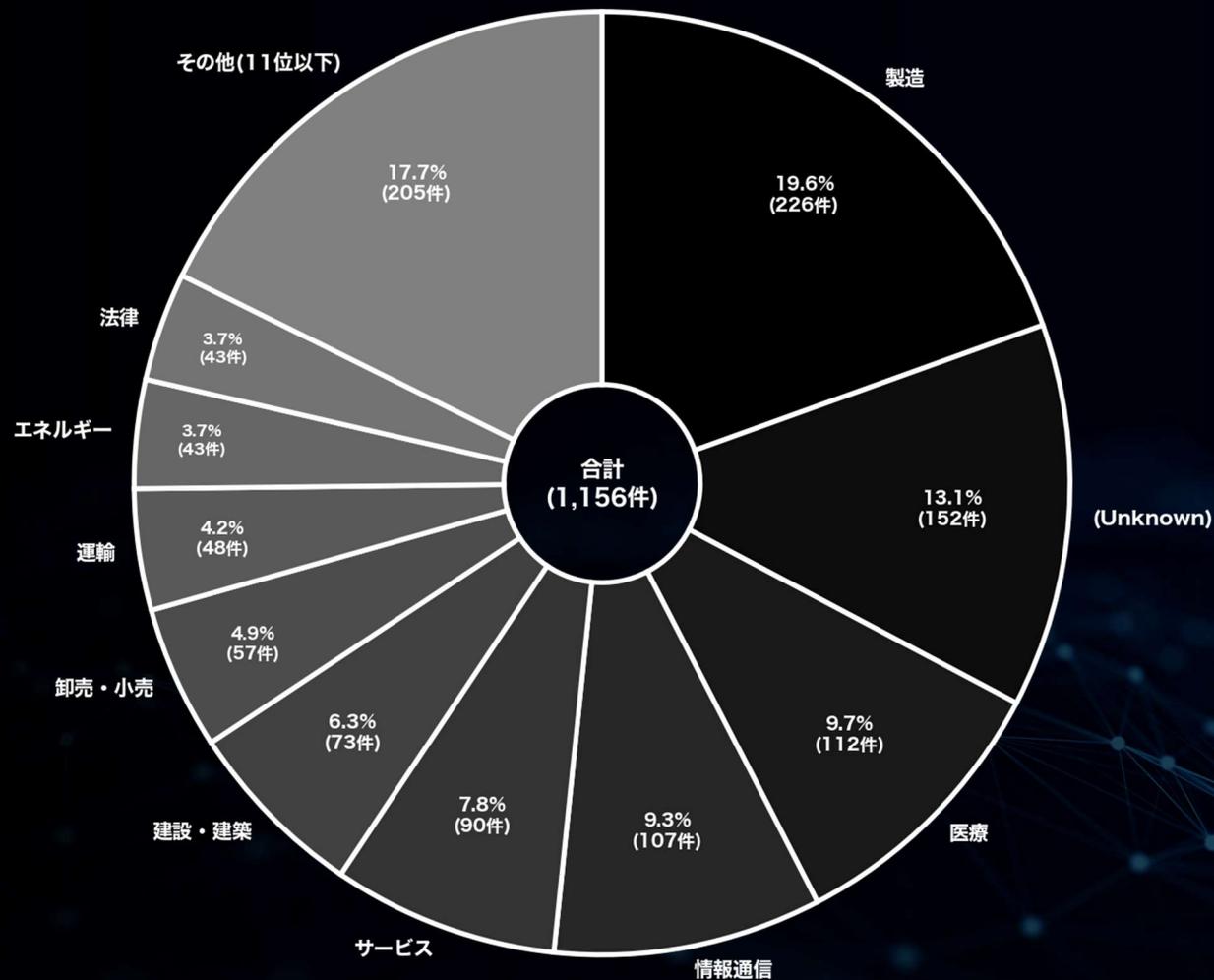
# 月別内訳 業種 TOP10 (全世界)

(2026年 2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	226	19.6	+ 84
(Unknown)	152	13.1	+ 109
医療	112	9.7	+ 58
情報通信	107	9.3	+ 8
サービス	90	7.8	+ 25
建設・建築	73	6.3	- 1
卸売・小売	57	4.9	- 6
運輸	48	4.2	+ 18
エネルギー	43	3.7	+ 16
法律	43	3.7	+ 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  
2

# 被害数の推移 (全世界及び国内)

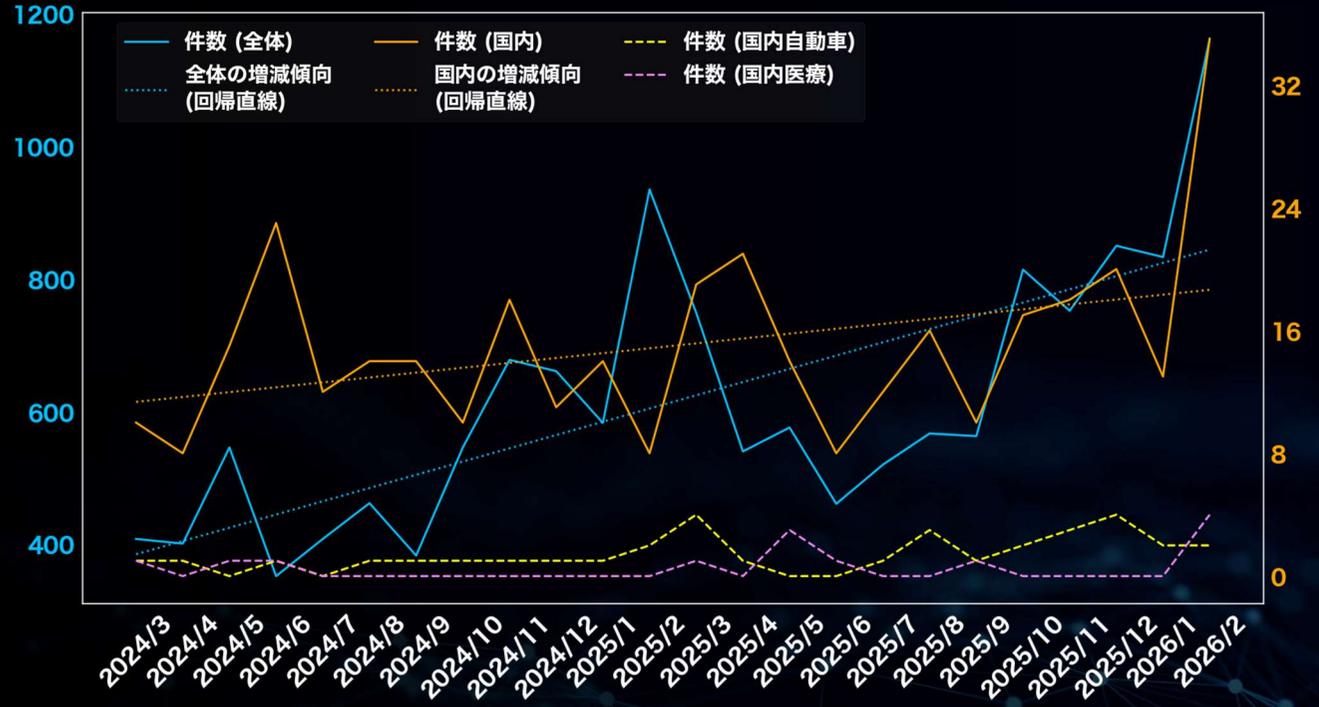
## (過去2年間 / 2024年3月～2026年2月)

※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)
2024/3	408	10	1	1
2024/4	401	8	1	0
2024/5	546	15	0	1
2024/6	352	23	1	1
2024/7	408	12	0	0
2024/8	462	14	1	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	19	4	1
2025/4	540	21	1	0
2025/5	576	14	0	3
2025/6	461	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	18	3	0
2025/12	850	20	4	0
2026/1	833	13	2	0
2026/2	1162	35	2	4
合計	14750	360	34	13

### ▼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

2

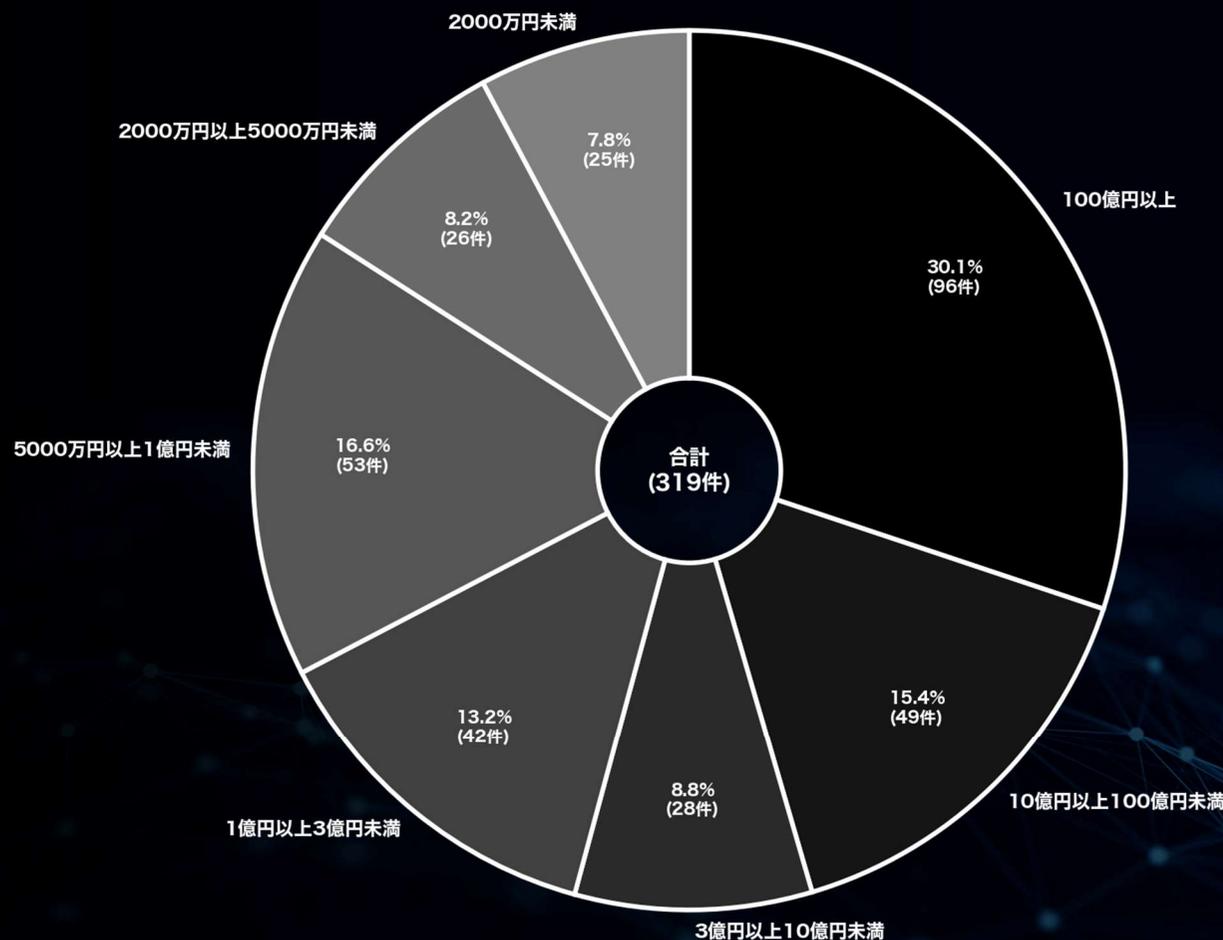
# 資本金別 (国内)

(過去2年間 / 2024年3月～2026年2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	96	30.1
10億円以上100億円未満	49	15.4
3億円以上10億円未満	28	8.8
1億円以上3億円未満	42	13.2
5000万円以上1億円未満	53	16.6
2000万円以上5000万円未満	26	8.2
2000万円未満	25	7.8

▼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)

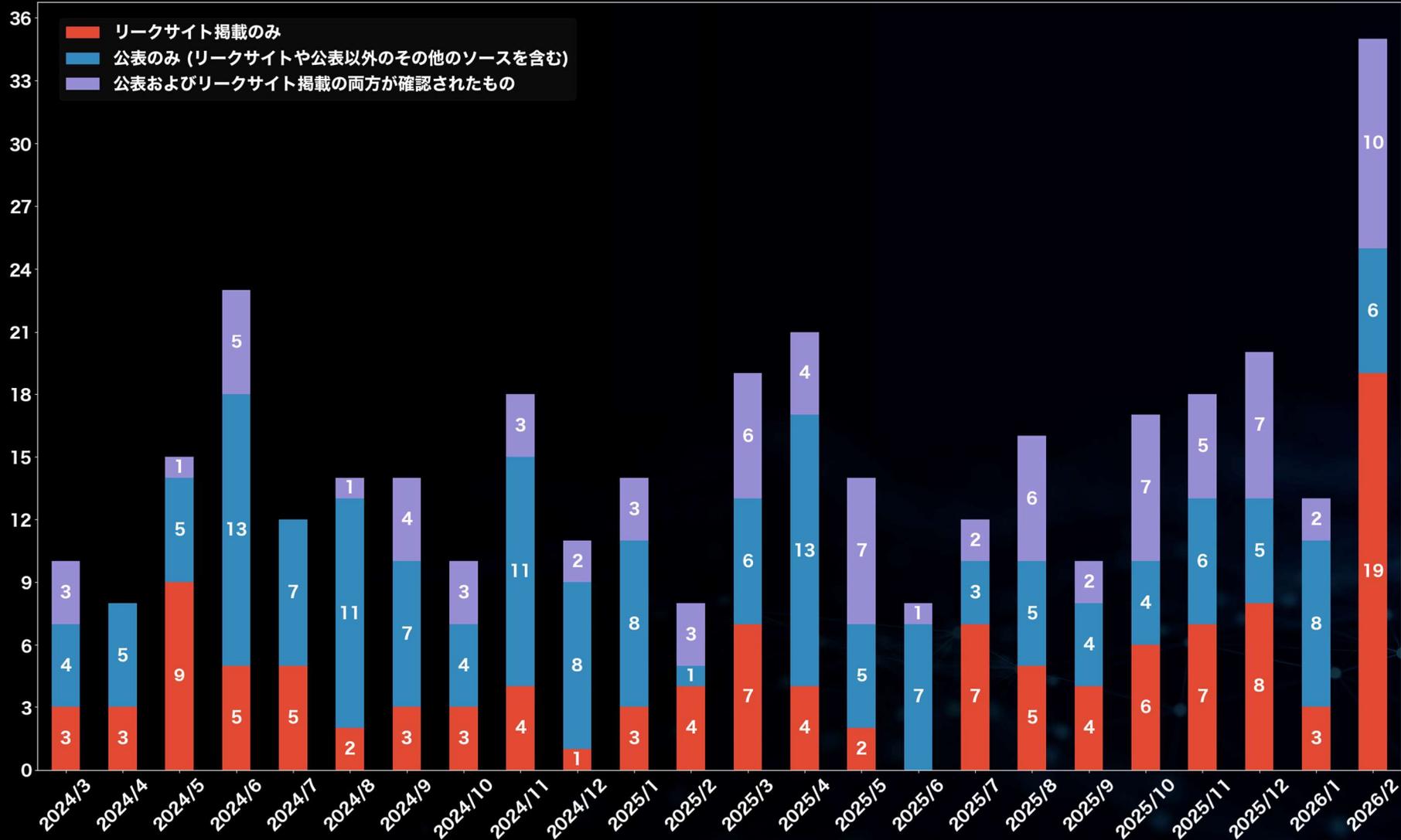
2026

2

# 公表割合 月別内訳 (国内)

(過去2年間 / 2024年3月～2026年2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

2

# 公となった国内被害組織概要一覧 (国内)

## (過去1年間/2025年3月~2026年2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
2025/3	(Unknown)	粘着テープ製造(海外拠点)
2025/3	Qilin (Agenda)	医療機関
2025/3	RansomHub	リビルド品製造
2025/3	(Unknown)	不動産仲介
2025/3	Night Spire	塗料メーカー
2025/3	Qilin (Agenda)	産業用機器メーカー(海外拠点)
2025/3	Night Spire	ボンディングワイヤーメーカー(海外拠点)
2025/3	Qilin (Agenda)	自動制御機器製品メーカー(海外拠点)
2025/3	CACTUS	自動車部品メーカー(海外拠点)
2025/3	(Unknown)	流体制御機器 (バルブ) 製造
2025/3	(Unknown)	ソフトウェア開発
2025/3	Blackout	機器部品メーカー
2025/3	Cicada3301	精密部品メーカー
2025/3	RansomHub	一般機械器具製造業
2025/3	Night Spire	特殊鋼部品メーカー(海外拠点)
2025/3	Night Spire	切削工具メーカー(海外拠点)
2025/3	(Unknown)	百貨店業
2025/3	(Unknown)	鉄鋼製品メーカー(海外拠点)
2025/3	KILLSEC	事務機器メーカー(海外拠点)
2025/4	KILLSEC	情報機器メーカー(海外拠点)
2025/4	AKIRA	大手総合印刷・電子材料メーカー(海外拠点)
2025/4	SARCOMA	大手総合化学メーカー(海外拠点)
2025/4	AKIRA	自動化装置メーカー(海外拠点)
2025/4	(Unknown)	総合エンジニアリング企業
2025/4	(Unknown)	トラック・バス等販売
2025/4	Night Spire	センサ・電子部品メーカー
2025/4	(Unknown)	総合建設業
2025/4	(Unknown)	総合物流事業者
2025/4	Qilin (Agenda)	精密機械製造(海外拠点)
2025/4	(Unknown)	エネルギーコンサルティング
2025/4	(Unknown)	ガソリンスタンド運営
2025/4	(Unknown)	私立大学
2025/4	(Unknown)	総合建設業
2025/4	(Unknown)	総合建設業

被害月	攻撃グループ	業種概要
2025/4	(Unknown)	コンクリートの劣化調査
2025/4	(Unknown)	総合物流事業者
2025/4	Gunra	不動産会社
2025/4	(Unknown)	情報通信機器製造業(海外拠点)
2025/4	(Unknown)	ワイヤーハーネス製造
2025/4	Termite	光応用製品メーカー(海外拠点)
2025/5	LYNX	食品物流事業者
2025/5	Gunra	総合包装メーカー
2025/5	Gunra	船舶内装・総合建設業
2025/5	SAFEPAY	経営コンサルティング
2025/5	(Unknown)	学校法人
2025/5	Qilin (Agenda)	医薬品開発支援(海外拠点)
2025/5	(Unknown)	医療機器・介護用品商社
2025/5	(Unknown)	医療機器・消耗品商社
2025/5	BlackLock	大手映画制作・配給業
2025/5	DEVMAN	大手映画制作・配給業
2025/5	(Unknown)	化学メーカー
2025/5	(Unknown)	特殊鋼・合金メーカー
2025/5	Space Bears	ゴム製品メーカー(海外拠点)
2025/5	PLAY	通信機器メーカー(海外拠点)
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

被害月	攻撃グループ	業種概要
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	バ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
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\$ Hun...	大手自動車メーカー
2025/10	Scattered LAPSUS\$ Hun...	大手スポーツ用品メーカー

(※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3月~2026年2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
2025/10	Scattered LAPSUS\$ Hun...	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)	弁護士法人
2025/11	(Unknown)	システムインテグレーター
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
2025/12	(Unknown)	エレクトロニクス専門商社(海外拠点)

被害月	攻撃グループ	業種概要
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	総合テレオペラー
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)
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

被害月	攻撃グループ	業種概要
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)	総合テレオペラー
2026/2	NetRunner	総合病院
2026/2	(Unknown)	ホテル業・飲食店業
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	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

(※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)

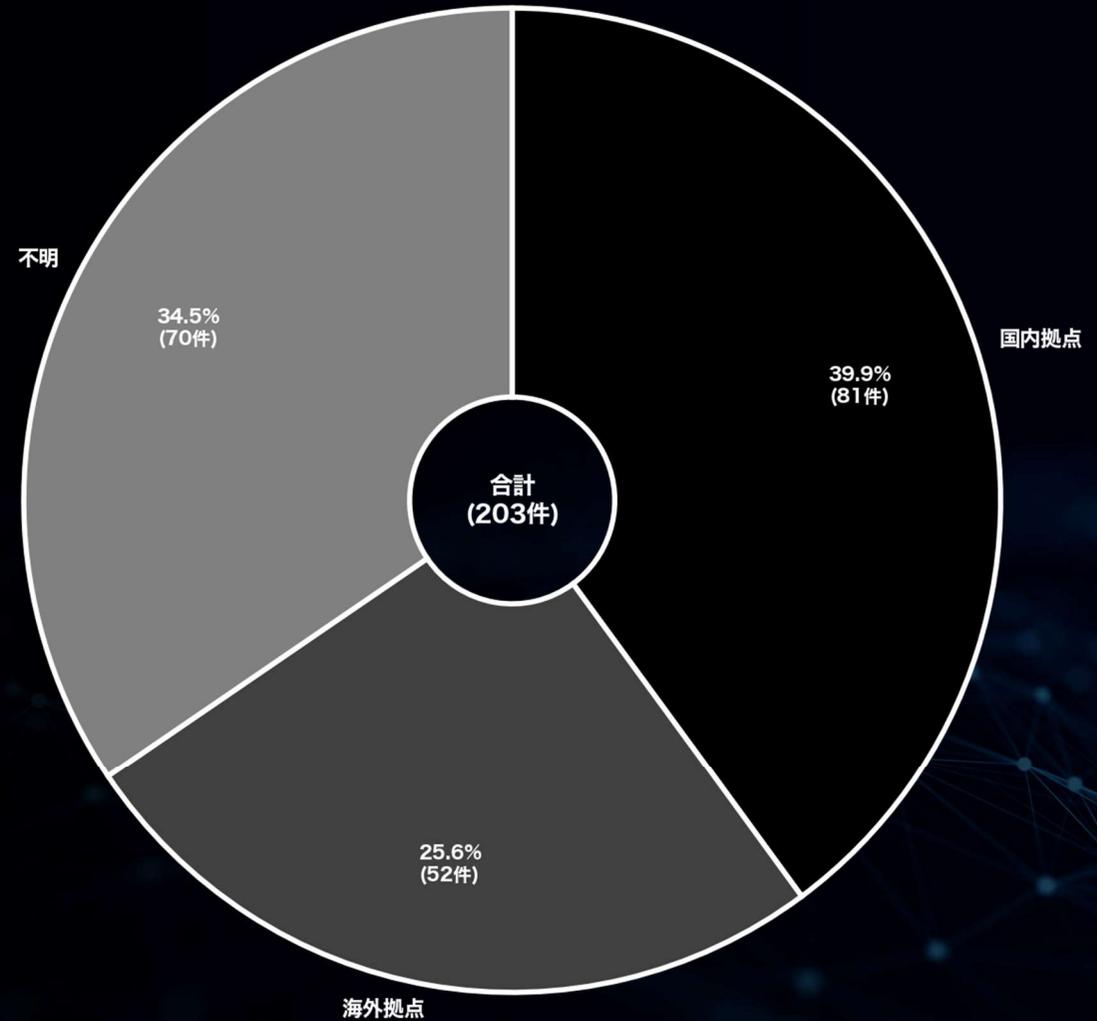
## (過去1年間/2025年3月~2026年2月)

(※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	81	39.9
海外拠点	52	25.6
不明	70	34.5



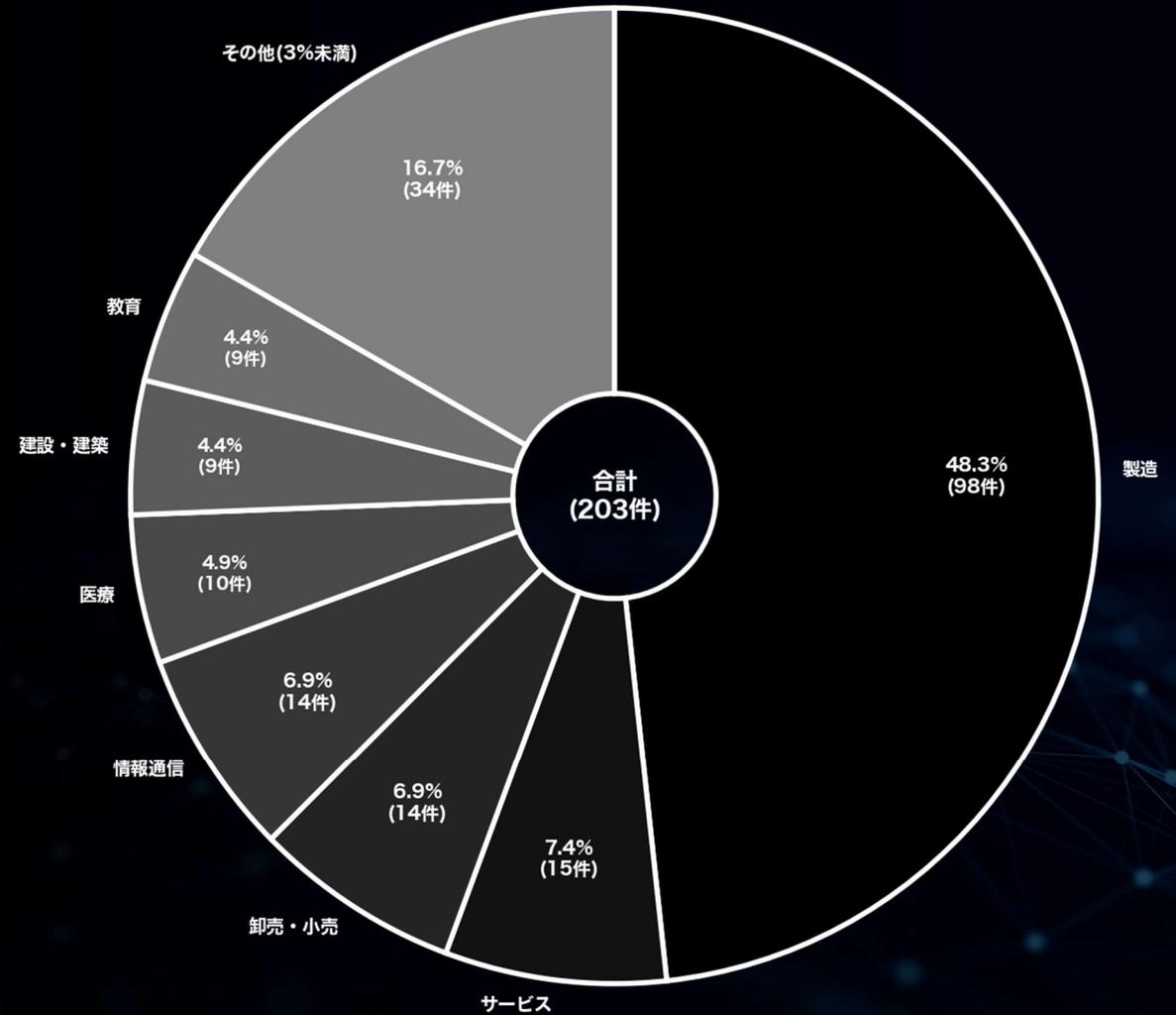
(※本ページの表/グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

# 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3月~2026年2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	98	48.3
サービス	15	7.4
卸売・小売	14	6.9
情報通信	14	6.9
医療	10	4.9
建設・建築	9	4.4
教育	9	4.4
その他(3%未満)	34	16.7



(※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

2

# 中小企業における被害分析

(国内)

中小企業の定義<sup>\*</sup>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)

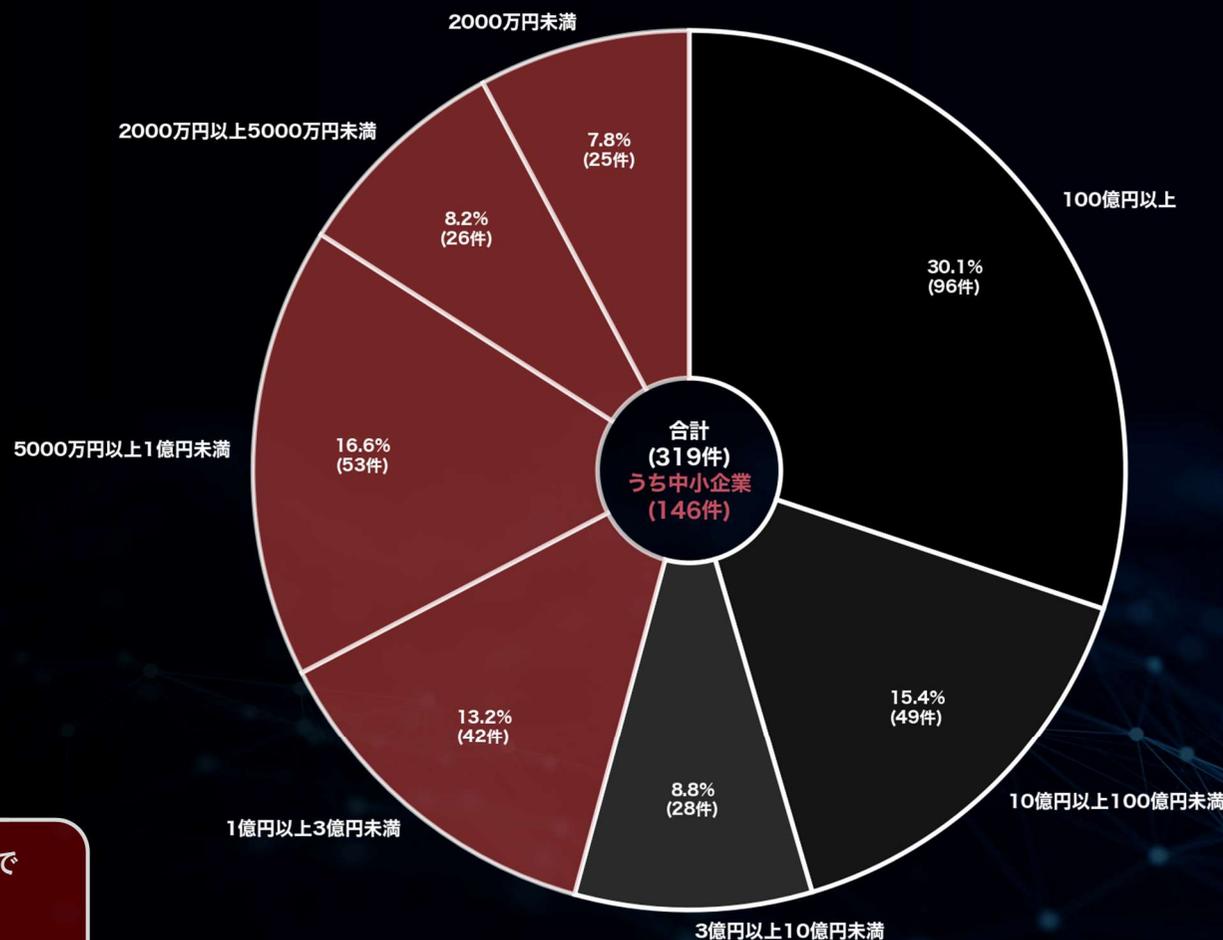
(過去2年間 / 2024年3月～2026年2月)

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	96	30.1
10億円以上100億円未満	49	15.4
3億円以上10億円未満	28	8.8
1億円以上3億円未満	42	13.2
5000万円以上1億円未満	53	16.6
2000万円以上5000万円未満	26	8.2
2000万円未満	25	7.8

▼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146件にのぼり、全体の45.8%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。

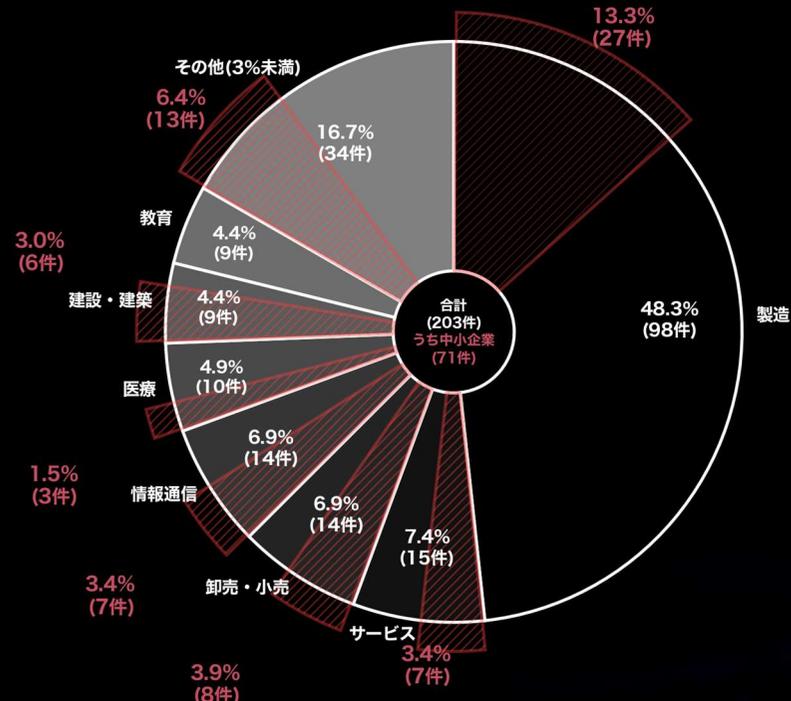
(※本ページの表/グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

# 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3月~2026年2月)

赤色は中小企業を示す

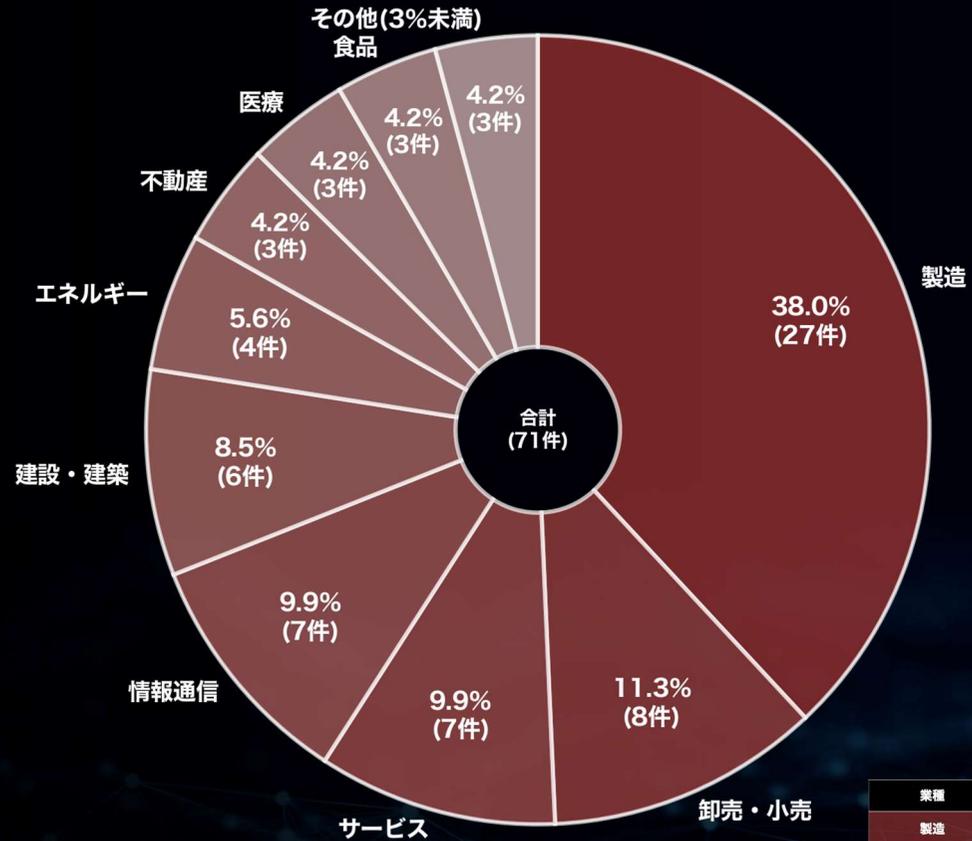
▼全体割合



※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	98 (27)	48.3 (13.3)
サービス	15 (7)	7.4 (3.4)
卸売・小売	14 (8)	6.9 (3.9)
情報通信	14 (7)	6.9 (3.4)
医療	10 (3)	4.9 (1.5)
建設・建築	9 (6)	4.4 (3.0)
教育	9	4.4
その他(3%未満)	34 (13)	16.7 (6.4)

▼中小企業のための割合



業種	件数	割合 (%)
製造	27	38.0
卸売・小売	8	11.3
サービス	7	9.9
情報通信	7	9.9
建設・建築	6	8.5
エネルギー	4	5.6
不動産	3	4.2
医療	3	4.2
食品	3	4.2
その他(3%未満)	3	4.2

過去1年間の業種別分析においては、中小企業のみには抜粋すると、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

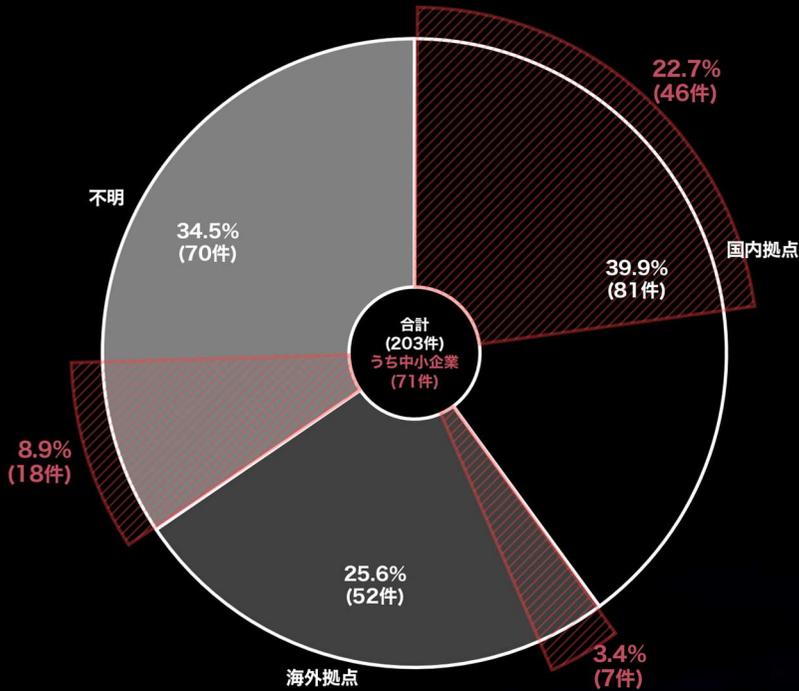
(※本ページの表/グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

# 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)

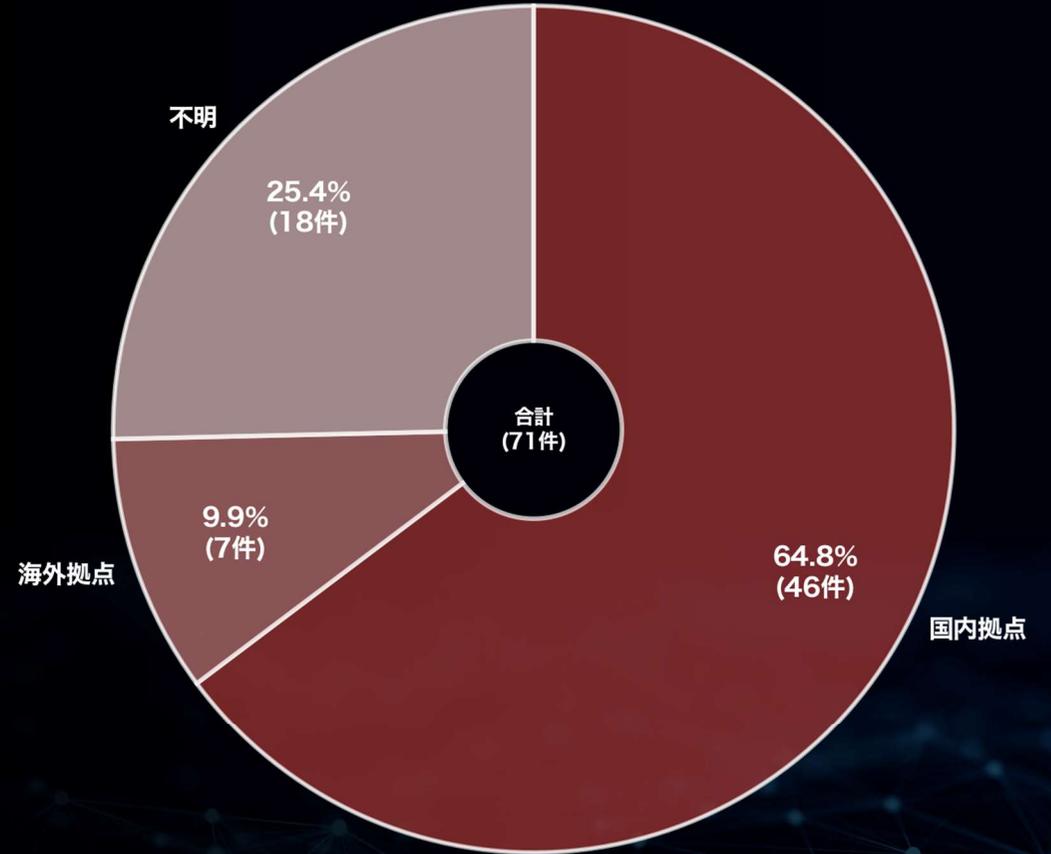
(過去1年間/2025年3月~2026年2月)

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	81 (46)	39.9 (22.7)
海外拠点	52 (7)	25.6 (3.4)
不明	70 (18)	34.5 (8.9)
合計	203 (71)	100 (35.0)

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	46	64.8
海外拠点	7	9.9
不明	18	25.4

(※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)

# 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3月~2026年2月)

赤色は中小企業を示す

被害月	攻撃グループ	業種概要
2025/3	(Unknown)	粘着テープ製造(海外拠点)
2025/3	Qilin (Agenda)	医療機関
2025/3	RansomHub	リビルド品製造
2025/3	(Unknown)	不動産仲介
2025/3	Night Spire	塗料メーカー
2025/3	Qilin (Agenda)	産業用機器メーカー(海外拠点)
2025/3	Night Spire	ボンディングワイヤメーカー(海外拠点)
2025/3	Qilin (Agenda)	自動制御機器製品メーカー(海外拠点)
2025/3	CACTUS	自動車部品メーカー(海外拠点)
2025/3	(Unknown)	流体制御機器(バルブ)製造
2025/3	(Unknown)	ソフトウェア開発
2025/3	Blackout	機器部品メーカー
2025/3	Cicada3301	精密部品メーカー
2025/3	RansomHub	一般機械器具製造業
2025/3	Night Spire	特殊鋼部品メーカー(海外拠点)
2025/3	Night Spire	切削工具メーカー(海外拠点)
2025/3	(Unknown)	百貨店業
2025/3	(Unknown)	鉄鋼製品メーカー(海外拠点)
2025/3	KILLSEC	事務機器メーカー(海外拠点)
2025/4	KILLSEC	情報機器メーカー(海外拠点)
2025/4	AKIRA	大手総合印刷・電子材料メーカー(海外拠点)
2025/4	SARCOMA	大手総合化学メーカー(海外拠点)
2025/4	AKIRA	自動化装置メーカー(海外拠点)
2025/4	(Unknown)	総合エンジニアリング企業
2025/4	(Unknown)	トラック・バス等販売
2025/4	Night Spire	センサ・電子部品メーカー
2025/4	(Unknown)	総合建設業
2025/4	(Unknown)	総合物流事業者
2025/4	Qilin (Agenda)	精密機械製造(海外拠点)
2025/4	(Unknown)	エネルギーコンサルティング
2025/4	(Unknown)	ガソリンスタンド運営
2025/4	(Unknown)	私立大学
2025/4	(Unknown)	総合建設業
2025/4	(Unknown)	総合建設業

被害月	攻撃グループ	業種概要
2025/4	(Unknown)	コンクリートの劣化調査
2025/4	(Unknown)	総合物流事業者
2025/4	Gunra	不動産会社
2025/4	(Unknown)	情報通信機器製造業(海外拠点)
2025/4	(Unknown)	ワイヤーハーネス製造
2025/4	Termite	光応用製品メーカー(海外拠点)
2025/5	LYNX	食品物流事業者
2025/5	Gunra	総合包装メーカー
2025/5	Gunra	船舶内装・総合建設業
2025/5	SAFEPAY	経営コンサルティング
2025/5	(Unknown)	学校法人
2025/5	Qilin (Agenda)	医薬品開発支援(海外拠点)
2025/5	(Unknown)	医療機器・介護用品商社
2025/5	(Unknown)	医療機器・消耗品商社
2025/5	BlackLock	大手映画制作・配給業
2025/5	DEVMAN	大手映画制作・配給業
2025/5	(Unknown)	化学メーカー
2025/5	(Unknown)	特殊鋼・合金メーカー
2025/5	Space Bears	ゴム製品メーカー(海外拠点)
2025/5	PLAY	通信機器メーカー(海外拠点)
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

被害月	攻撃グループ	業種概要
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	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
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\$ Hun...	大手自動車メーカー
2025/10	Scattered LAPSUS\$ Hun...	大手スポーツ用品メーカー

※ (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3月~2026年2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
2025/10	Scattered LAPSUS\$ Hun...	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
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
2025/12	(Unknown)	エレクトロニクス専門商社(海外拠点)

被害月	攻撃グループ	業種概要
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	総合テロップター
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)
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

被害月	攻撃グループ	業種概要
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)	総合テロップター
2026/2	NetRunner	総合病院
2026/2	(Unknown)	ホテル業・飲食店業
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	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

※ (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

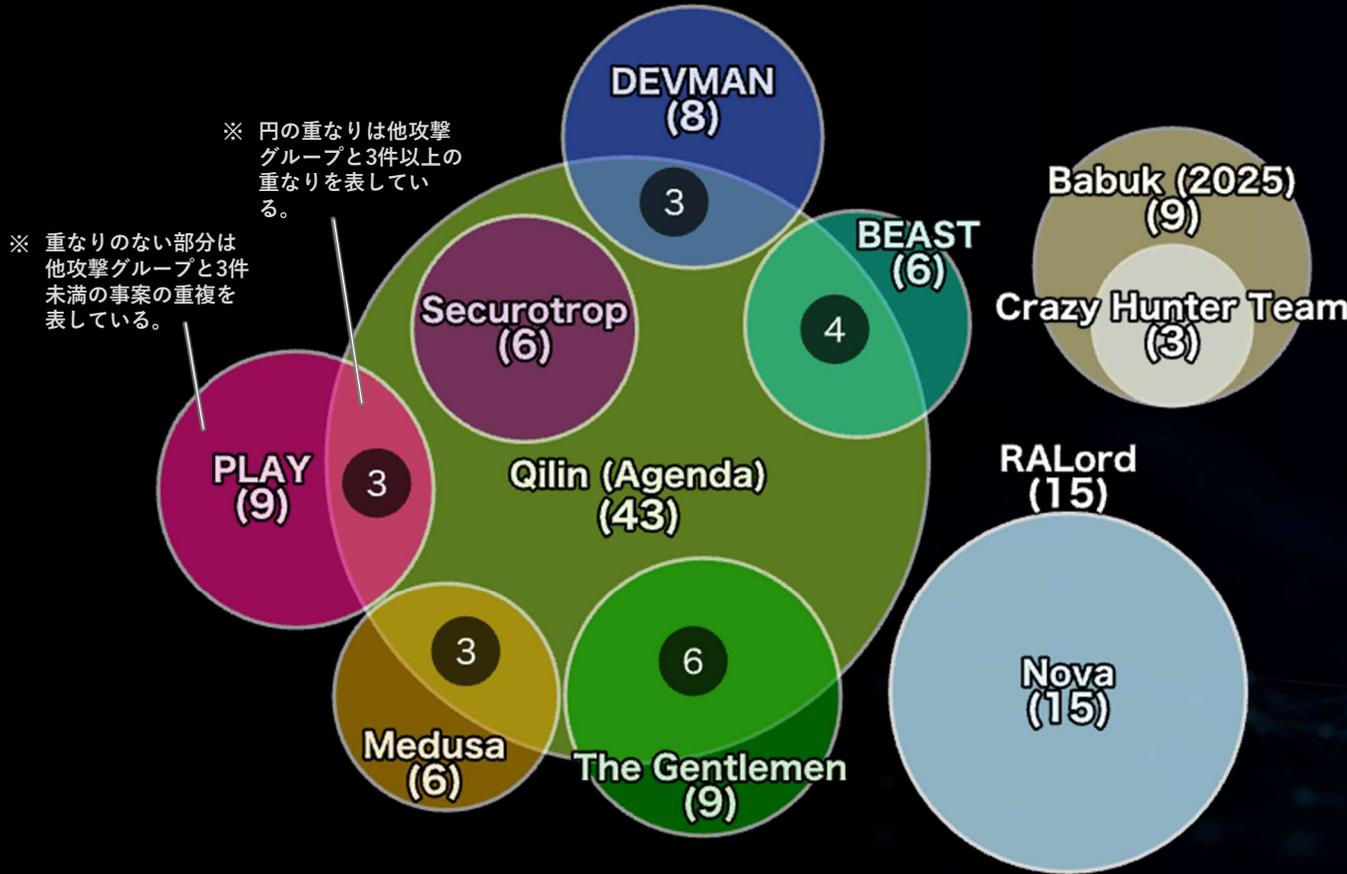
# 多重被害に関する分析

2026

2

# 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3月～2026年2月) (累計136件) ※多重被害に遭った組織数の累計



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。

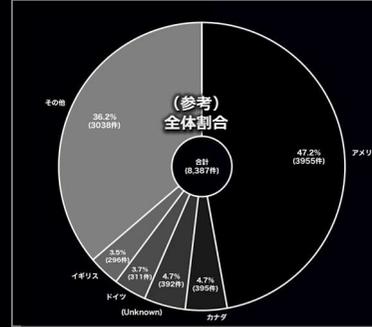
※異なる攻撃グループによるリークサイトへの掲載件数を元に算出

# 多重被害に遭った被害組織の傾向と分析 (全世界)

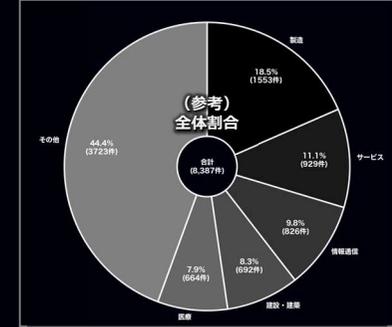
(過去1年間 / 2025年3月～2026年2月)

※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

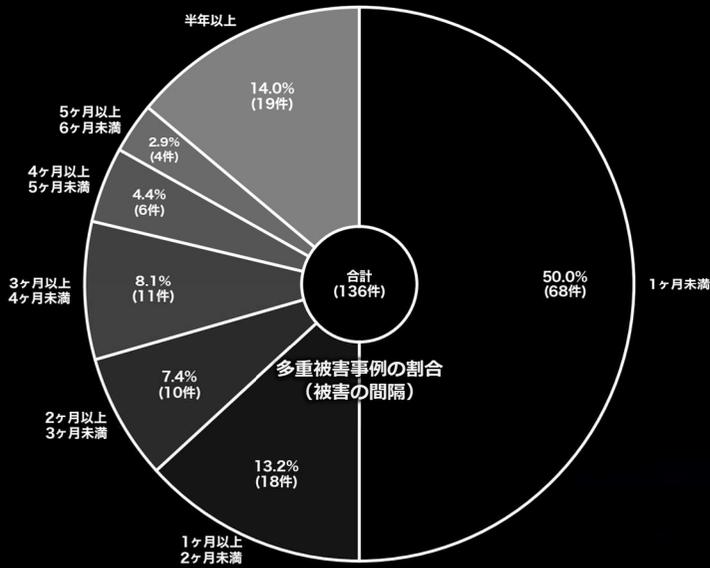


(参考比較) 同期間の全データにおける割合

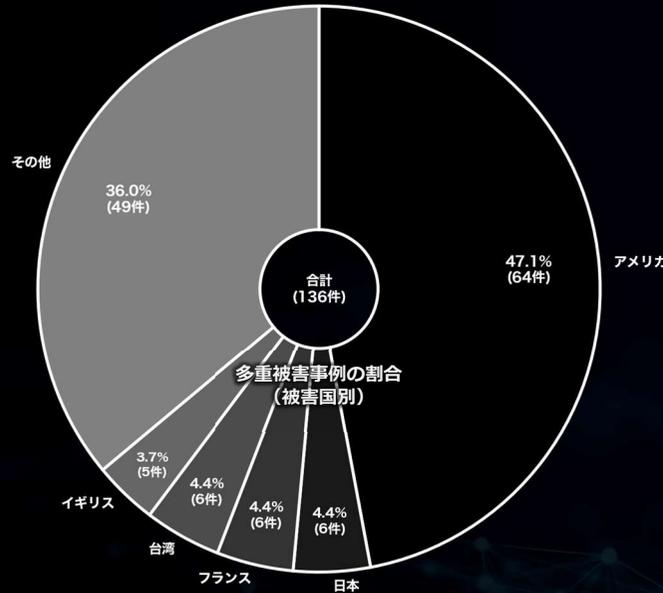


## ▼被害の間隔

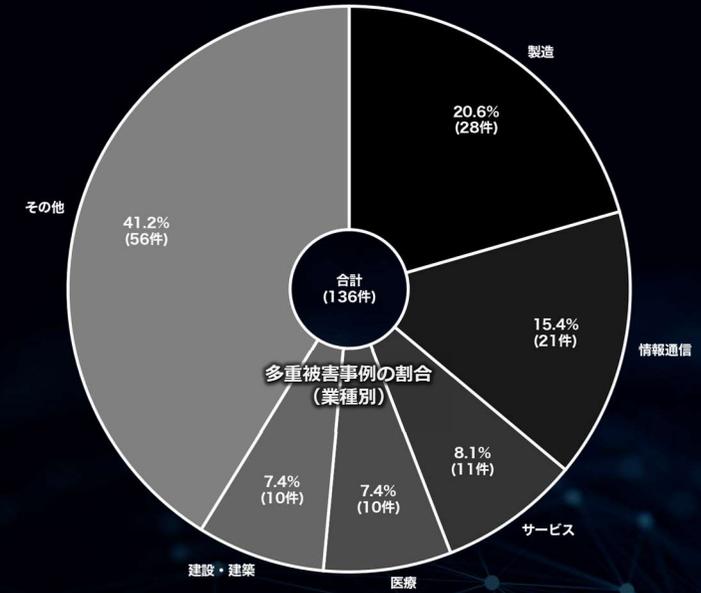
(一度目の被害から二度目の被害までの間隔)



## ▼被害国別



## ▼業種別



## ▶多重被害に遭った組織数の累計：136件 (全体8387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)

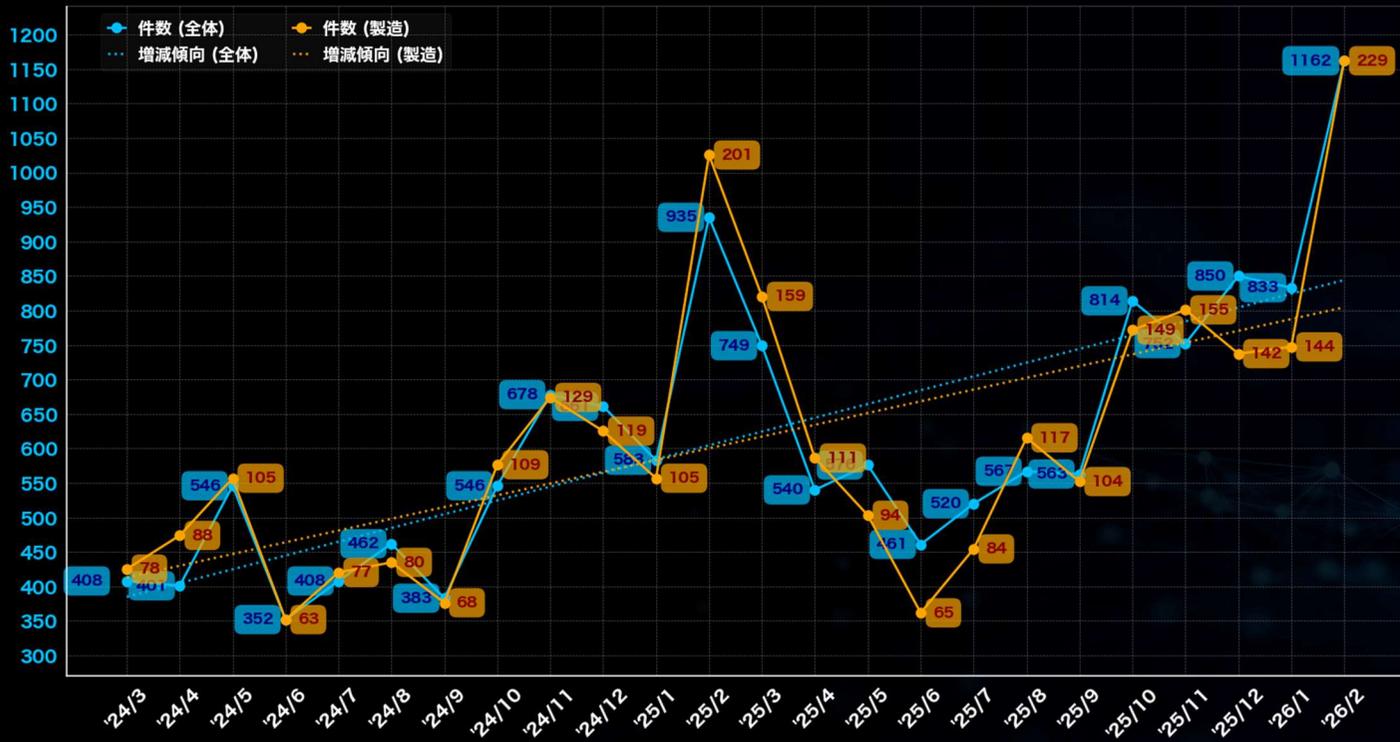
2026  
2

# 業種に関する分析 (全世界)

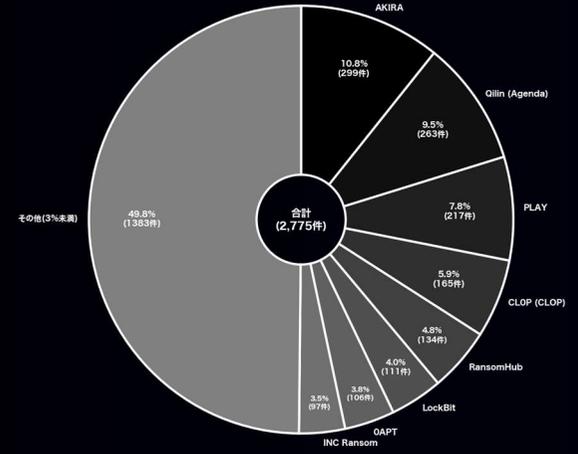
## (過去2年間 / 2024年3月～2026年2月)

### 製造

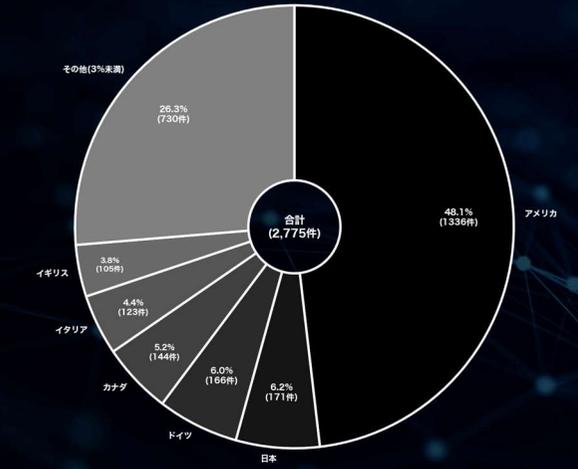
「製造」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年2月で、229件の掲載があった。一方、最も少なかった月は2024年6月で、63件であった。被害組織の所在国の割合では、アメリカが約48%と最も多く、次いで日本とドイツがそれぞれ約6%である。攻撃グループについては、少なくとも135のグループが関与しており、特に「AKIRA」が299件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「PLAY」がそれぞれ263件と217件の掲載を行っている。製造関連の件数は全体件数に対して高い割合で推移しており、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)

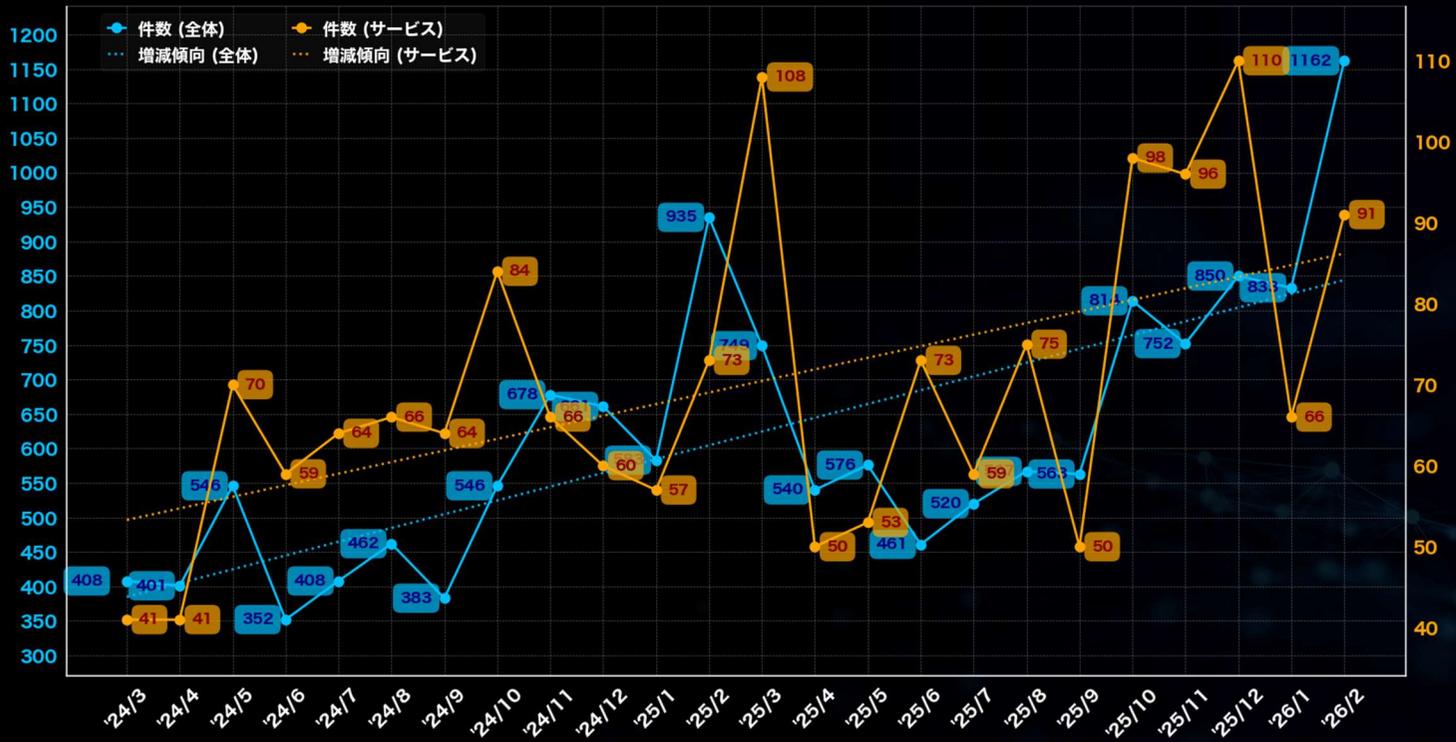
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

# 業種に関する分析 (全世界)

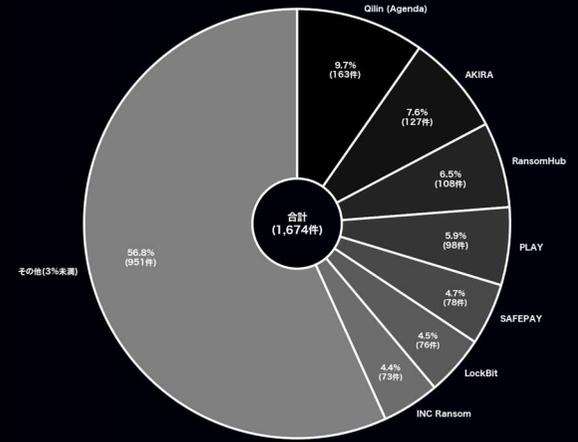
## (過去2年間 / 2024年3月 ~ 2026年2月)

### サービス

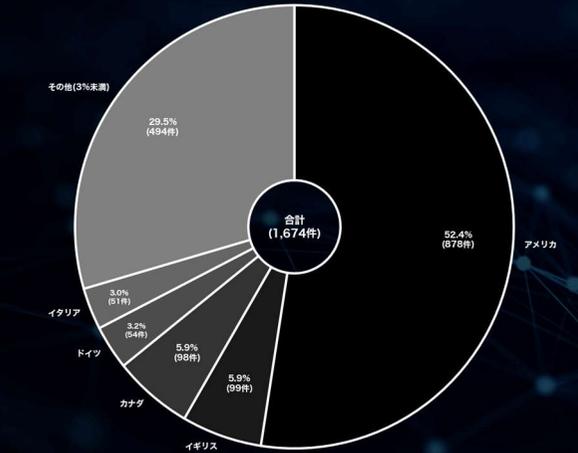
「サービス」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年12月で、110件の掲載があった。一方、最も少なかった月は2024年3月および4月で、41件であった。被害組織の所在国の割合では、アメリカが約52%と最も多く、次いでイギリスとカナダがそれぞれ約6%である。攻撃グループについては、少なくとも129のグループが関与しており、特に「Qilin (Agenda)」が163件のリークサイト掲載を実施している。次いで「AKIRA」と「RansomHub」がそれぞれ127件と108件の掲載を行っている。サービス関連の件数は製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)

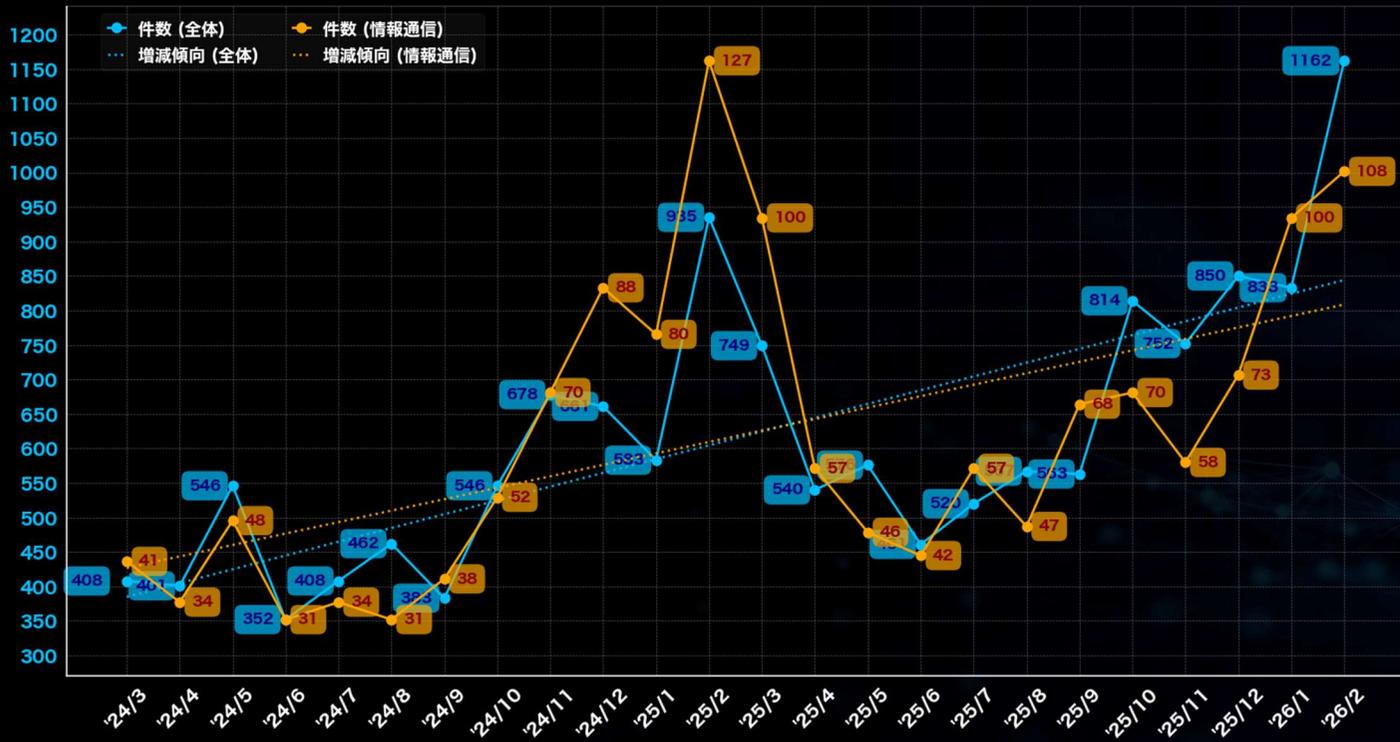
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

# 業種に関する分析 (全世界)

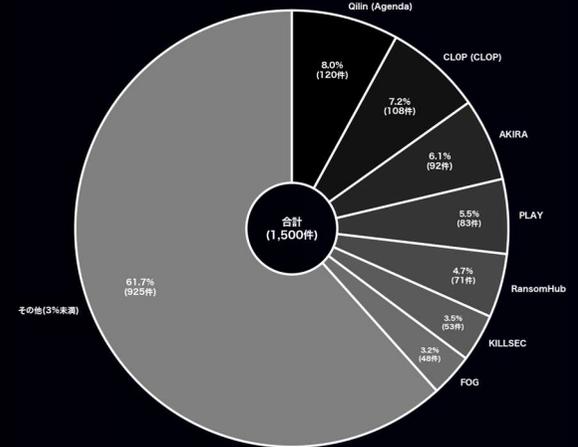
(過去2年間 / 2024年3月 ~ 2026年2月)

## 情報通信

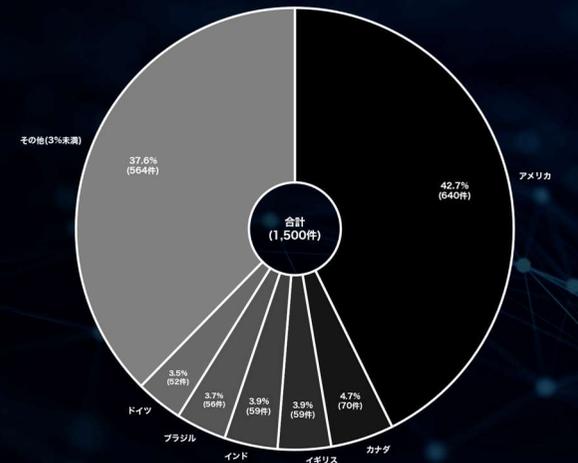
「情報通信」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、127件の掲載があった。一方、最も少なかった月は2024年6月および8月で、31件であった。被害組織の所在国の割合では、アメリカが約43%と最も多く、次いでカナダとイギリスがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも132のグループが関与しており、特に「Qilin (Agenda)」が120件のリークサイト掲載を実施している。次いで「CLOP (CLOP)」と「AKIRA」がそれぞれ108件と92件の掲載を行っている。過去2年間におけるリークサイト掲載件数は明確な増加傾向にある。



▼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)

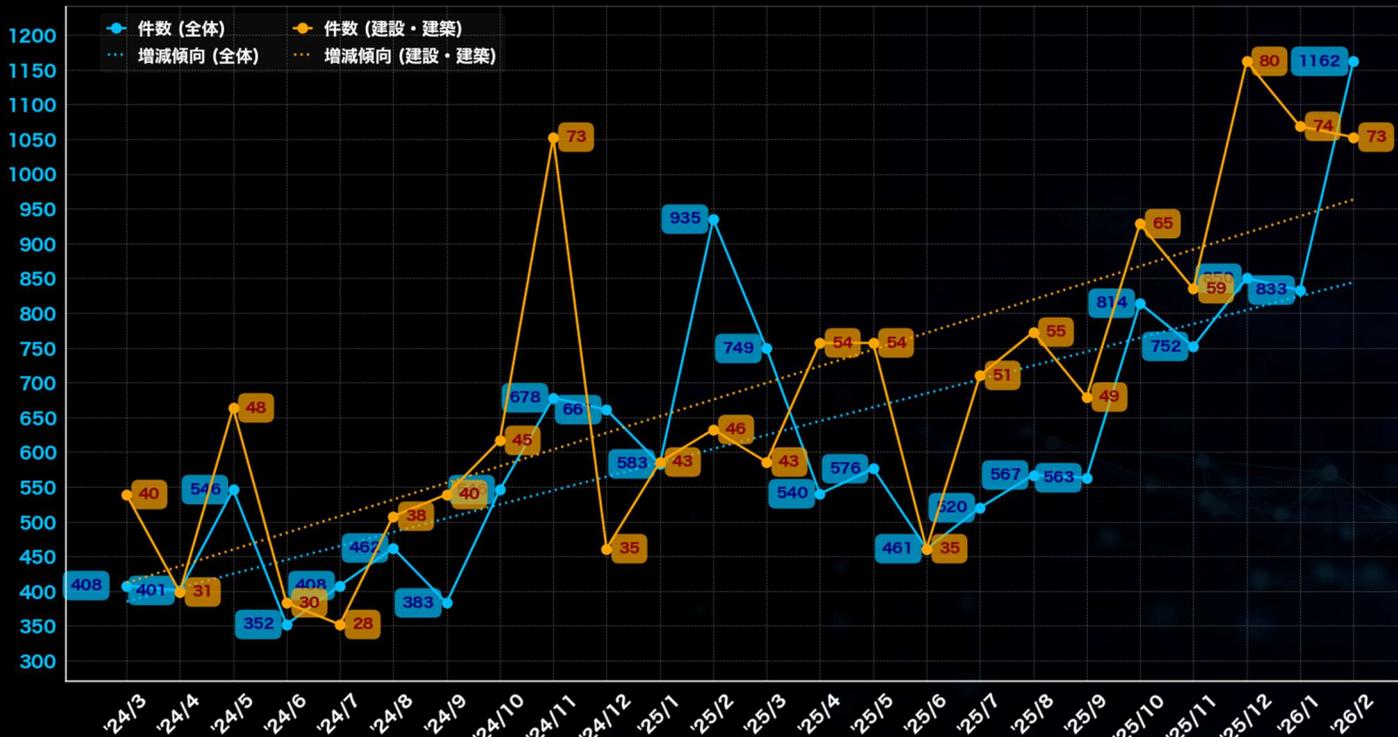
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

# 業種に関する分析 (全世界)

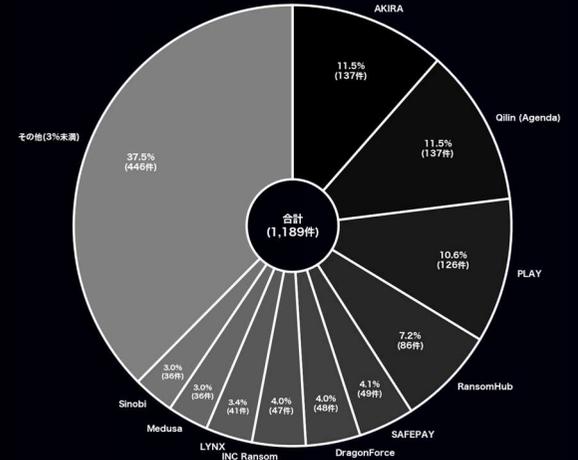
(過去2年間 / 2024年3月～2026年2月)

## 建設・建築

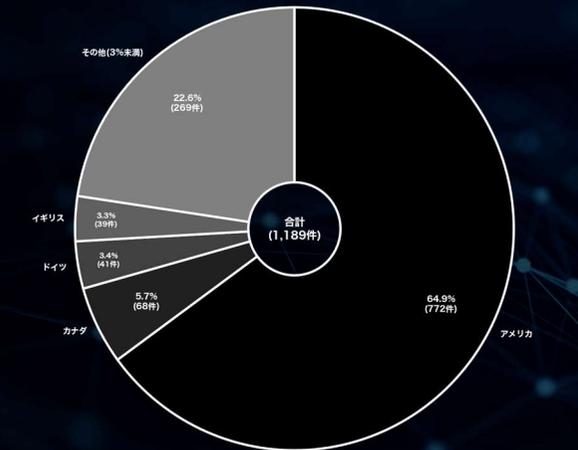
「建設・建築」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年12月で、80件の掲載があった。一方、最も少なかった月は2024年7月で、28件であった。被害組織の所在国の割合では、アメリカが約65%と最も多く、次いでカナダとドイツがそれぞれ約6%と約3%である。攻撃グループについては、少なくとも101のグループが関与しており、特に「AKIRA」が137件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「PLAY」がそれぞれ137件と126件の掲載を行っている。製造関連などと比べると件数は少ないものの、明確な増加傾向にある。



▼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

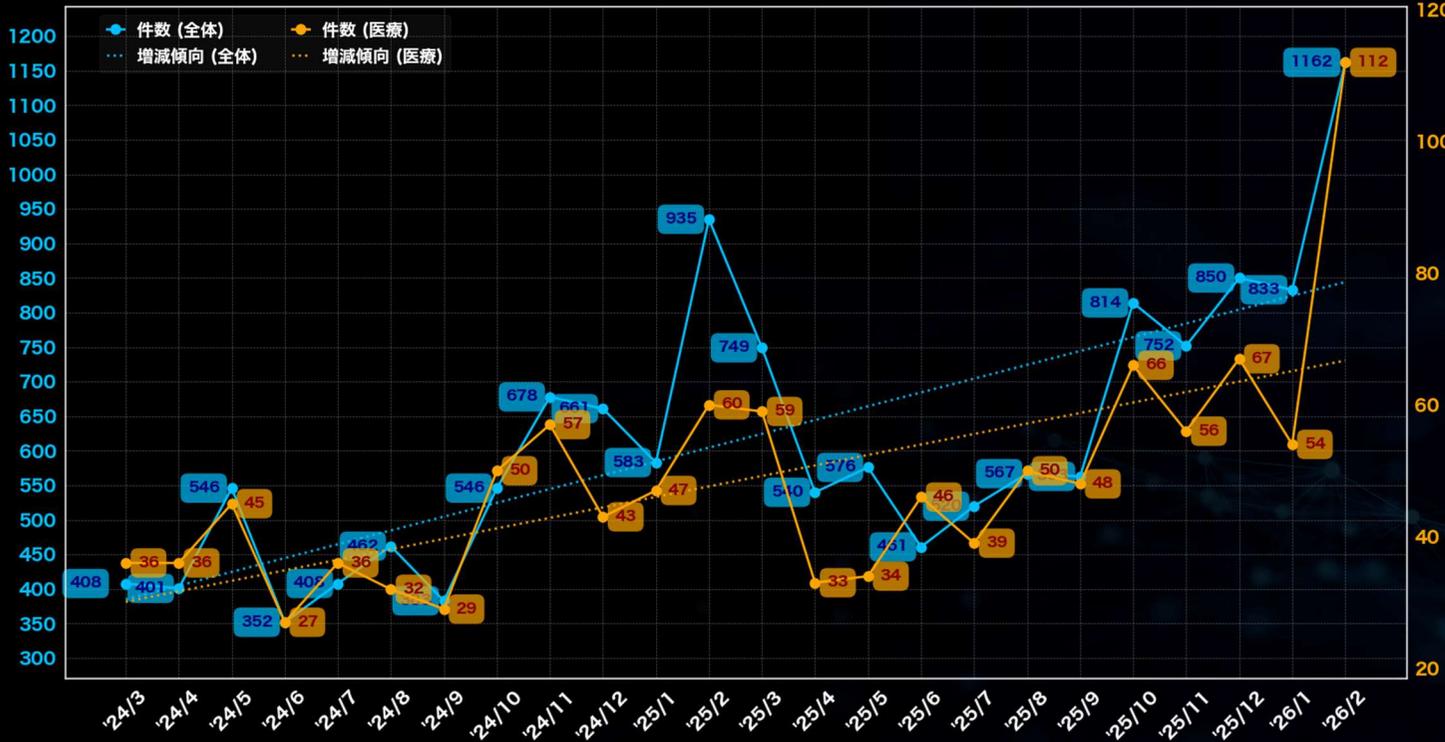
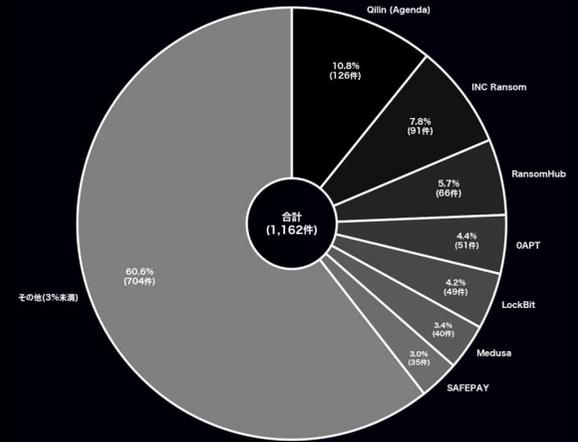
# 業種に関する分析 (全世界)

(過去2年間 / 2024年3月～2026年2月)

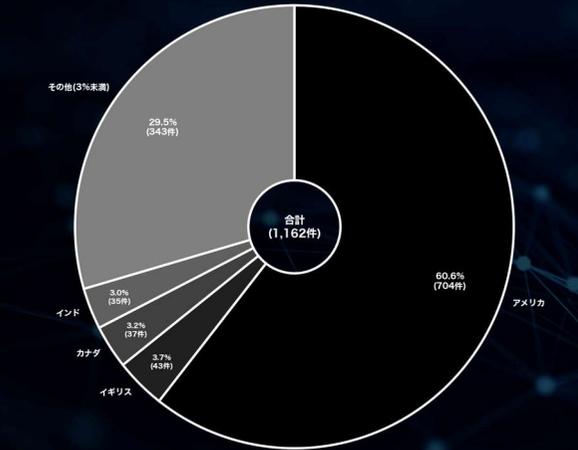
## 医療

「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、112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61%と最も多く、次いでイギリス、カナダがそれぞれ約4%と約3%である。攻撃グループについては、少なくとも116のグループが関与しており、特に「Qilin (Agenda)」が126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91件と66件の掲載を行っている。かつては低水準だった医療関連の被害数は2023年3月頃に増加し、その後もその後も増加傾向が続いている。この変化の背景には、攻撃グループが生存競争の中で業種を問わない攻撃へと方針を転換していった可能性も否定できない。また、国別に見る傾向としてアメリカにおける被害が非常に高い割合を占めている点が顕著である。

▼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

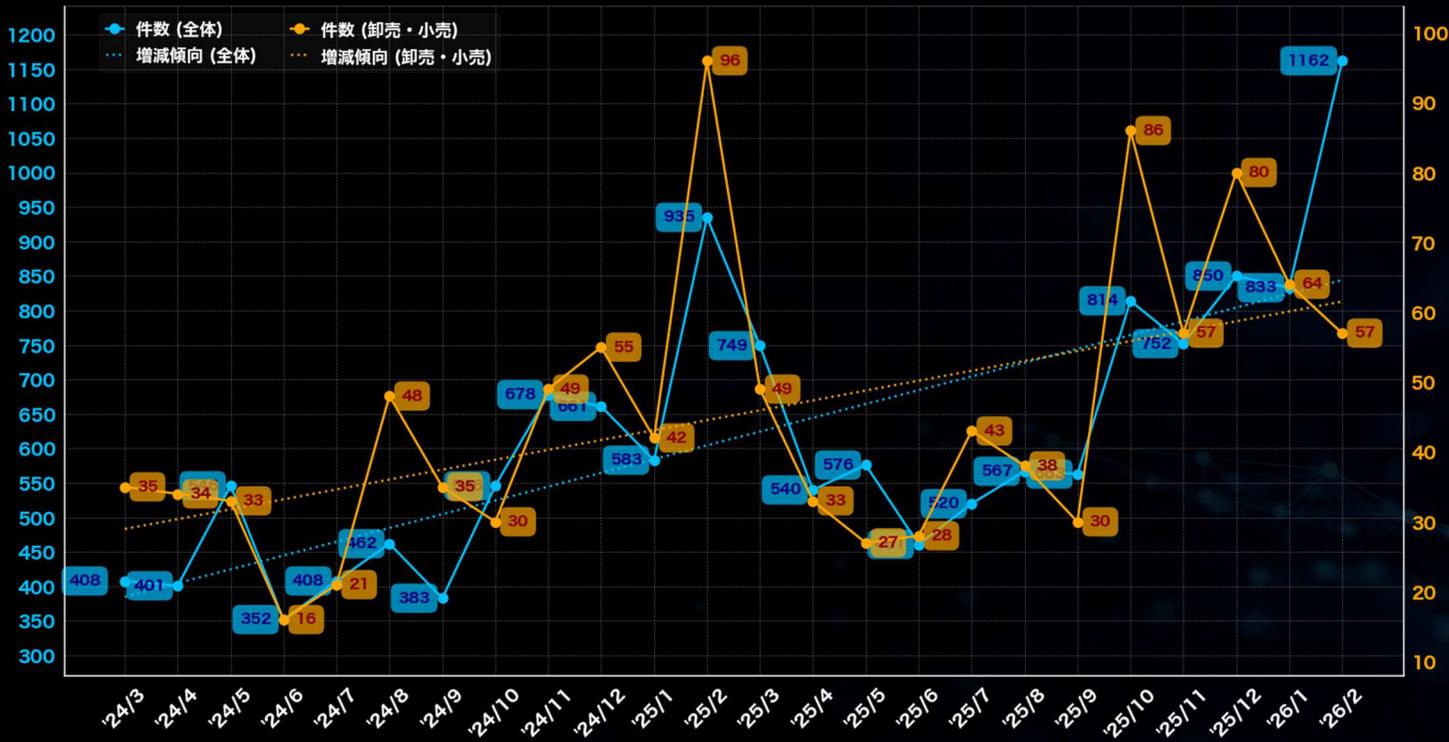
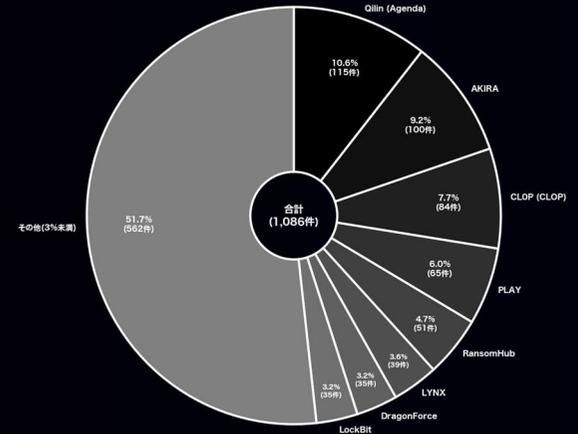
# 業種に関する分析 (全世界)

(過去2年間 / 2024年3月 ~ 2026年2月)

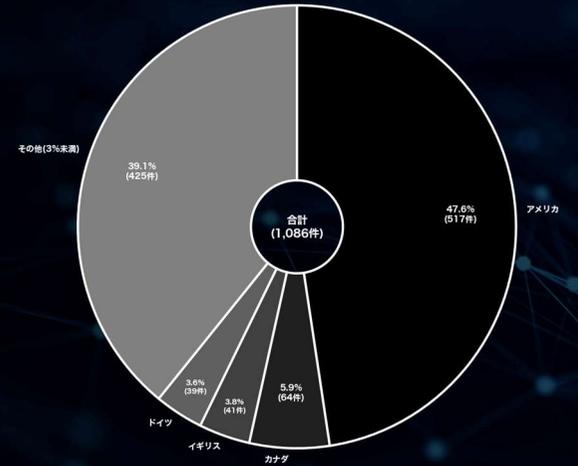
## 卸売・小売

「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48%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104のグループが関与しており、特に「Qilin (Agenda)」が115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100件と84件の掲載を行っている。卸売・小売関連は大きな増減の波があるものの、過去2年間の推移としては明確な増加傾向がある。

▼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)

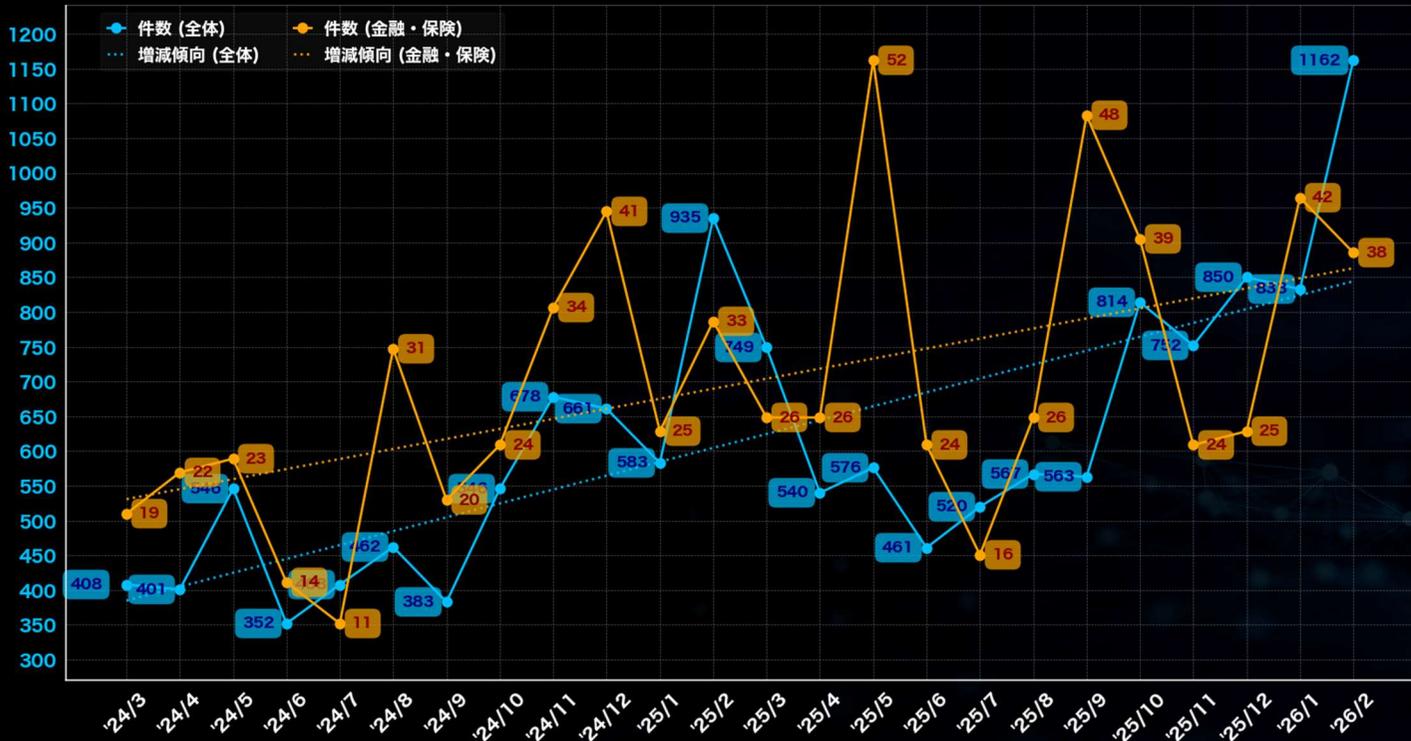
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

# 業種に関する分析 (全世界)

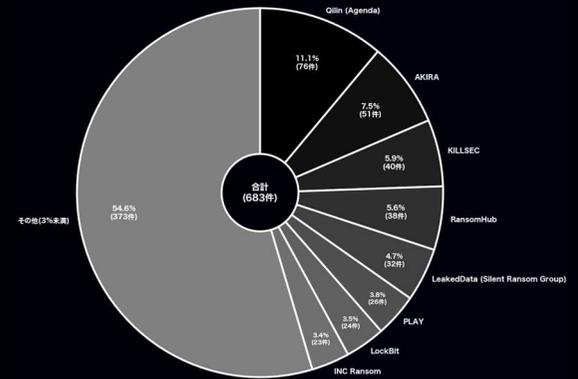
## (過去2年間 / 2024年3月～2026年2月)

### 金融・保険

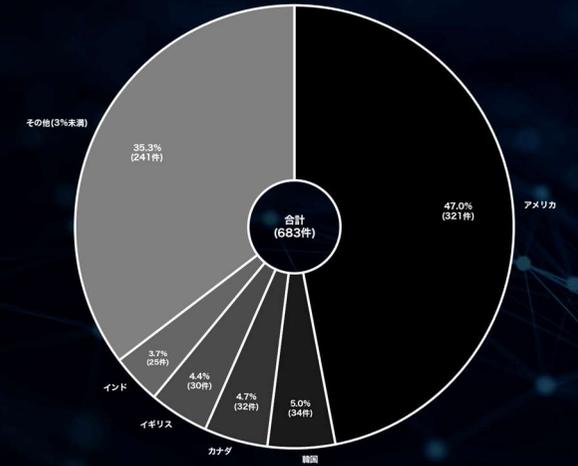
「金融・保険」業界に対するランサムウェア攻撃のリークサイト掲載件数は、最も多かった月が2025年5月で、52件の掲載があった。一方、最も少なかった月は2024年7月で、11件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いで韓国とカナダがそれぞれ約5%である。攻撃グループについては、少なくとも107のグループが関与しており、特に「Qilin (Agenda)」が76件のリークサイト掲載を実施している。次いで「AKIRA」と「KILLSEC」がそれぞれ51件と40件の掲載を行っている。金融・保険関連は全体件数に対する割合は低いものの明確な増加傾向にある。



#### ▼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

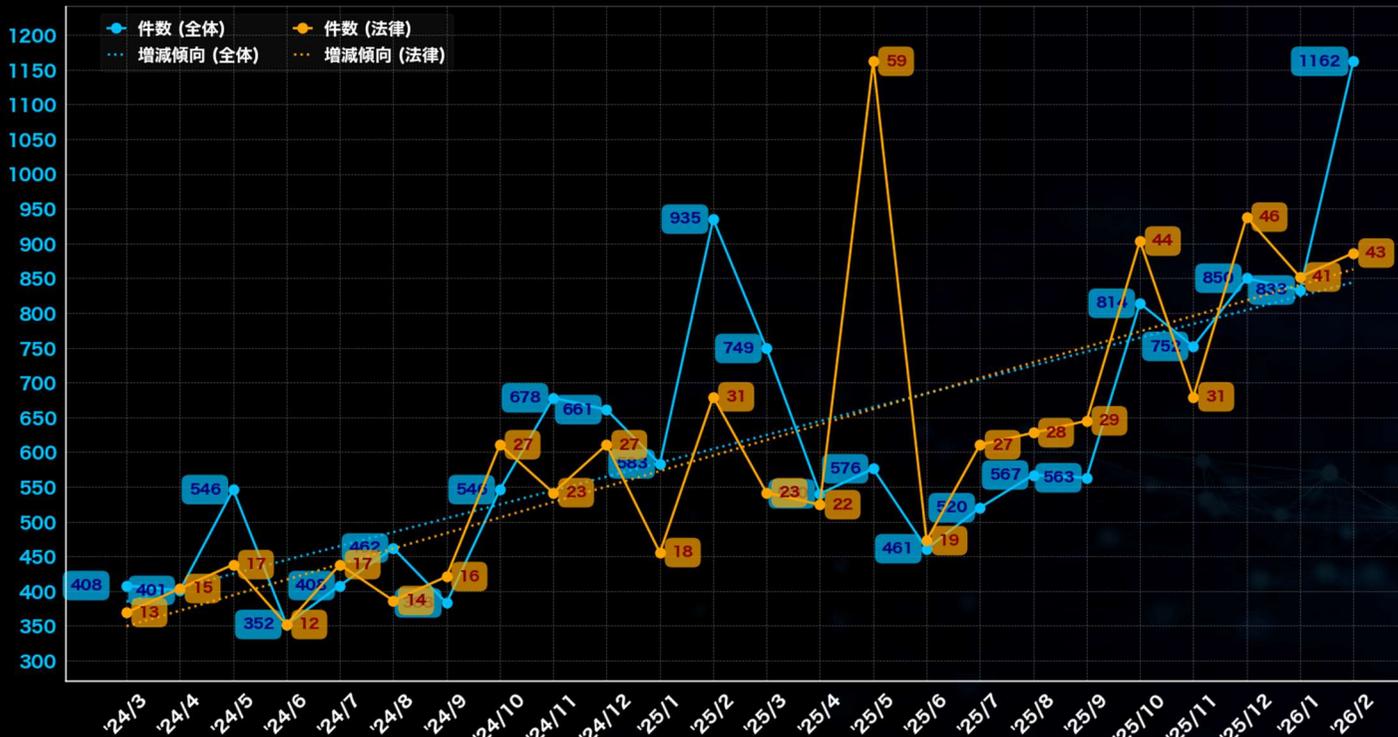
# 業種に関する分析 (全世界)

## (過去2年間 / 2024年3月～2026年2月)

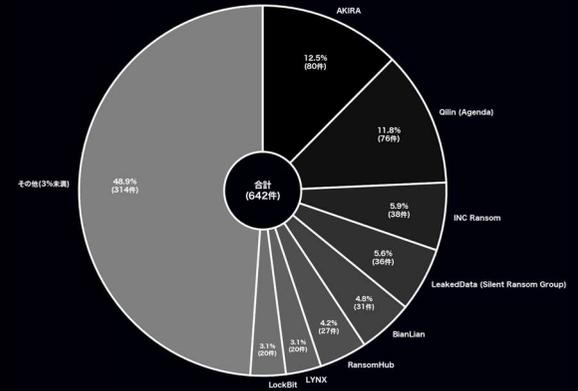


### 法律

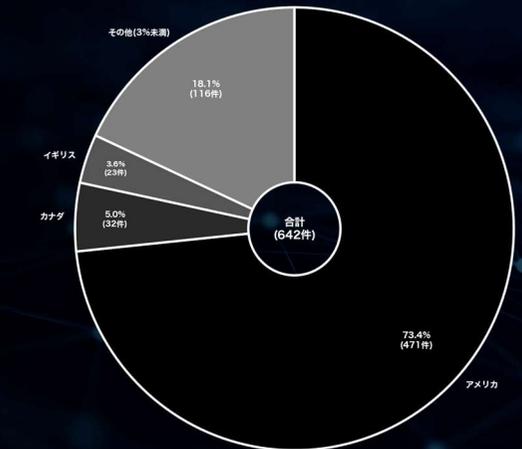
「法律」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年5月で、59件の掲載があった。一方、最も少なかった月は2024年6月で、12件であった。被害組織の所在国の割合では、アメリカが約73%と最も多く、次いでカナダとイギリスがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも87のグループが関与しており、特に「AKIRA」が80件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「INC Ransom」がそれぞれ76件と38件の掲載を行っている。法律関連は2023年末以降、減少傾向が見られたが、2024年9月から10月、2025年4月から5月のように突発的に大きく件数を伸ばす時期があることを確認している。過去2年間においては明確な増加傾向にある。



### ▼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

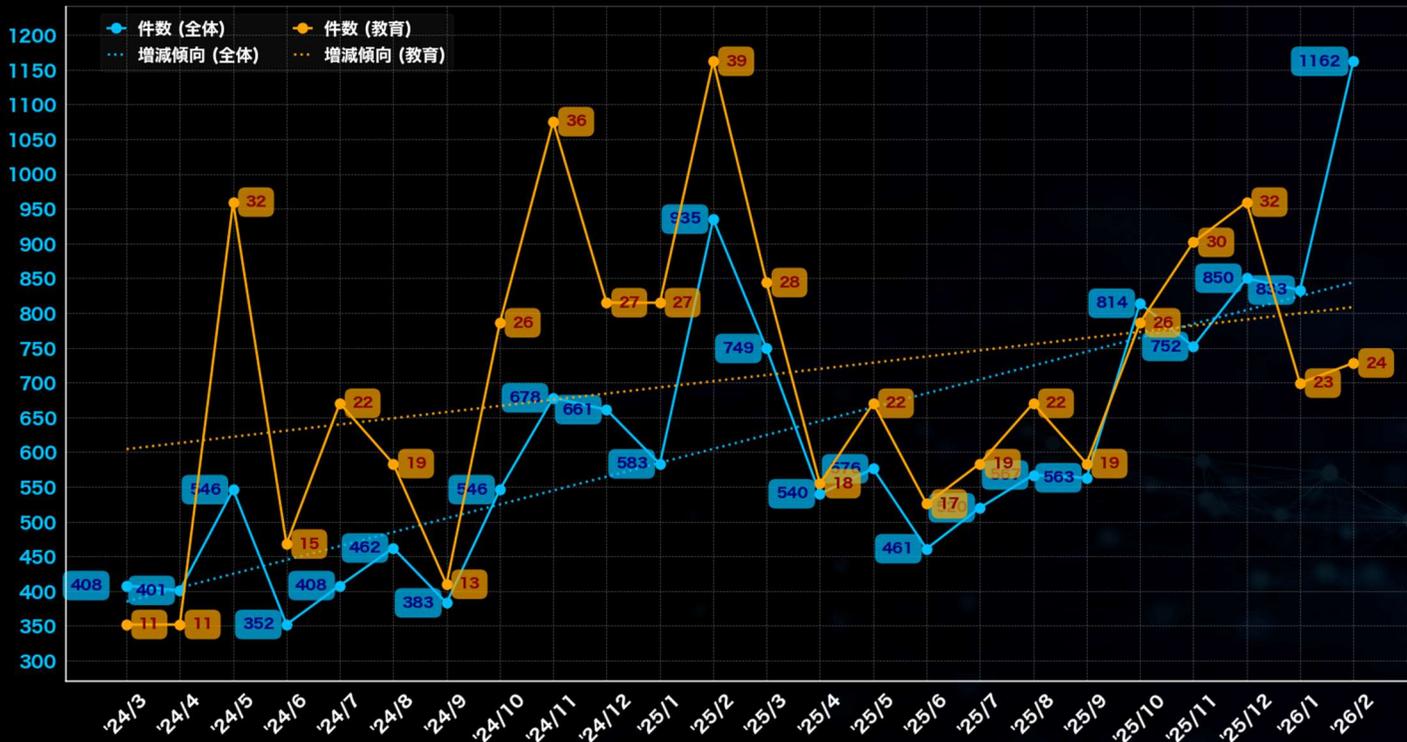


# 業種に関する分析 (全世界)

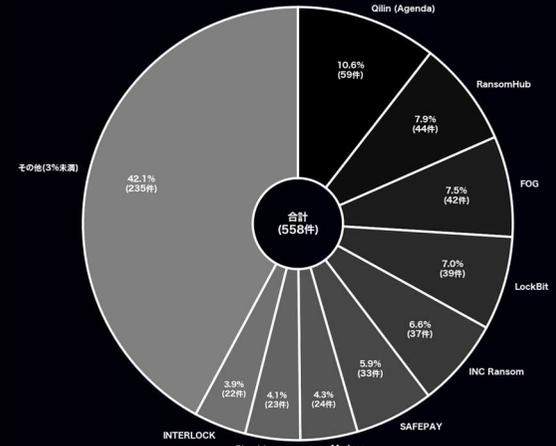
## (過去2年間 / 2024年3月 ~ 2026年2月)

### 教育

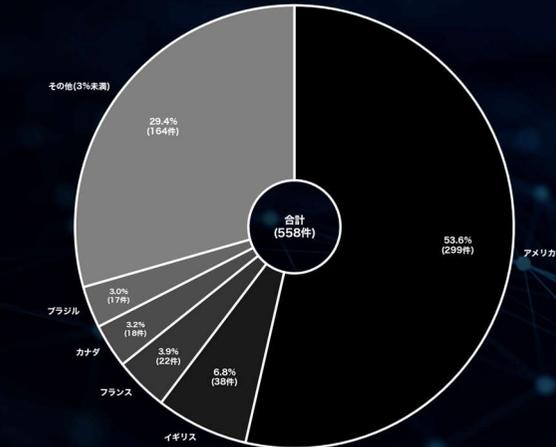
「教育」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、39件の掲載があった。一方、最も少なかった月は2024年3月と4月で、11件であった。被害組織の所在国の割合では、アメリカが約54%と最も多く、次いでイギリスとフランスがそれぞれ約7%と約4%である。攻撃グループについては、少なくとも88のグループが関与しており、特に「Qilin (Agenda)」が59件のリークサイト掲載を実施している。次いで「RansomHub」と「FOG」がそれぞれ44件と42件の掲載を行っている。過去2年間の推移は緩やかな増加傾向となっている。



▼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)

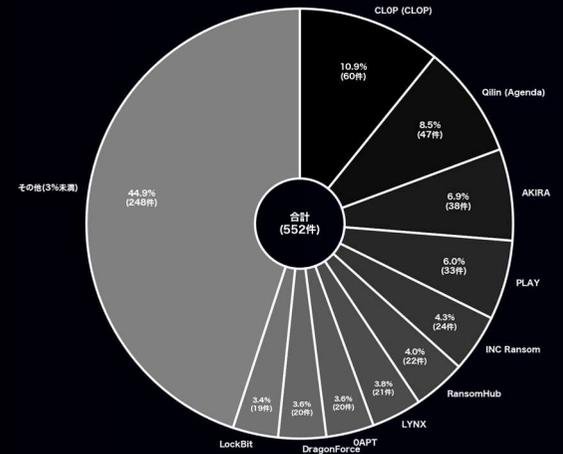
## (過去2年間 / 2024年3月 ~ 2026年2月)

### 運輸

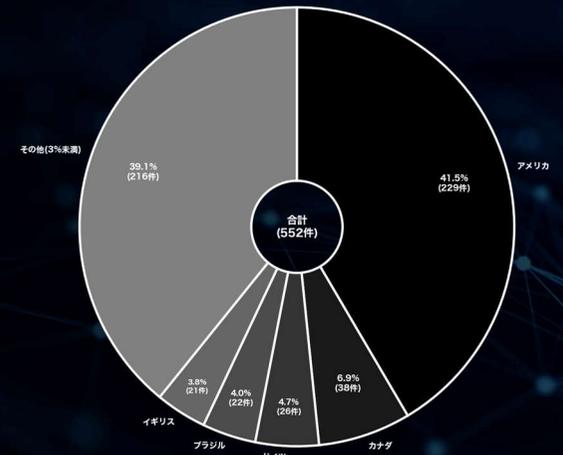
「運輸」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、67件の掲載があった。一方、最も少なかった月は2025年7月で、9件であった。被害組織の所在国の割合では、アメリカが約42%と最も多く、次いでカナダとドイツがそれぞれ約7%と約5%である。攻撃グループについては、少なくとも92のグループが関与しており、特に「CLOP (CLOP)」が60件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「AKIRA」がそれぞれ47件と38件の掲載を行っている。運輸関係は全体件数に対する割合こそ低く、過去2年間では著しく被害が減少するケースもある一方で、緩やかな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

# 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。

- ランサムウェア／攻撃グループの変遷と繋がり (MBSD RANSOMWARE MAP) :

<https://www.mbsd.jp/research/20230201/whitepaper/>

- CIGランサム統計だより :

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

- 技術ブログ :

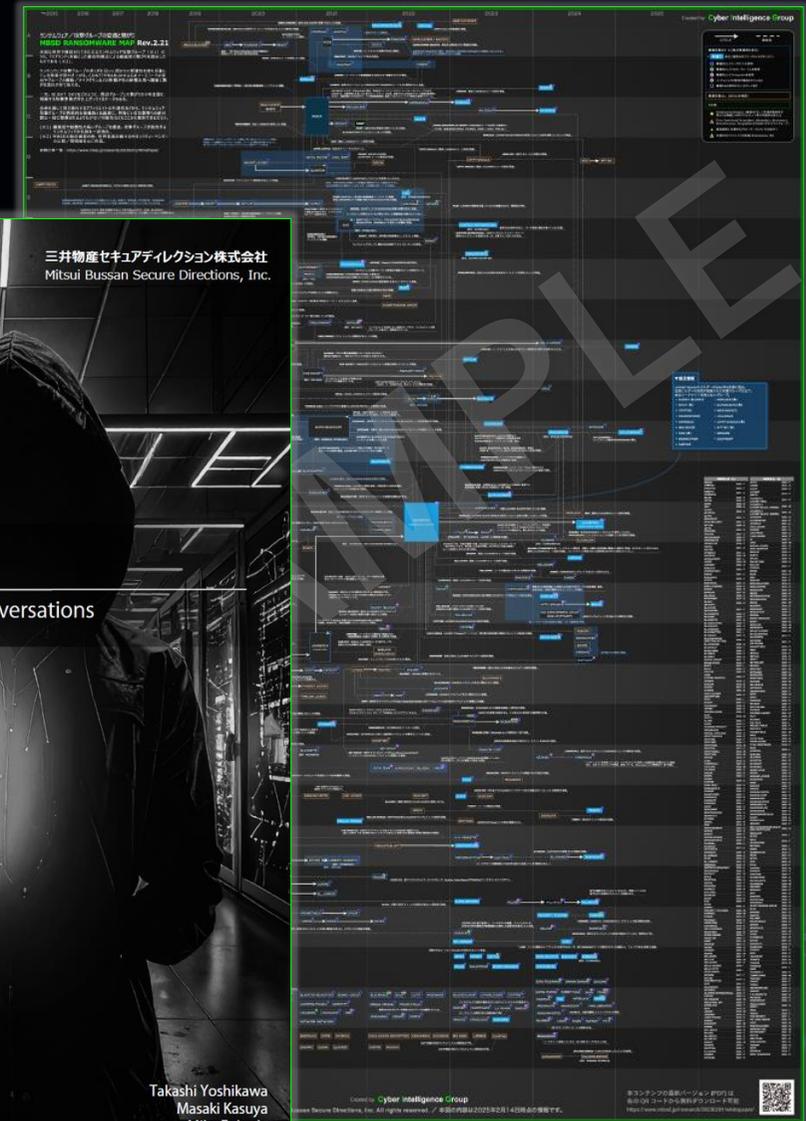
<https://www.mbsd.jp/research/cig/>

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

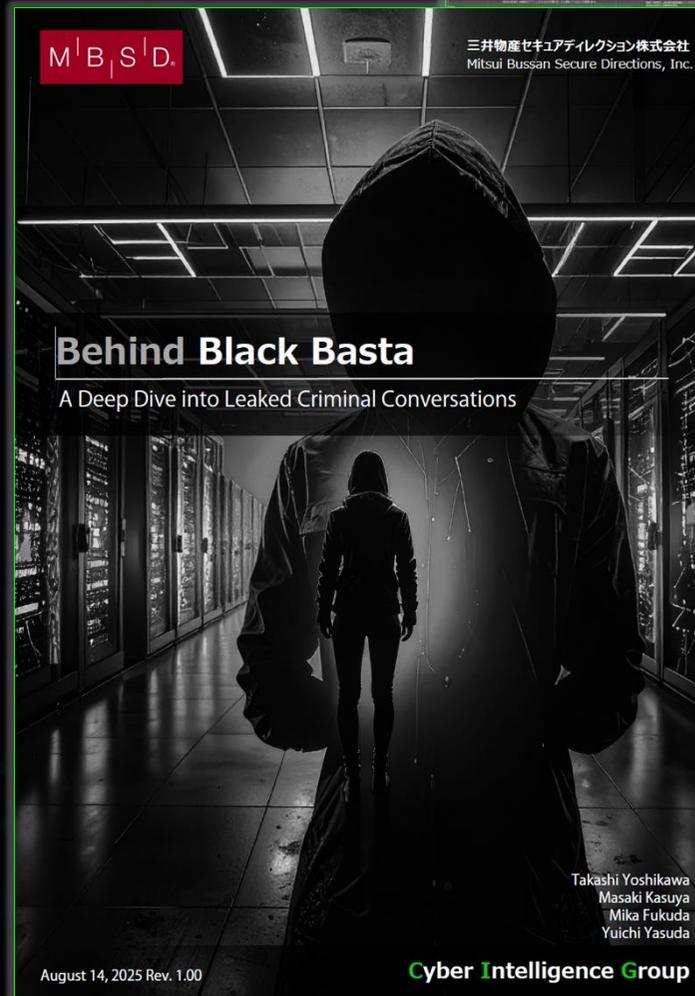
- 分析レポート :

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

MBSD RANSOMWARE MAP (Rev.2)



Black Basta 内部チャット分析レポート



# 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