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2月号 Rev 1.00
(2026年1月分)

2026
1

Cyber Intelligence Group

目次

総括と監視対象（レポート① ~ ④）

グローバル統計（レポート⑤ ~ ⑰）

日本関連組織を対象とした統計（レポート⑱ ~ ㉓）

中小企業における被害分析（レポート㉔ ~ ㉗）

多重被害に関する分析（レポート㉘ ~ ㉙）

業種に関する分析（レポート㉚）

その他

総括と監視対象

2026

1

今月のハイライト

● 新興グループ 0APT の出現と掲載データの信憑性

2026年1月下旬、新興ランサムウェア攻撃グループ「0APT」が出現し、わずか数日で71件をリークサイトに掲載した。1月の掲載数は Qilin (Agenda)、CL0P (CLOP)、AKIRA に次ぐ件数となり、2月は16日時点で既に380件を超えている。これは、Qilin などの主要グループと比較しても突出した水準と言える。2月の掲載情報には日本組織19件に対する攻撃の主張も含まれ、一見すると勢いのある攻撃グループの台頭のように見えるが、実態としては疑わしい状況が複数観測されている。

0APT リークサイトについて

・提示されたデータリンクが機能しない
・被害組織ごとのページが削除される
など不自然な挙動

0APT と主要グループの掲載数比較

主要グループの掲載数

グループ名	単月最大（※）
Qilin (Agenda)	205
AKIRA	99
CL0P (CLOP)	97
Sinobi	74
INC Ransom	55

※単月最大：過去半年のうち、最大だった月の掲載数

0APTの掲載数

382件 (2月1日～2月16日　※速報値)

2月：約半月で、Qilin の単月最大件数（205件）を大きく上回る件数

71件 (1月28日～1月31日)

1月：出現からわずか数日で主要グループの中でも上位に入る件数

0APT の信憑性が疑われる理由

- リークサイトには特定困難な被害組織が多数掲載されており、日本組織についても2月以降に掲載された19件中4件は特定できない。
- 窃取の根拠として提示されたデータリンクが機能しない事例や、被害組織ごとのページが削除されるなど、不自然な挙動が見られる。
- 主要グループと比較しても突出した掲載数。新興グループとしては異例であり、水増しの可能性がある。

その他の留意事項※1, ※2, ※3

0APT については掲載情報の水増しの疑いから、実態を誇張した掲載によって RaaSプログラムへの参加者を募り、参加費を詐取する目的のグループという見方もある。一方で、検体にはファイル暗号化および Torサイトへの誘導機能があることから、実際の攻撃能力を有している点には留意が必要である。

※1：https://theravenfile.com/2026/02/14/0apt-ransomware-the-real-fake/
※2：https://socradar.io/blog/dark-web-profile-0apt-ransomware/
※3：https://www.s-rminform.com/latest-thinking/impostor-ransomware-actor-0apt-triggers-panic

侵害の有無が不明な場合でも、リークサイトへの掲載自体が風評被害や対応コストの発生要因となりうる。一方的に攻撃を主張されるだけで事案対応を迫られ、事実関係が不確定なまま意思決定を強いられる場面も想定される。インシデント発生後に対応策を検討するのではなく、平時から対応方針を整備したうえで、内部ログなどの証跡に基づく迅速な検証体制を構築しておくことが望ましい。

※ 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

ランサムウェア関連記事 | 今月のピックアップ （期間：2026年1月13日～2026年2月12日）

【ウクライナ国家警察は、ランサム攻撃などに関与した国際ハッカー組織の構成員を摘発し首謀者を特定したと正式発表】（ウクライナ国家警察サイバー警察局：2026/1/15）
ウクライナとドイツの法執行機関は、ハッカーグループのメンバーを摘発し捜索を行った。世界中の企業に数億ユーロの損害を与えてきたこのグループのリーダーは、国際指名手配リストに掲載されている。
https://cyberpolice.gov.ua/news/naczpolicziya-vykryla-chleniv-mizhnarodnogo-xakerskogo-ugrupovannya-ta-identyfikuvala-jogo-organizatora-6407/

【INCランサムウェアの運用セキュリティの失敗により、12社のデータ復旧が可能になった】（Bleeping Computer：2026/1/22）
INCランサムウェアグループのミスにより、セキュリティ企業 Cyber Centaurs が暗号化されたデータを復元。米国12組織の窃取データが身代金を払わずに回収された。
https://www.bleepingcomputer.com/news/security/inc-ransomware-opsec-fail-allowed-data-recovery-for-12-us-orgs/

【FBI、ランサムウェア集団が利用していたサイバー犯罪フォーラム「RAMP」を押収】（Bleeping Computer：2026/1/28）
FBIは、悪名高いRAMPサイバー犯罪フォーラムを押収した。同フォーラムは、マルウェアやハッキングサービスの宣伝に使われ、ランサムウェア活動を公然と宣伝していた数少ない残存フォーラムの一つであった。
https://www.bleepingcomputer.com/news/security/fbi-seizes-ramp-cybercrime-forum-used-by-ransomware-gangs/

【情報セキュリティ10大脅威 2026】（IPA（情報処理推進機構）：2026/1/29）
「情報セキュリティ10大脅威 2026」は、2025年に社会的影響が大きかった情報セキュリティ事故や攻撃をもとに、IPAが候補を選定、約250名の「10大脅威選考会」が審議・投票して決定したもの。
https://www.ipa.go.jp/security/10threats/10threats2026.html

【公安・国土安全保障局がランサムウェア攻撃対策のベストプラクティスを発表】（FCC：2026/1/29）
FCC公共安全局が発表したパブリックノーティス DA 26-96 は、通信事業者に対し、ランサムウェア攻撃からの防御のためのサイバーセキュリティのベストプラクティスを実施するよう促している。
https://www.fcc.gov/document/pshsb-highlights-ransomware-risks-and-best-practices
DA 26-96 PDF → https://docs.fcc.gov/public/attachments/DA-26-96A1.pdf

【認証なしでインターネットに公開されたMongoDBが標的となり、データベースが削除されて身代金要求メッセージが残された】（Cyber Security News：2026/2/2）
攻撃者はインターネット上でアクセス可能な、認証なしで公開されている MongoDB をスキャンし、保存されているデータを削除し、ビットコインでの支払いを要求する身代金要求メモを挿入している。
https://cybersecuritynews.com/mongodb-instances-hacked/

【Nitrogenランサムウェアは非常に脆弱で、犯罪者でさえファイルのロックを解除できない】（The Register：2026/2/4）
Nitrogenランサムウェアの ESXi 向け亜種は、内部にプログラミングエラーがあり、公開鍵が破損してしまう。そのため、被害者が身代金を払って復号ツールを入手しても、ファイルの復号は不可能である。
https://www.theregister.com/2026/02/04/nitrogen_ransomware_broken_decryptor/

【CISA、VMware ESXiのゼロデイ脆弱性がランサムウェア攻撃に悪用される可能性を警告】（Cyber Security News：2026/2/5）
CISAは、高深刻度の VMware ESXi サンドボックスのエスケープに関する重大な脆弱性 CVE-2025-22225（CVSSスコア8.2）がランサムウェアグループにより悪用されていると確認した。
https://cybersecuritynews.com/vmware-esxi-0-day-ransomware-attack/

【Reynoldsランサムウェアは、暗号化前にBYOVDを使用してセキュリティを無効化する】（Security Affairs：2026/2/11）
研究者らは、システムを暗号化する前にセキュリティツールを無効にして検出を回避するために、脆弱なドライバー持ち込み（BYOVD）技術を実装する、Reynolds という新しいランサムウェアを発見した。
https://securityaffairs.com/187869/security/reynolds-ransomware-uses-byovd-to-disable-security-before-encryption.html

【ランサムウェア集団が企業の「中の人」を狙う時代：Qilinの脅威と対策】（Zenn：2026/2/12）
ランサムウェアグループが技術的な侵入よりも、企業の内部者協力の獲得に重心を移しつつあり、Qilin をはじめとする RaaS が“社員の買収”をビジネスとして本格的に展開している現状を解説。
https://zenn.dev/headwaters/articles/b12aefc5ce95e9

※ 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（※1）：300（※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：57

※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

● 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）

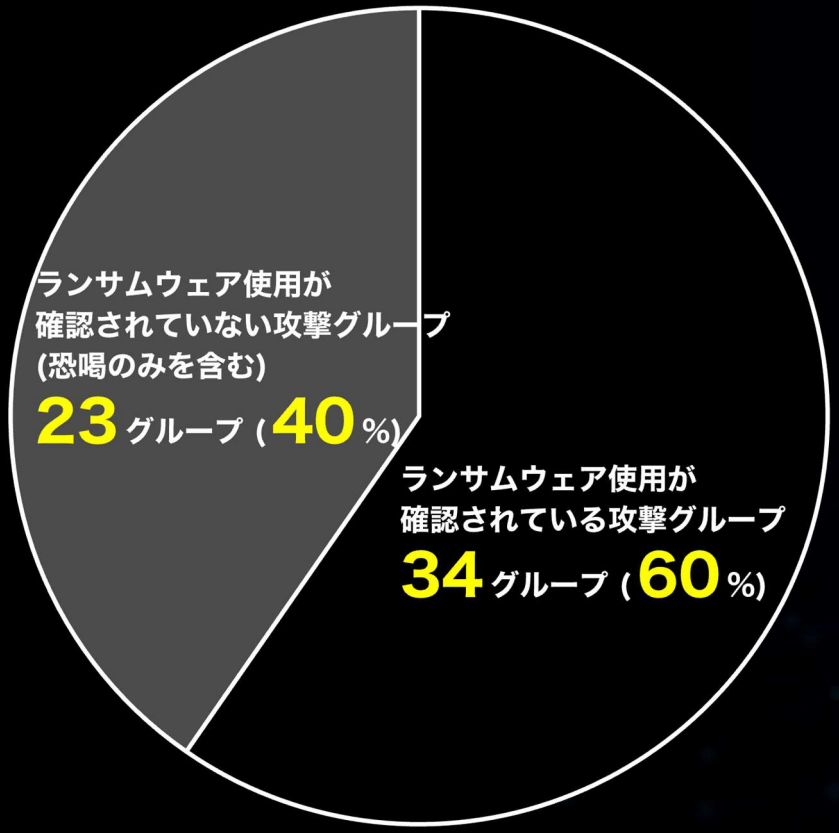
- ● 0APT
- 0mega (Omega)
- 8BASE
- Abyss
- AKIRA
- AKO
- Alpha (MYDATA)
- AlphV (BlackCat)
- Anubis
- Apos Security
- APT73 (Eraleig)
- ARACHNA
- ARCUS MEDIA
- Argonauts
- Arkana
- ArvinClub
- Astro (Astra)
- AtomSilo
- Avaddon
- AvosLocker
- ● AWARE
- Axxes
- AzzaSec
- Babuk
- Babuk (2025)
- BASHE
- BEAST
- Benzona
- BERT
- BianLian
- BL0ODY (BLOODY)
- Bl4ckt0r (BlackTor)
- Black Basta
- BlackByte
- BlackDolphin
- BlackLock
- BlackMatter
- Black Nevas
- Blackout
- BLACKSHRANTAC
- BlackSuit
- BLUEBOX
- BLUESKY
- BQTLOCK
- Brain Cipher
- ● BRAVOX
- Brotherhood
- BULLY
- Business Data Leaks
- CACTUS
- Cephalus
- CHAOS (2025)
- CHEERS
- ChileLocker (Arcrypter)
- CHORT
- Cicada3301
- CiphBit
- CipherLocker
- CL0P (CLOP)
- Cloak
- COINBASE CARTEL
- Conti
- Cooming Project
- Crazy Hunter Team
- CROSSLOCK
- CRY0
- CryptBB
- CRYPTNET
- CRYPTO24
- CryptOn
- Cuba
- Cyclops
- D4RK4RMY
- DAGON
- DAIXIN
- dAn0n (danon)
- Dark Angels
- DARKBIT
- DARKPOWER
- DarkRace
- DarkRypt
- Dark Shinigamis
- Darkside
- Dark Vault
- DataCarry
- ● Datakeeper
- Desolator
- 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
- 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
- ICEFIRE
- IMN Crew
- INC Ransom
- Insane
- INTERLOCK
- J GROUP
- KAIROS
- Karakurt
- Karma
- Kawa4096
- Kazu
- KILLSEC
- Knight
- Kraken (HelloKitty)
- Kryptos
- Kyber
- LAMBDA
- La Piovra
- LAPSUS$
- LAPSUS$ Group
- LeakedData (Silent Ransom Group)
- LEAKNET
- LILITH
- Linkc
- LockBit
- Lorenz
- LostTrust
- LunaLock
- LV
- LYNX
- MADCAT
- MAD LIBERATOR
- MALAS
- MalekTeam
- Mallox
- Mamona RIP
- MBC
- Medusa
- MEOW
- Metaencryptor
- Midas
- MIGA
- Mindware
- Minteye
- Mogilevich [fraud]
- MOISHA
- Money Message
- Monti
- Morpheus
- Mount Locker
- MS13-089
- N3tw0rm (NetWorm)
- N4UGHTYSEC (NAUGHTYSEC)
- NASIR SECUTRIY
- Nefilim
- 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.bin
- Payouts King
- PEAR
- PLAY
- PLAYBOY
- 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)
- Rhysida
- Risen
- ROOK
- root
- Royal
- Rransom
- RunSomeWares
- Rusty Locker
- Sabbath (54bb47h)
- SAFEPAY
- SARCOMA
- SATAN LOCK
- SATANLOCK V2
- Scattered LAPSUS$ Hunters
- Secp0
- Securotrop
- SenSayQ
- shaoleaks
- ● SHINYHUNTERS
- Sicarii
- SIEGEDSEC
- Silent
- Sinobi
- SKIRA TEAM
- SLUG
- Snatch
- Solidbit
- Space Bears
- Sparta
- Spook
- STORMOUS
- Sugar
- Suncrypt
- SynACK
- TeamXXX
- TENGU
- Termite
- The Gentlemen
- ● THE GREEN BLOOD GROUP
- ThreeAM (3AM)
- TridentLocker
- TRIGONA
- TRINITY
- TRISEC
- Underground
- UnSafe
- Valencia
- VanHelsing
- VanirGroup
- ● Vect
- Vice Society
- V IS VENDETTA
- VSOP
- WALocker
- Warlock
- WEREWOLVES
- Weyhro
- WORLD LEAKS
- x001xs
- XING Team
- 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 1月）

（※当月にリークサイト掲載を確認した攻撃グループ全57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1月に活動中である事が確認された全57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。

※ 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

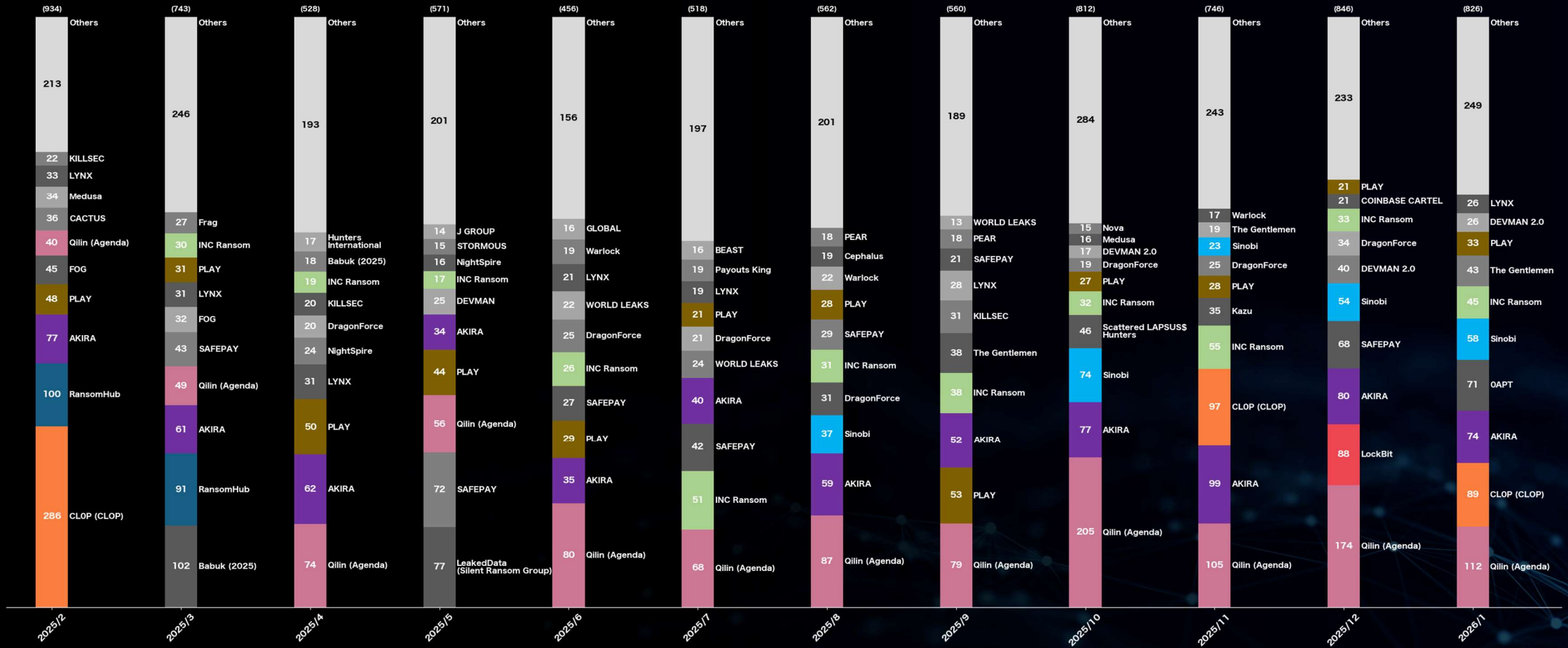
年間 統計
（全世界）

2026

1

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2月～2026年1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

攻撃グループ 月別統計

（全世界）

（過去3ヶ月分）

2026

1

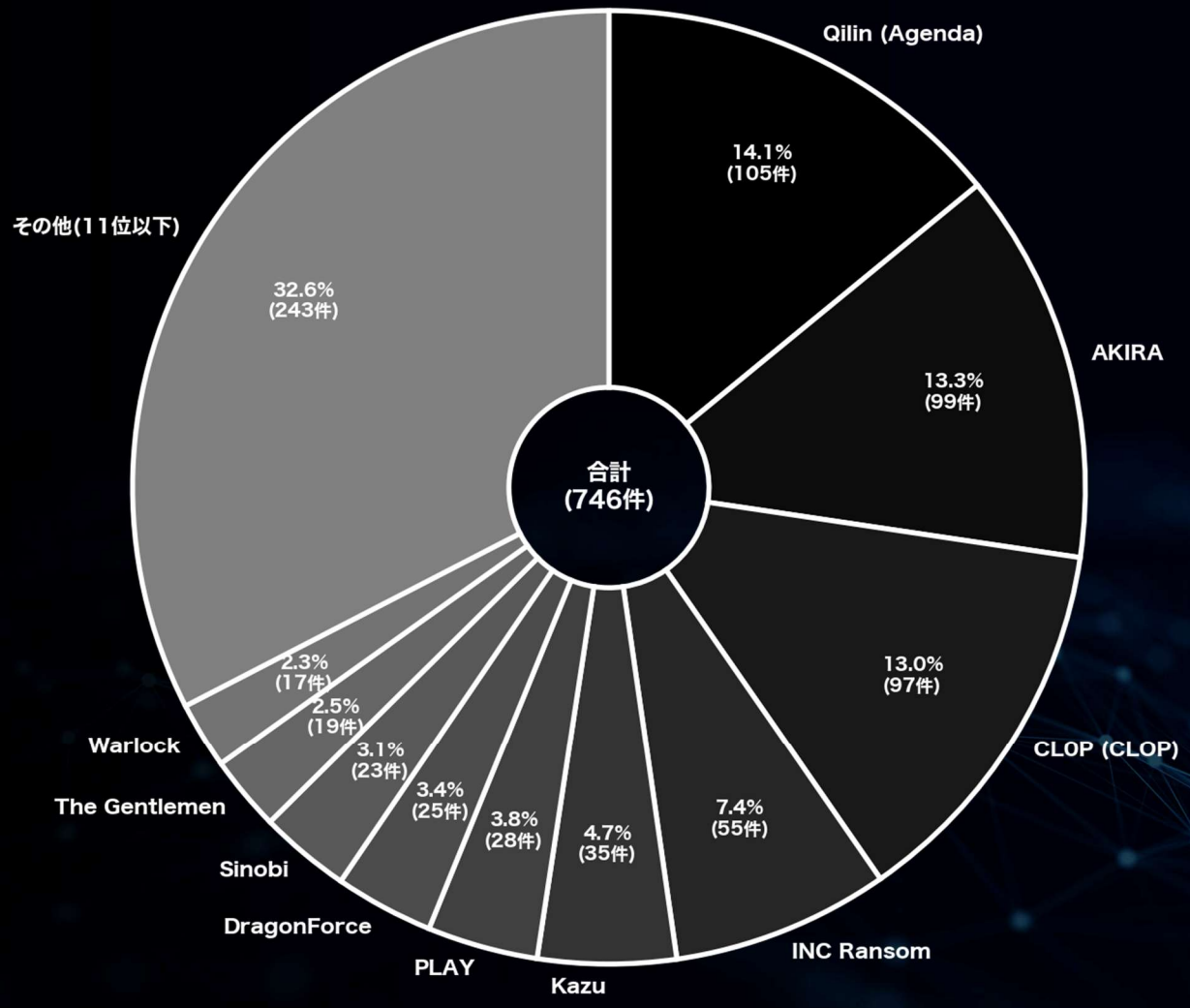
月別内訳 攻撃グループ TOP10（全世界）

（2025年 11 月）

※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)	105	14.1	- 100
AKIRA	99	13.3	+ 22
CL0P (CLOP)	97	13.0	+ 84
INC Ransom	55	7.4	+ 23
Kazu	35	4.7	+ 35
PLAY	28	3.8	+ 1
DragonForce	25	3.4	+ 6
Sinobi	23	3.1	- 51
The Gentlemen	19	2.5	+ 8
Warlock	17	2.3	+ 17

▼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）



※ 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

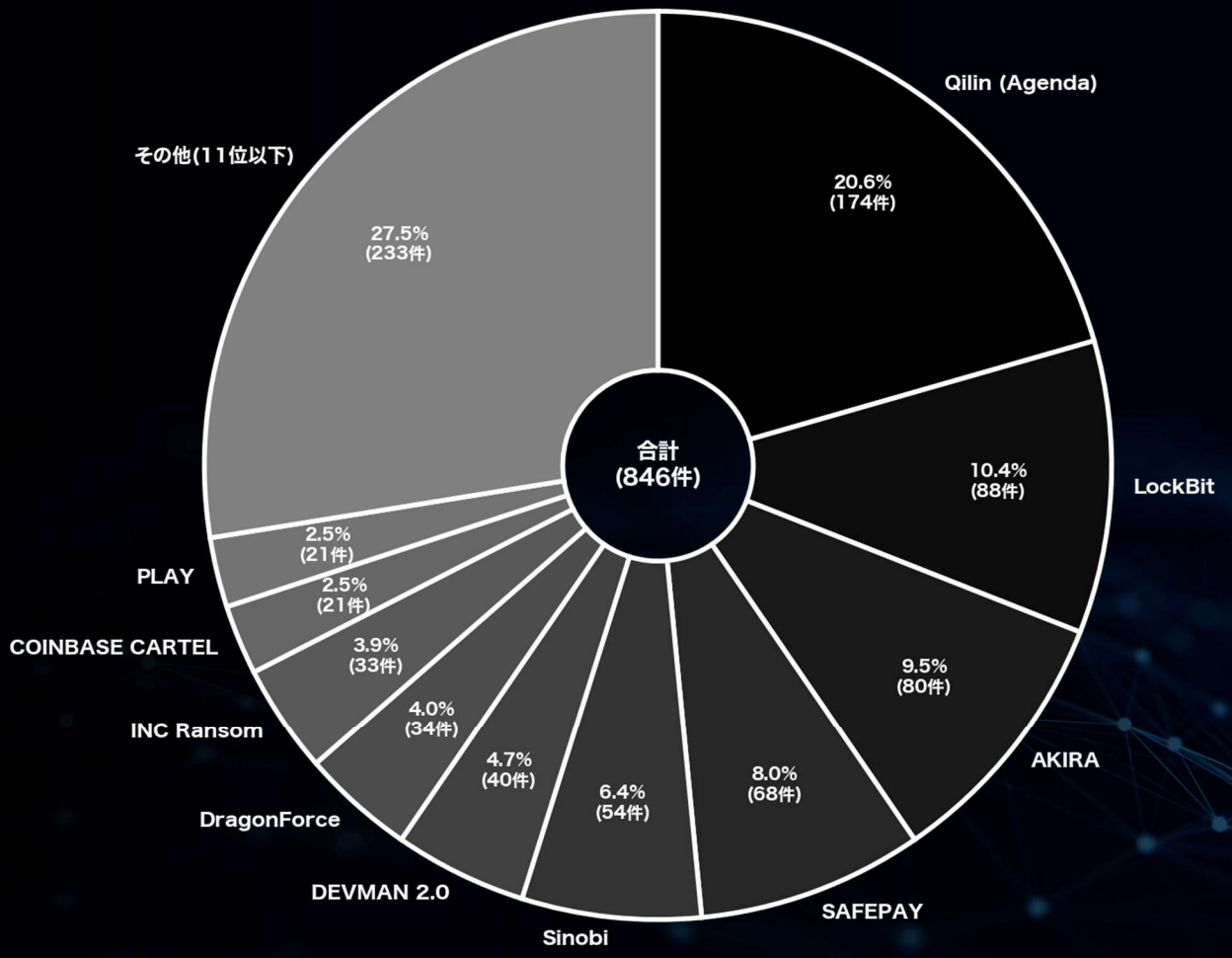
月別内訳 攻撃グループ TOP10（全世界）

（2025年 12 月）

※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

▼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）



※ 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

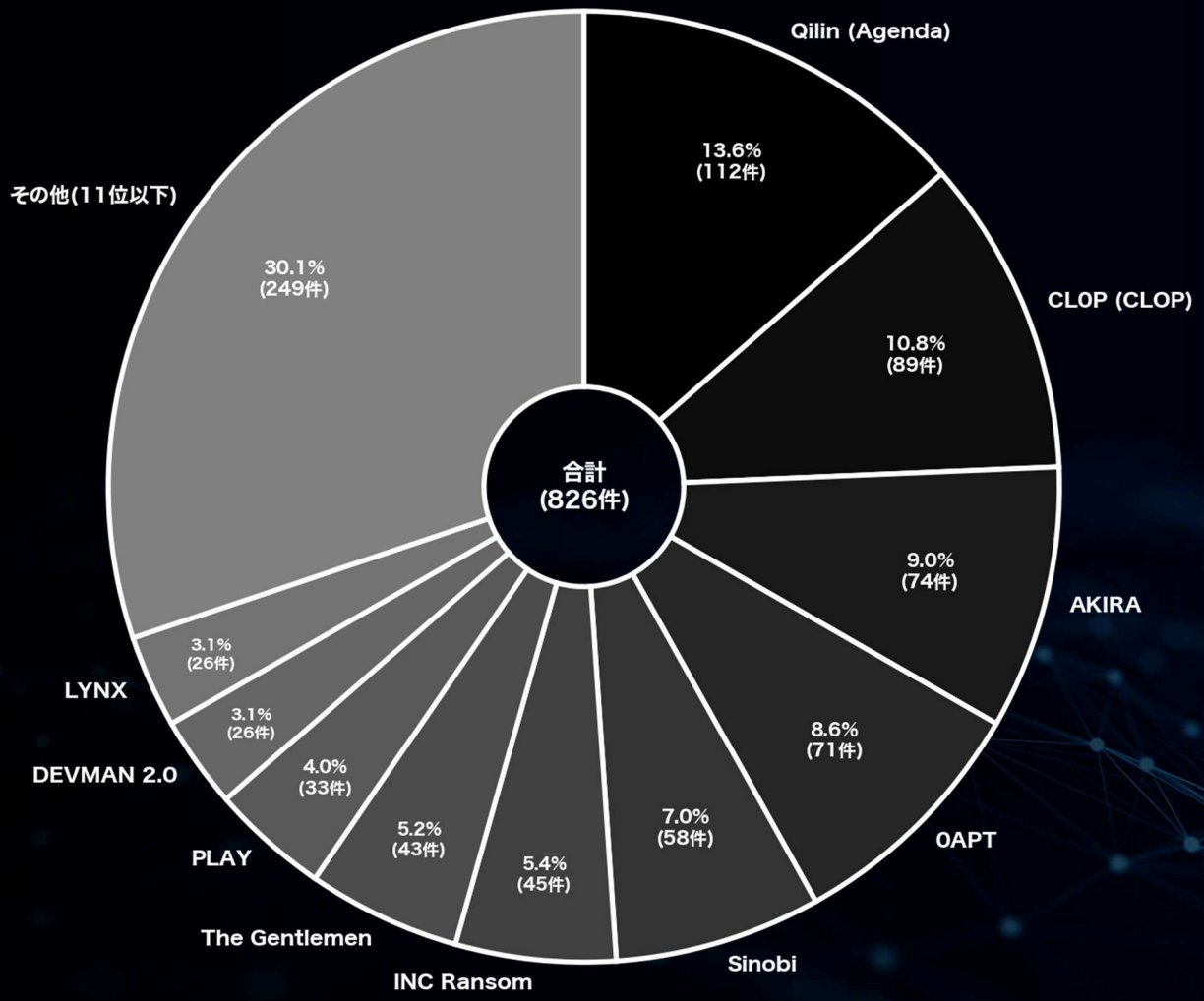
月別内訳 攻撃グループ TOP10（全世界）

（2026年 1 月）

※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
CL0P (CLOP)	89	10.8	+ 88
AKIRA	74	9.0	- 6
0APT	71	8.6	+ 71
Sinobi	58	7.0	+ 4
INC Ransom	45	5.4	+ 12
The Gentlemen	43	5.2	+ 32
PLAY	33	4.0	+ 12
DEVMAN 2.0	26	3.1	- 14
LYNX	26	3.1	+ 12

▼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）



※ 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

1

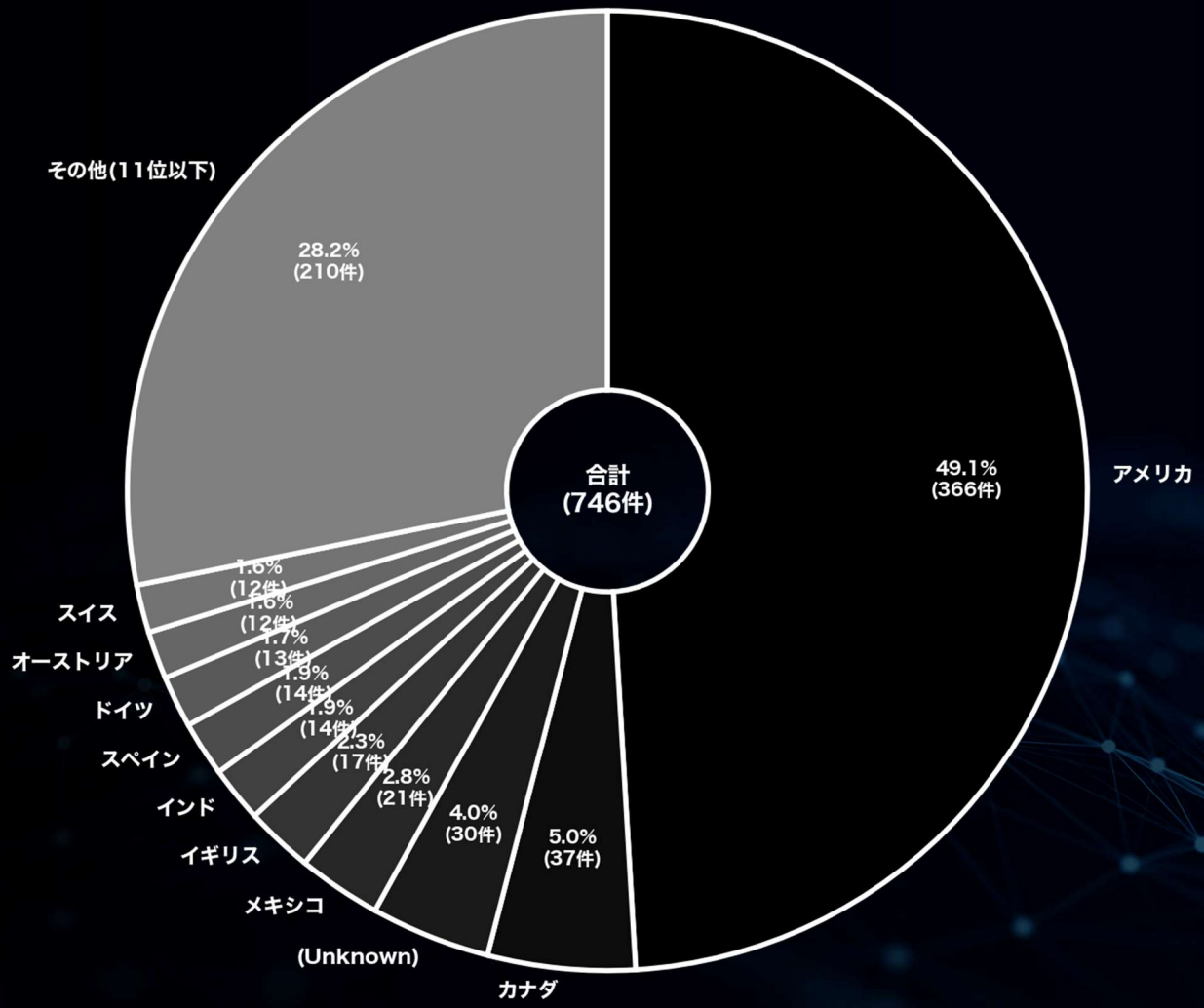
月別内訳 被害国TOP10（全世界）

（2025年 11 月）

※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	366	49.1	- 66
カナダ	37	5.0	- 11
(Unknown)	30	4.0	+ 5
メキシコ	21	2.8	+ 17
イギリス	17	2.3	- 2
インド	14	1.9	+ 7
スペイン	14	1.9	- 4
ドイツ	13	1.7	- 11
オーストリア	12	1.6	+ 9
スイス	12	1.6	+ 7

▼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）



※ 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

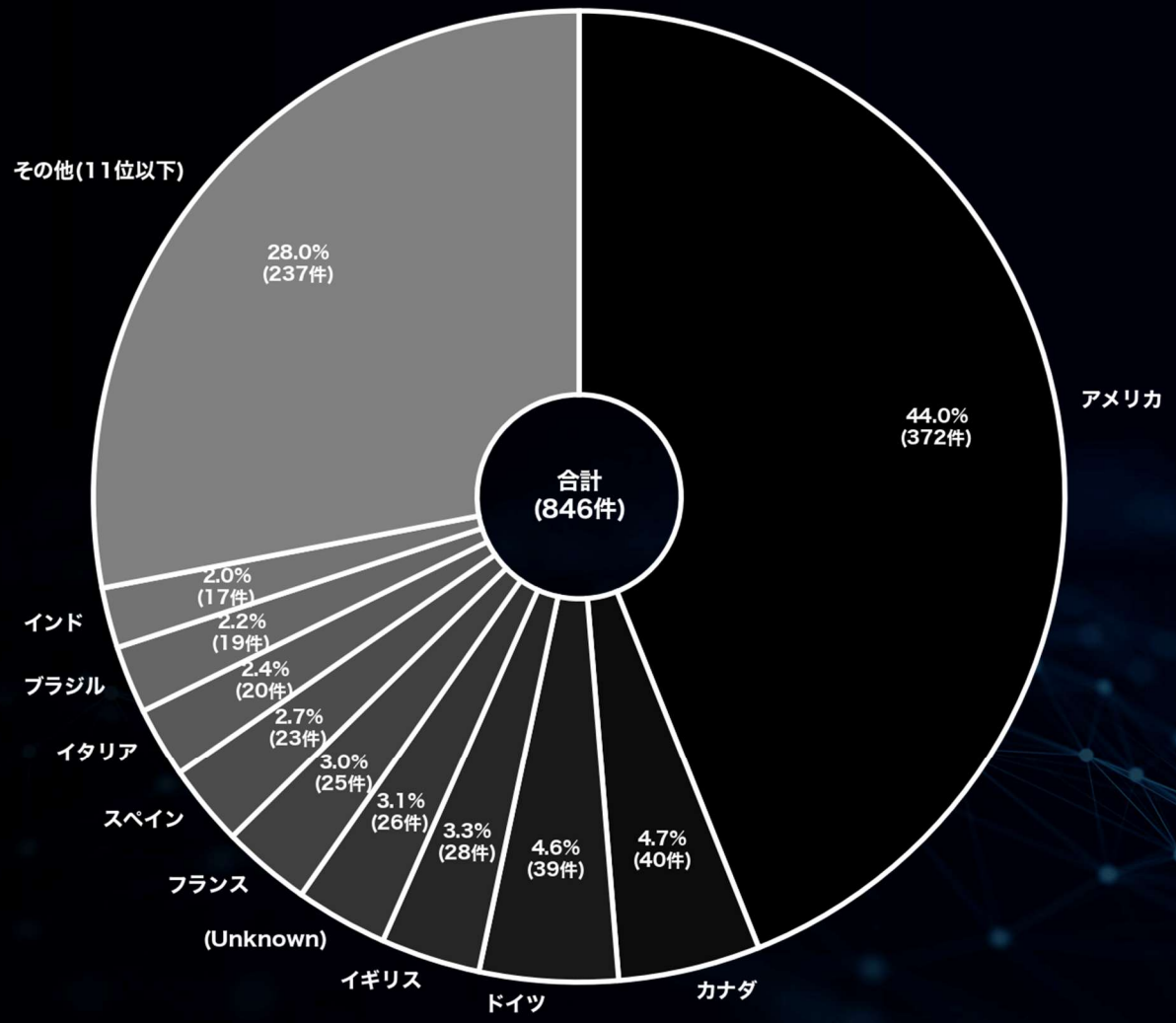
月別内訳 被害国TOP10（全世界）

（2025年 12 月）

※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

▼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）



※ 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

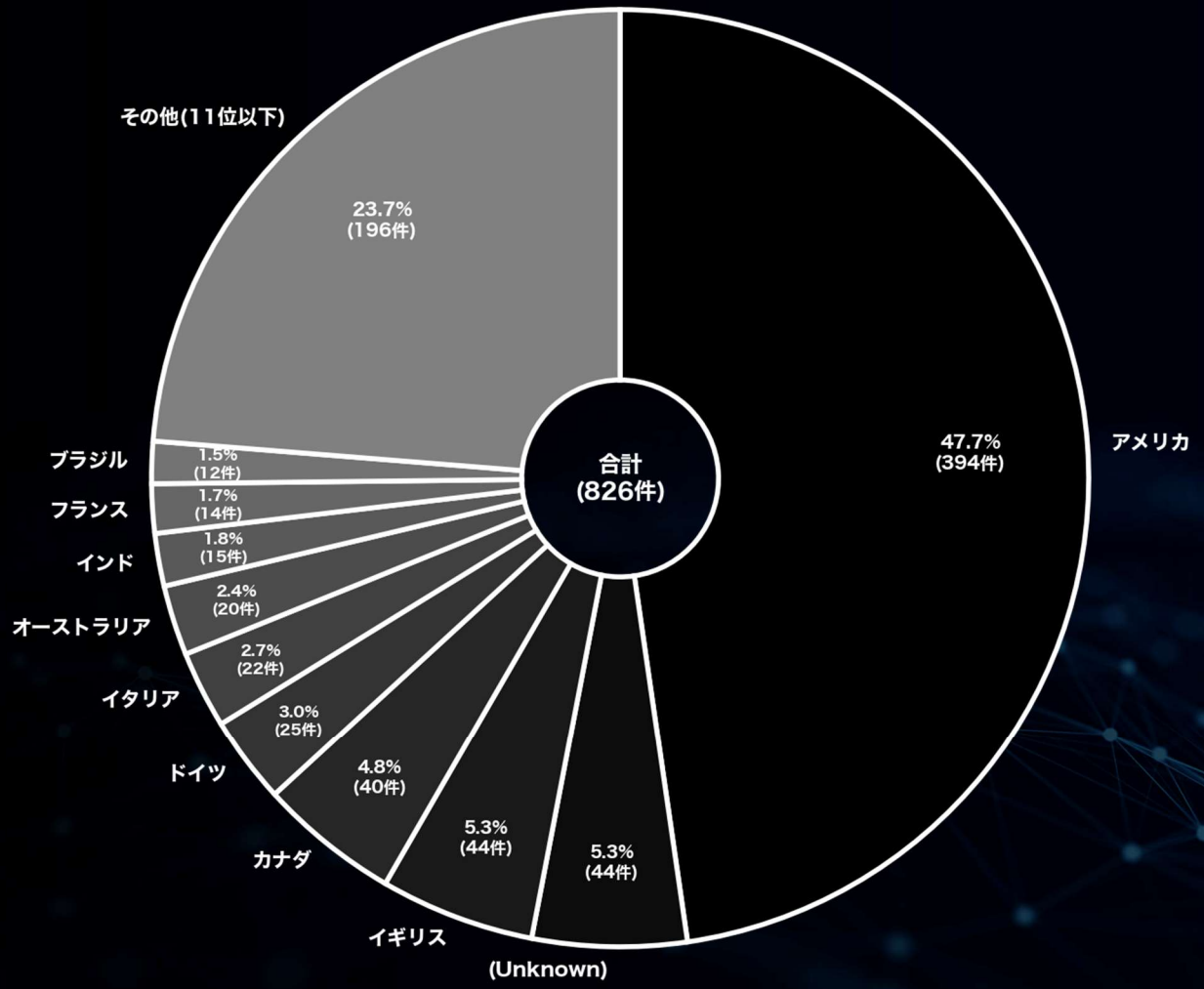
月別内訳 被害国TOP10（全世界）

（2026年 1 月）

※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	47.7	+ 22
(Unknown)	44	5.3	+ 18
イギリス	44	5.3	+ 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

▼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）



※ 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

1

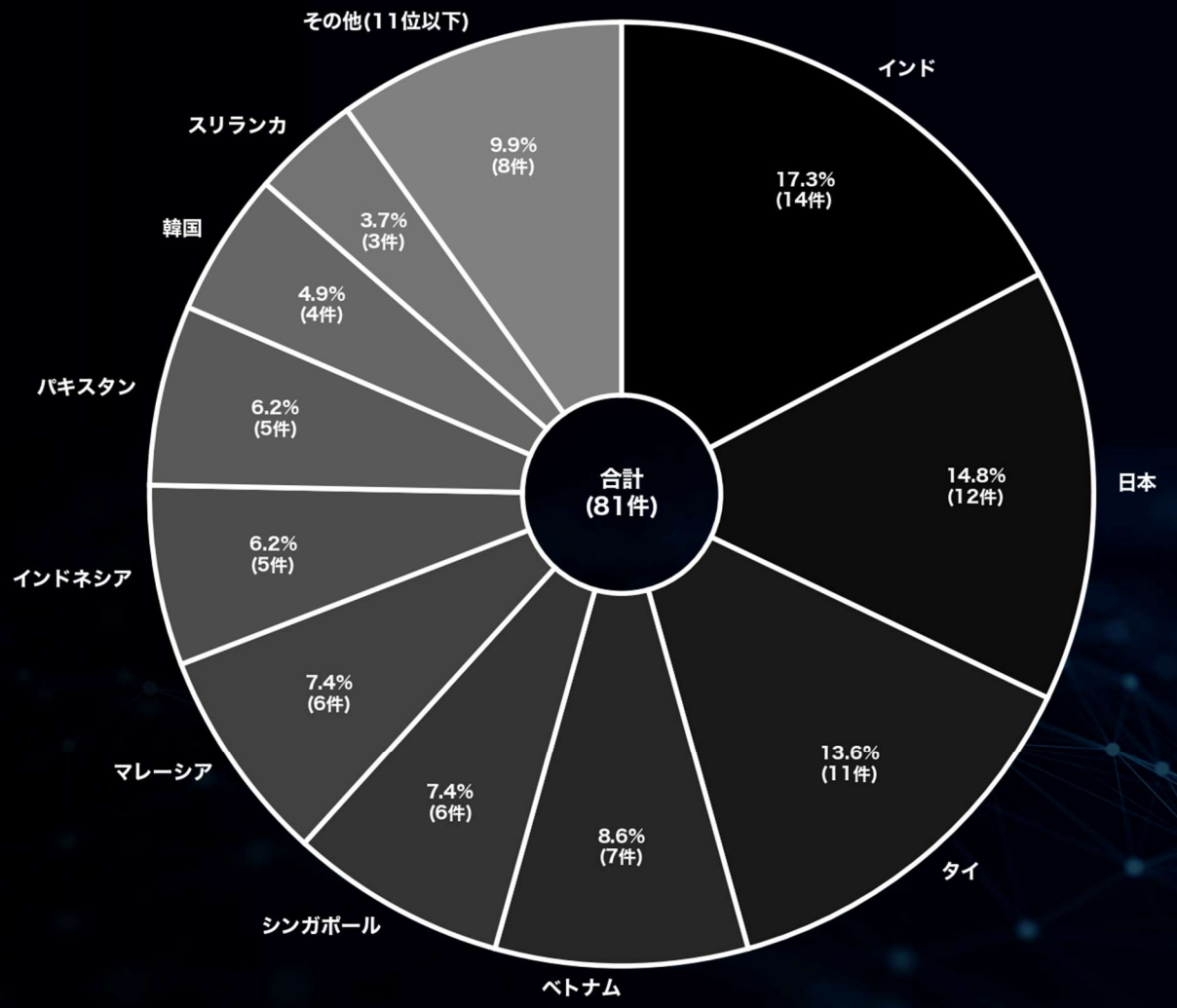
月別内訳 被害国TOP10（アジア）

（2025年 11 月）

※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	14	17.3	+ 7
日本	12	14.8	- 1
タイ	11	13.6	+ 4
ベトナム	7	8.6	+ 3
シンガポール	6	7.4	+ 2
マレーシア	6	7.4	+ 2
インドネシア	5	6.2	+ 1
パキスタン	5	6.2	+ 4
韓国	4	4.9	- 8
スリランカ	3	3.7	+ 3

▼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）



※ 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

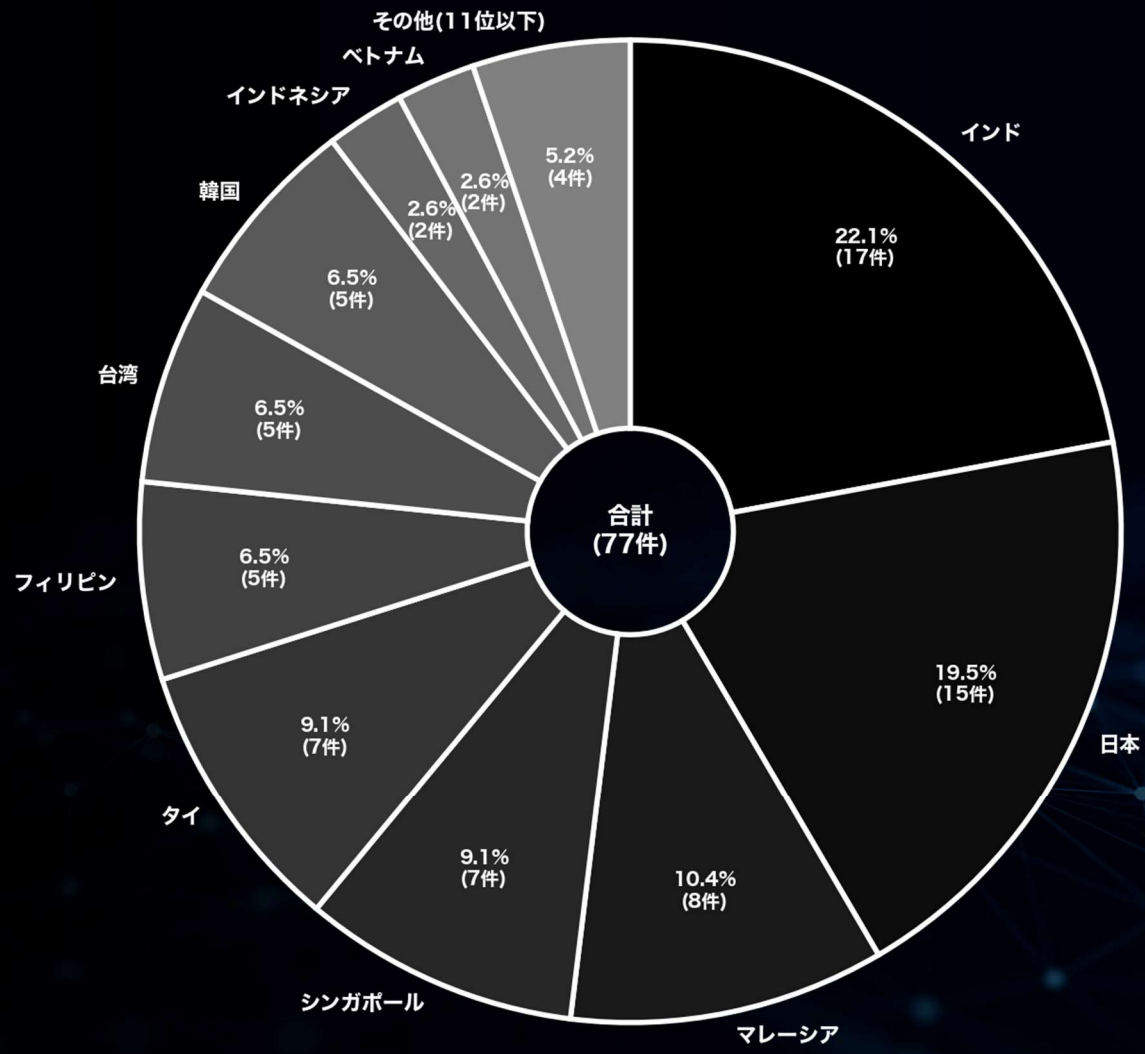
月別内訳 被害国TOP10（アジア）

（2025年 12 月）

※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

▼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）



※ 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

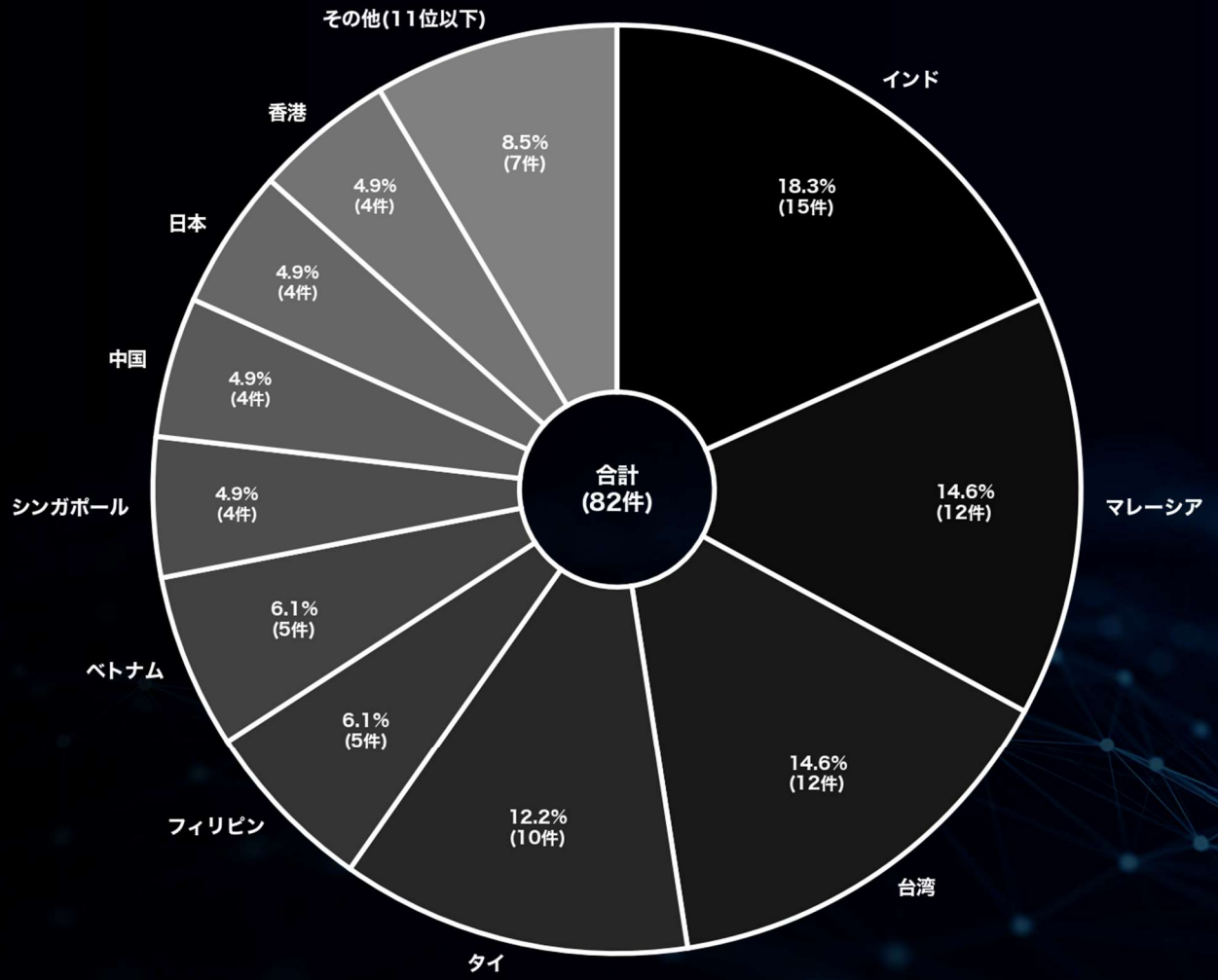
月別内訳 被害国TOP10（アジア）

（2026年 1 月）

※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	18.3	- 2
マレーシア	12	14.6	+ 4
台湾	12	14.6	+ 7
タイ	10	12.2	+ 3
フィリピン	5	6.1	± 0
ベトナム	5	6.1	+ 3
シンガポール	4	4.9	- 3
中国	4	4.9	+ 3
日本	4	4.9	- 11
香港	4	4.9	+ 3

▼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）



※ 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

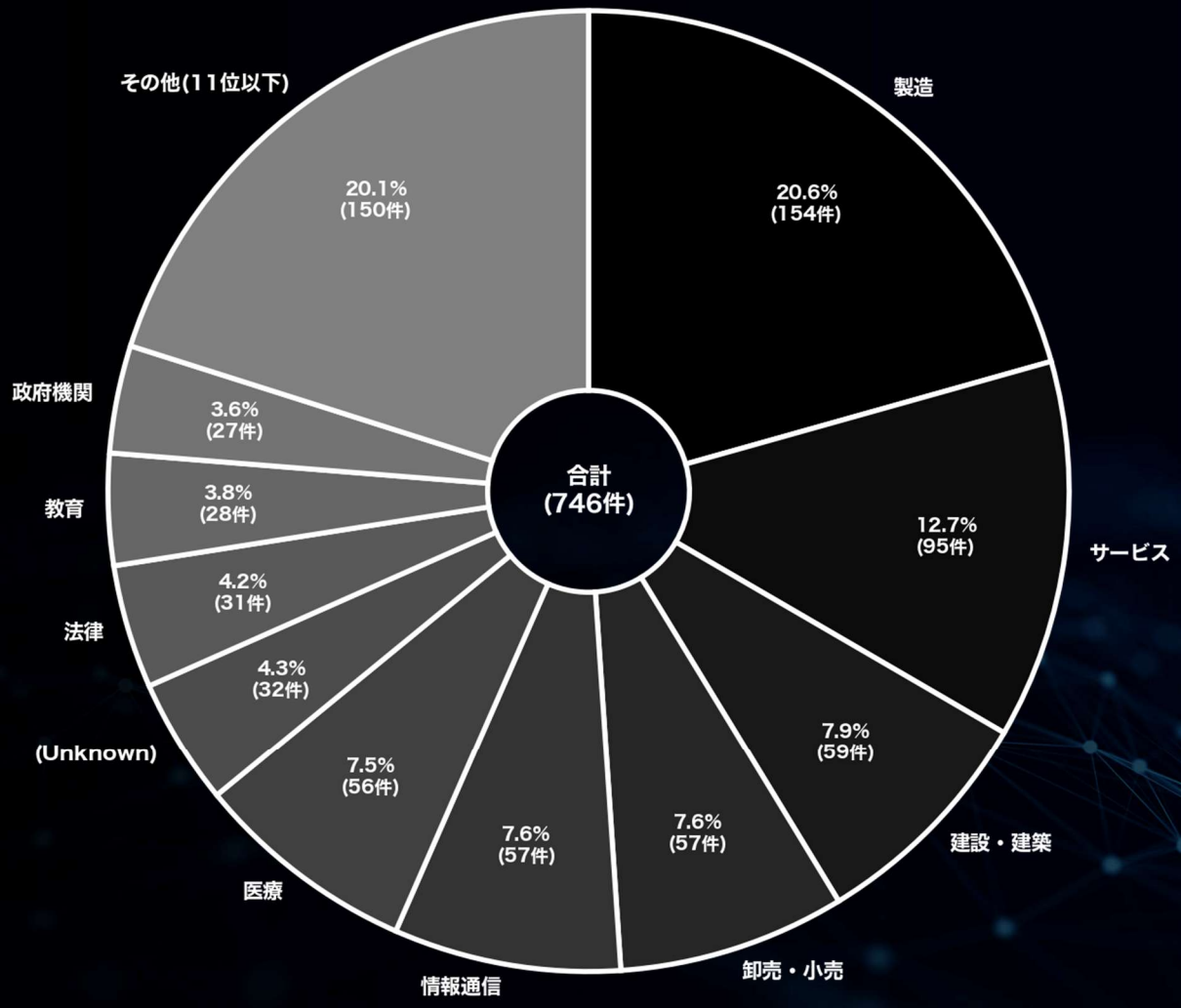
1

月別内訳 業種 TOP10（全世界）
（2025年 11 月）

※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	154	20.6	+ 6
サービス	95	12.7	- 4
建設・建築	59	7.9	- 6
卸売・小売	57	7.6	- 29
情報通信	57	7.6	- 12
医療	56	7.5	- 10
(Unknown)	32	4.3	+ 6
法律	31	4.2	- 13
教育	28	3.8	+ 4
政府機関	27	3.6	+ 19

▼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）



※ 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

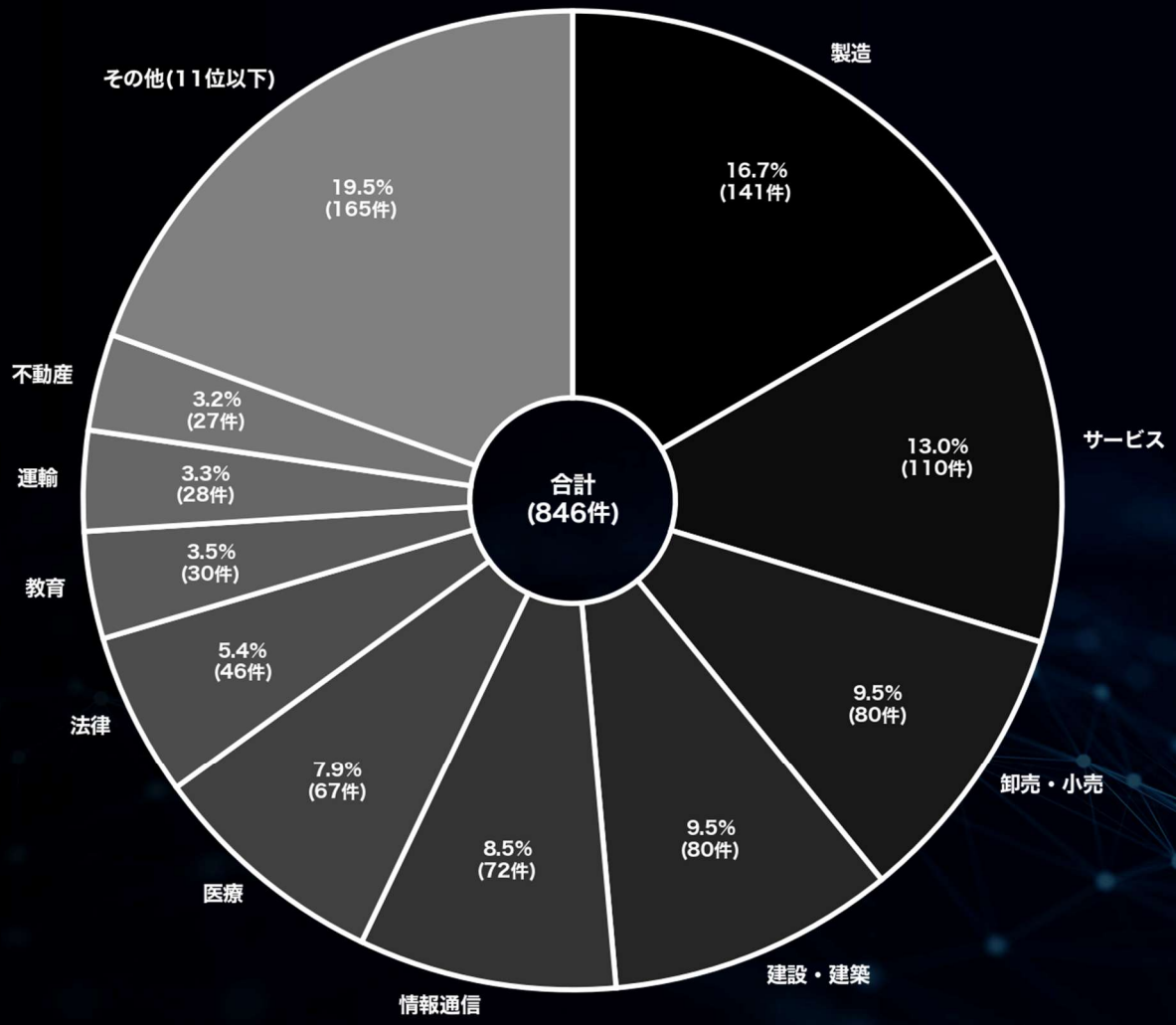
月別内訳 業種 TOP10（全世界）

（2025年 12 月）

※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

▼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）



※ 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

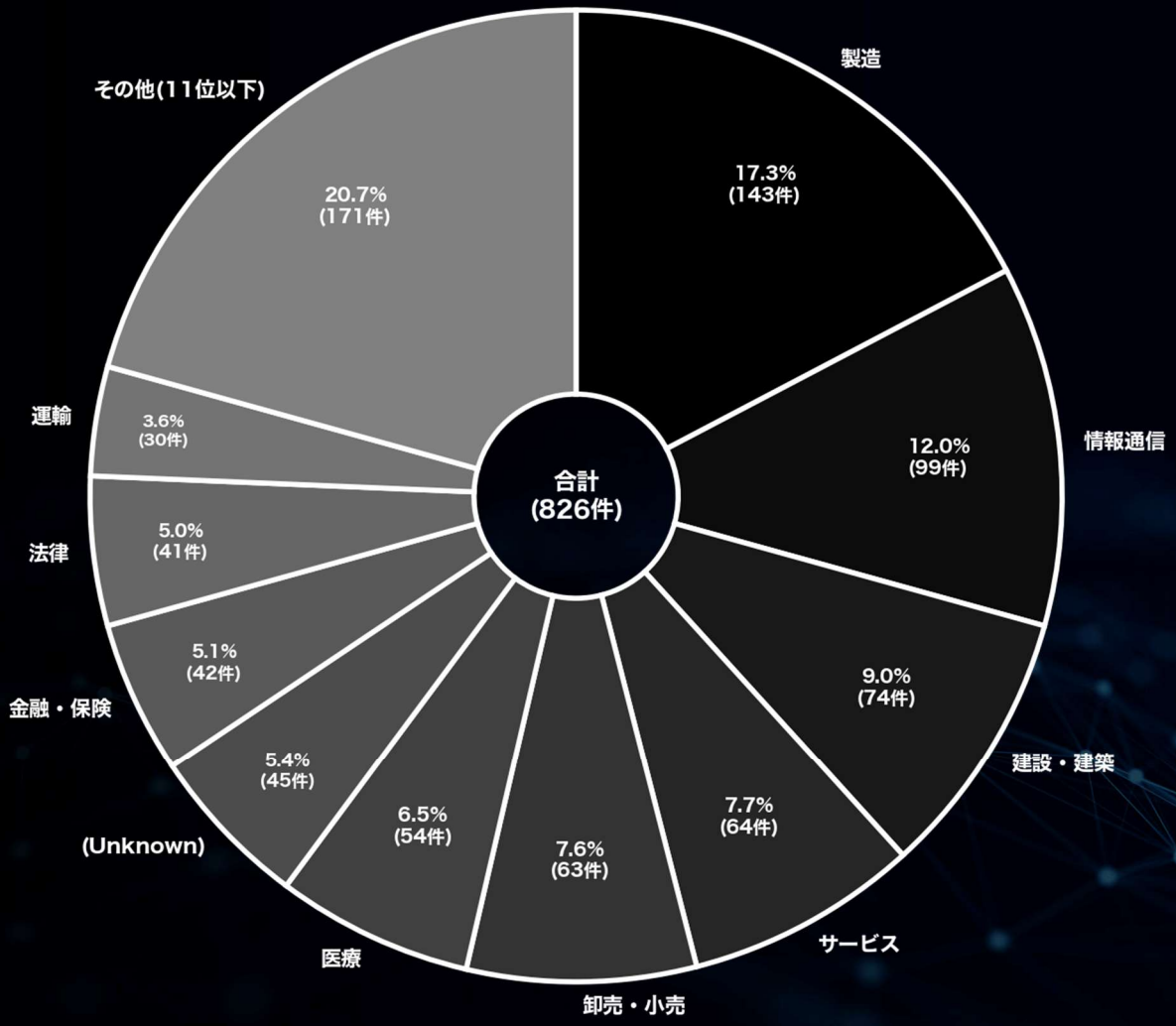
月別内訳 業種 TOP10（全世界）

（2026年 1 月）

※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	143	17.3	+ 2
情報通信	99	12.0	+ 27
建設・建築	74	9.0	- 6
サービス	64	7.7	- 46
卸売・小売	63	7.6	- 17
医療	54	6.5	- 13
(Unknown)	45	5.4	+ 19
金融・保険	42	5.1	+ 17
法律	41	5.0	- 5
運輸	30	3.6	+ 2

▼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）



※ 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

1

被害数の推移に関する統計

（全世界及び国内）

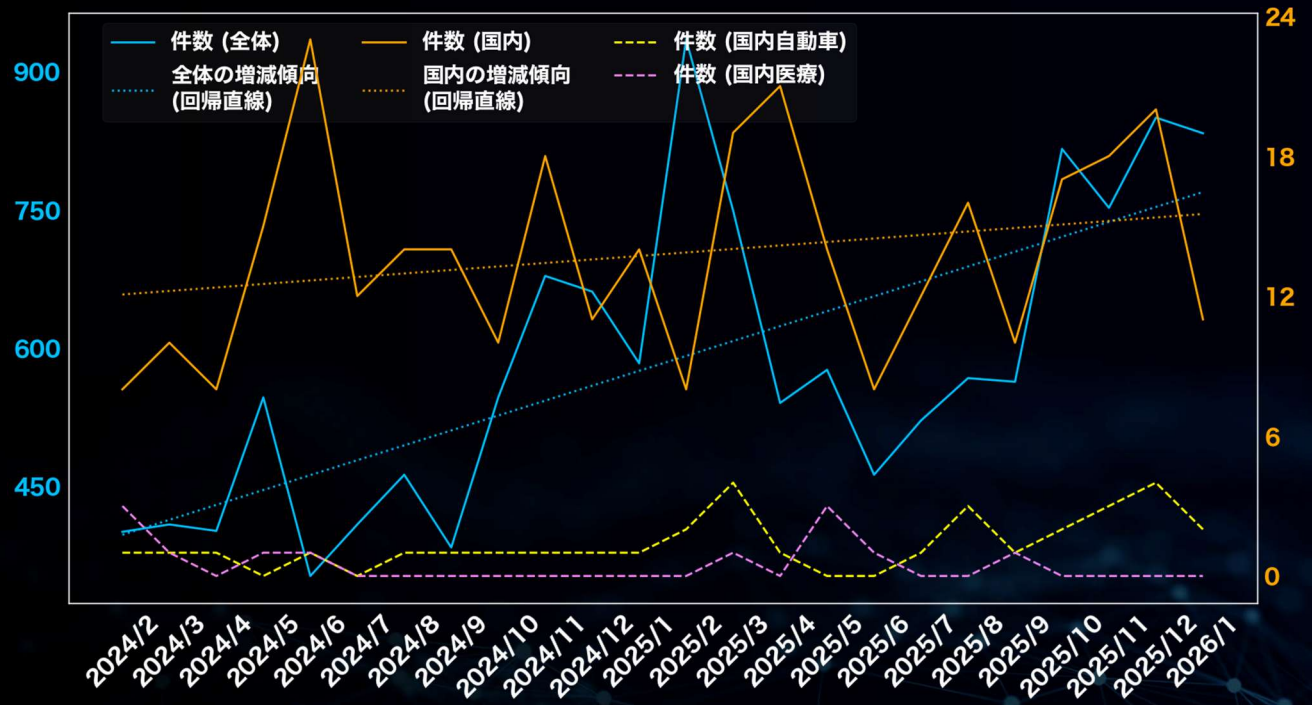
被害数の推移（全世界及び国内）
（過去2年間／2024年2月～2026年1月）

※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）
2024/2	400	8	1	3
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	462	8	0	1
2025/7	521	12	1	0
2025/8	567	16	3	0
2025/9	563	10	1	1
2025/10	816	17	2	0
2025/11	752	18	3	0
2025/12	850	20	4	0
2026/1	833	11	2	0
合計	13992	331	33	12

▼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）

※ 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

資本金別の統計
（国内）

2026

1

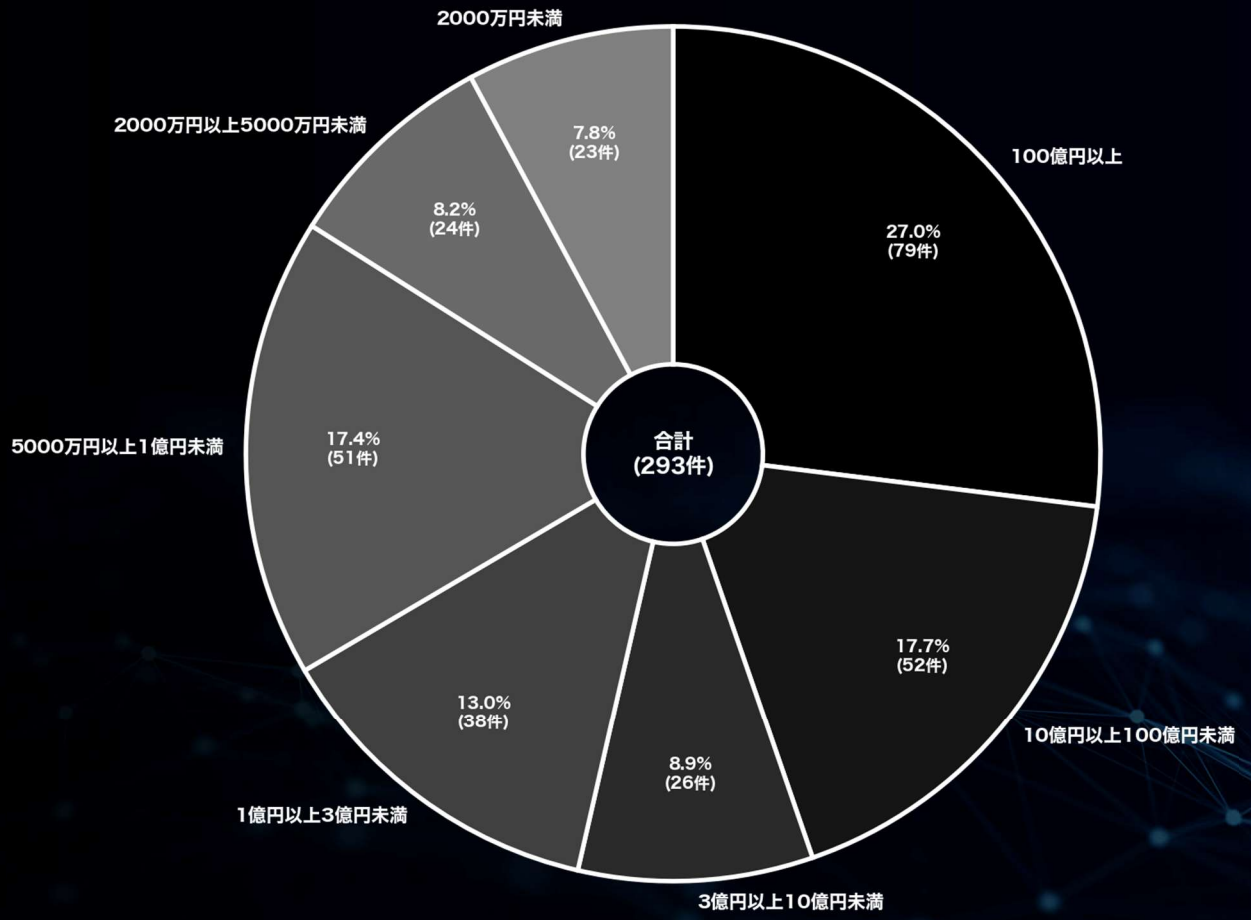
資本金別（国内）
（過去2年間／2024年2月～2026年1月）

※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	79	27.0
10億円以上100億円未満	52	17.7
3億円以上10億円未満	26	8.9
1億円以上3億円未満	38	13.0
5000万円以上1億円未満	51	17.4
2000万円以上5000万円未満	24	8.2
2000万円未満	23	7.8

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

▼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）



（※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

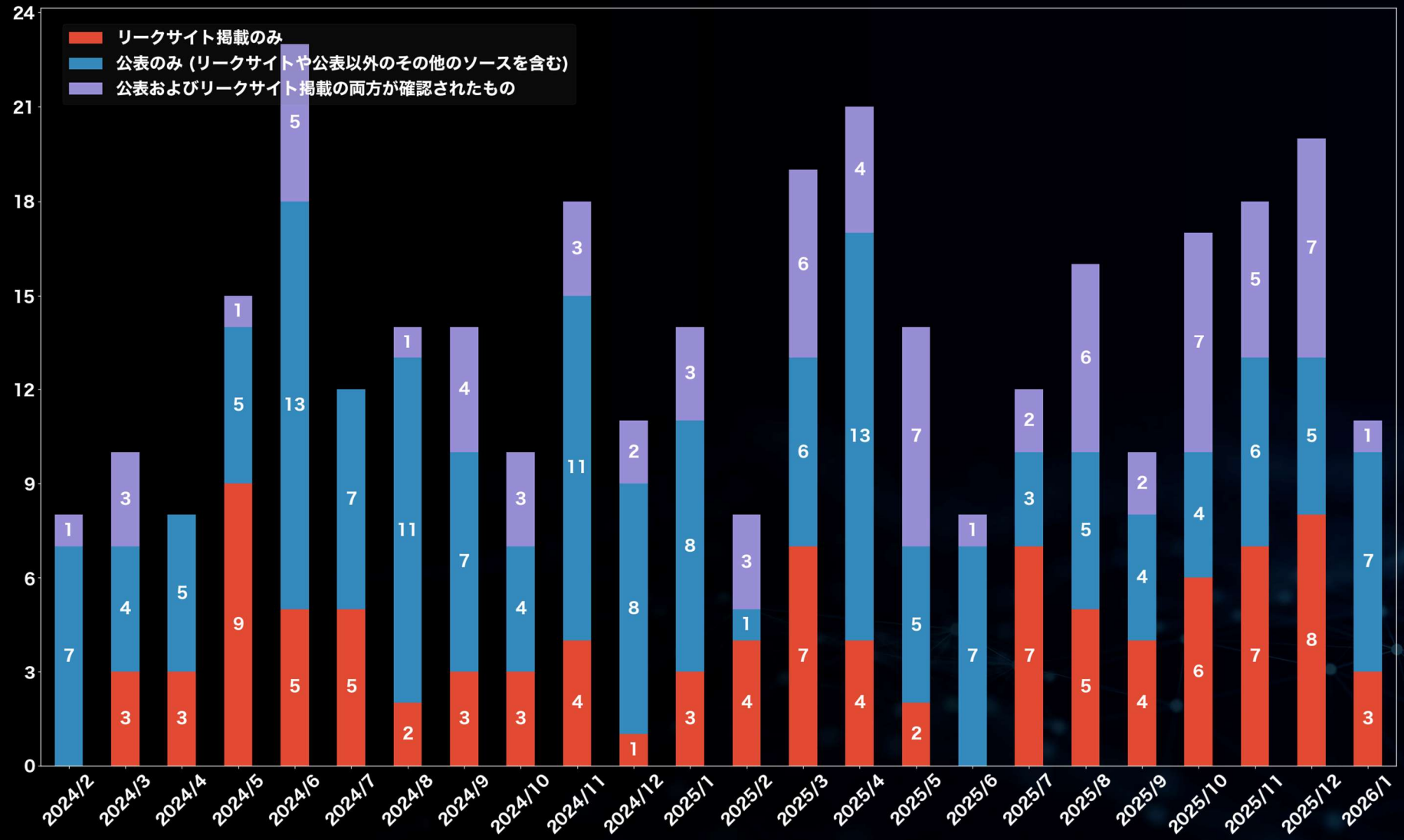
公表と暴露に関する統計
（国内）

2026

1

公表割合 月別内訳（国内）
（過去2年間／2024年2月～2026年1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

1

公となった国内被害組織概要一覧（国内）
（過去1年間／2025年2月～2026年1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
2025/2	Qilin (Agenda)	自動車部品メーカー
2025/2	Hunters International	住宅・施設建設
2025/2	FOG	ITサービス会社
2025/2	(Unknown)	保険代理店
2025/2	LYNX	ITサービス会社
2025/2	Cicada3301	システムインテグレーター
2025/2	Hunters International	緑化・造園業者
2025/2	CL0P (CLOP)	自動車部品メーカー
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(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
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	食品物流業事業者
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
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)

（※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）

※ 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（国内）
（過去1年間／2025年2月～2026年1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
2025/8	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
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	各種機械鋸・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	CL0P (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	CL0P (CLOP)	大手精密機器メーカー(海外拠点)
2025/11	CL0P (CLOP)	大手自動車メーカー
2025/11	CL0P (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)
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)
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	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	Brain Cipher	システムインテグレーター

（※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）

※ 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における拠点割合（国内）

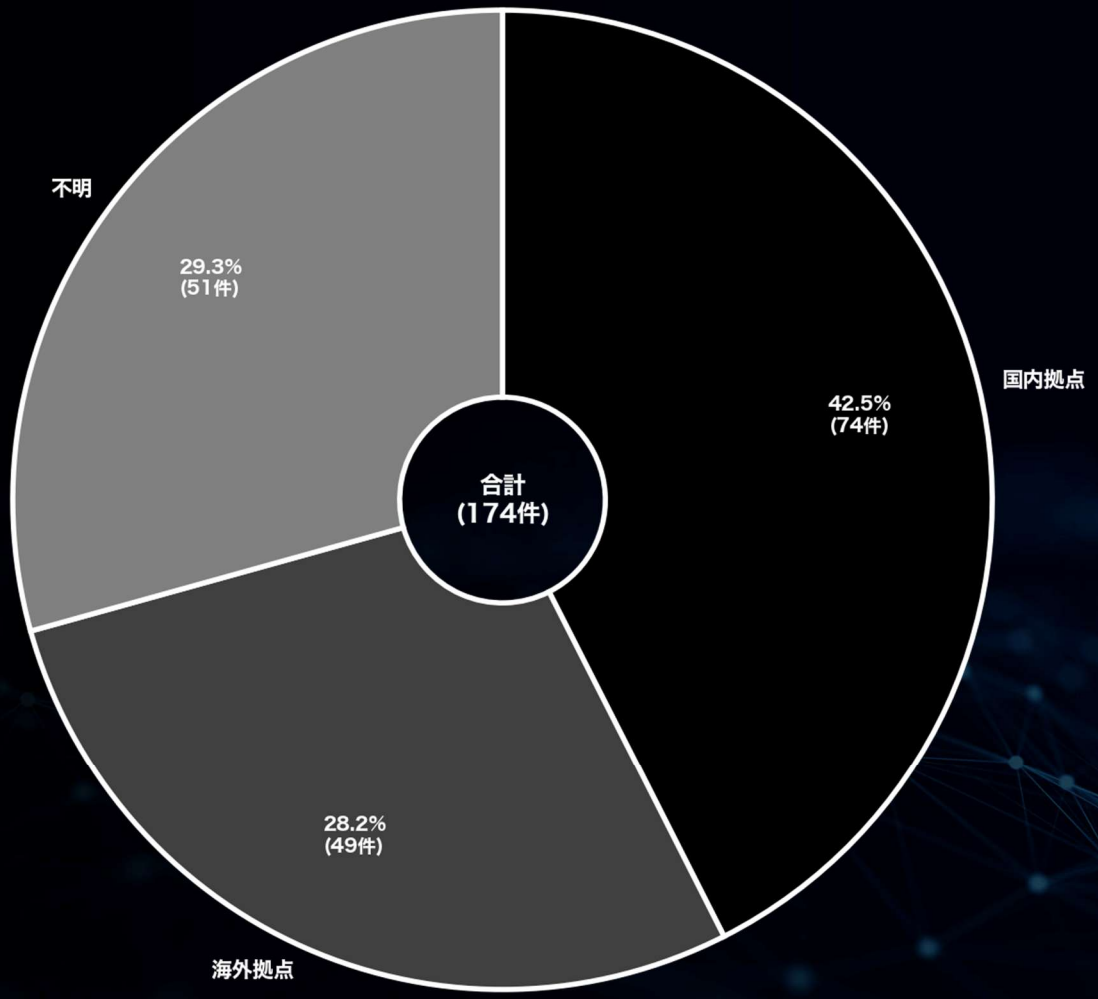
（過去1年間／2025年2月～2026年1月）

（※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）

※
「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	74	42.5
海外拠点	49	28.2
不明	51	29.3

▼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



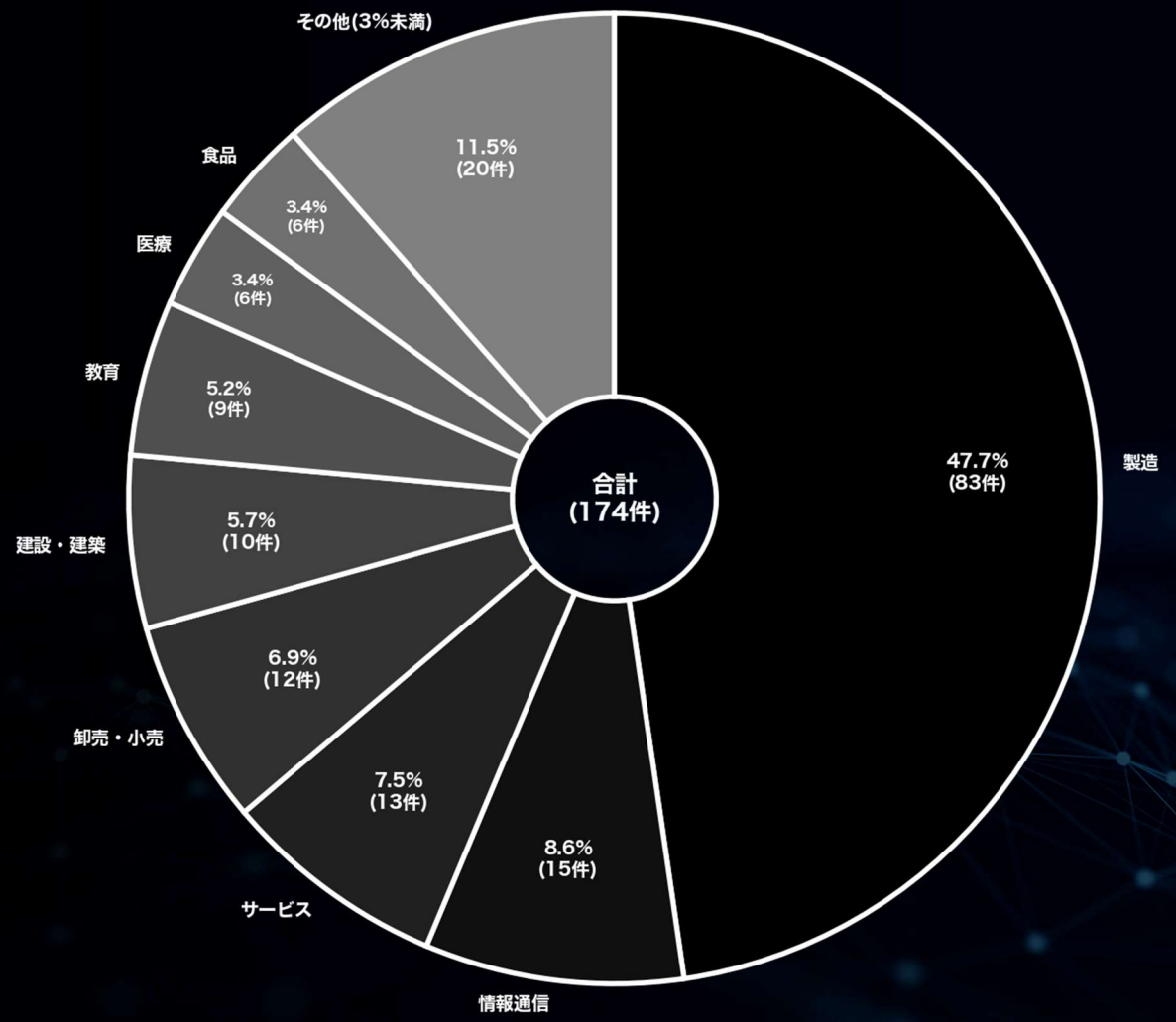
（※本ページの表／グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している）

※ 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における業種割合（国内）
（過去1年間／2025年2月～2026年1月）

業種	件数	割合(%)
製造	83	47.7
情報通信	15	8.6
サービス	13	7.5
卸売・小売	12	6.9
建設・建築	10	5.7
教育	9	5.2
医療	6	3.4
食品	6	3.4
その他(3%未満)	20	11.5

▼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



（※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

中小企業における被害分析
（国内）

2026

1

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/teigi.html

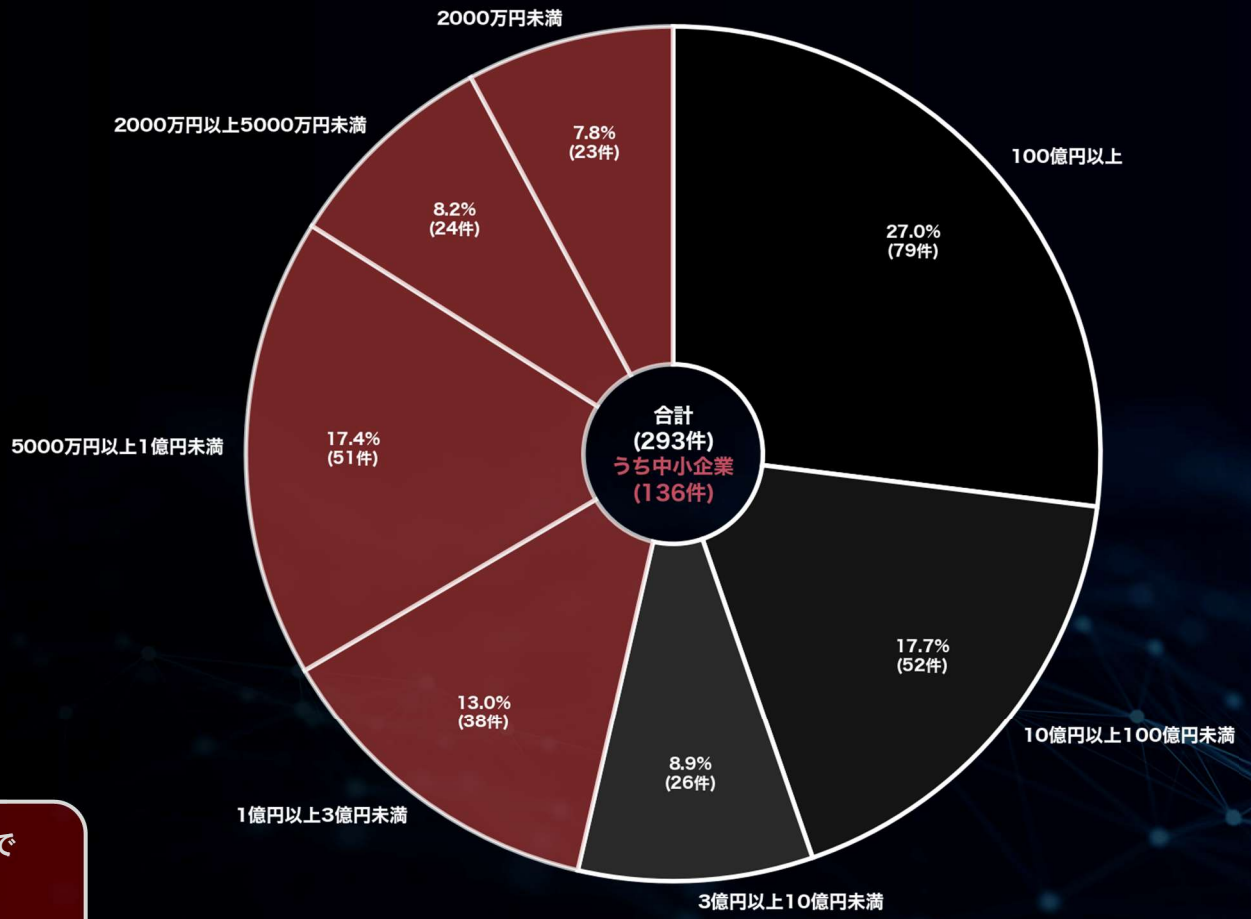
資本金別（国内-中小企業）
（過去2年間／2024年2月～2026年1月）

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	79	27.0
10億円以上100億円未満	52	17.7
3億円以上10億円未満	26	8.9
1億円以上3億円未満	38	13.0
5000万円以上1億円未満	51	17.4
2000万円以上5000万円未満	24	8.2
2000万円未満	23	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136件にのぼり、全体の46.4%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）

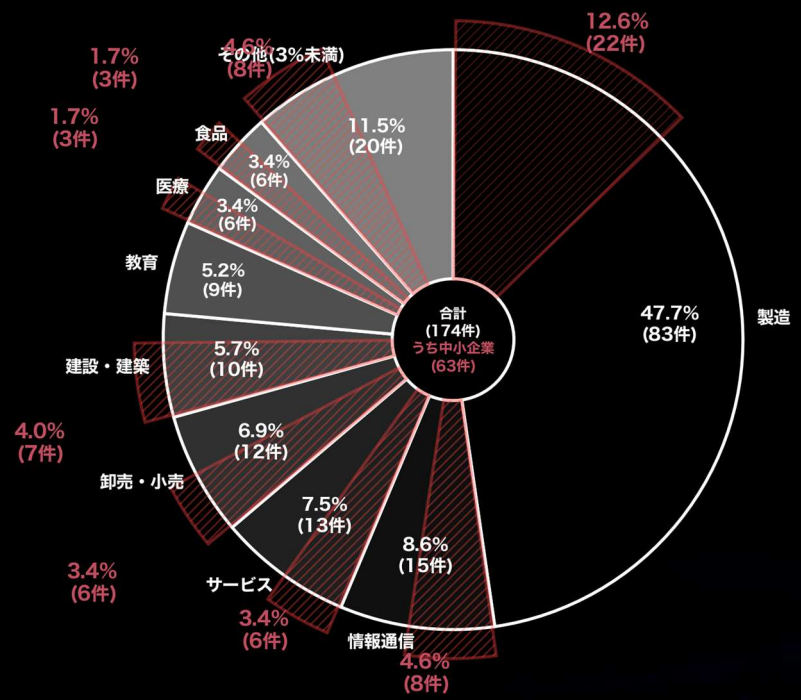
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

公となった国内被害組織における業種割合（国内-中小企業）

（過去1年間／2025年2月～2026年1月）

赤色は中小企業を示す

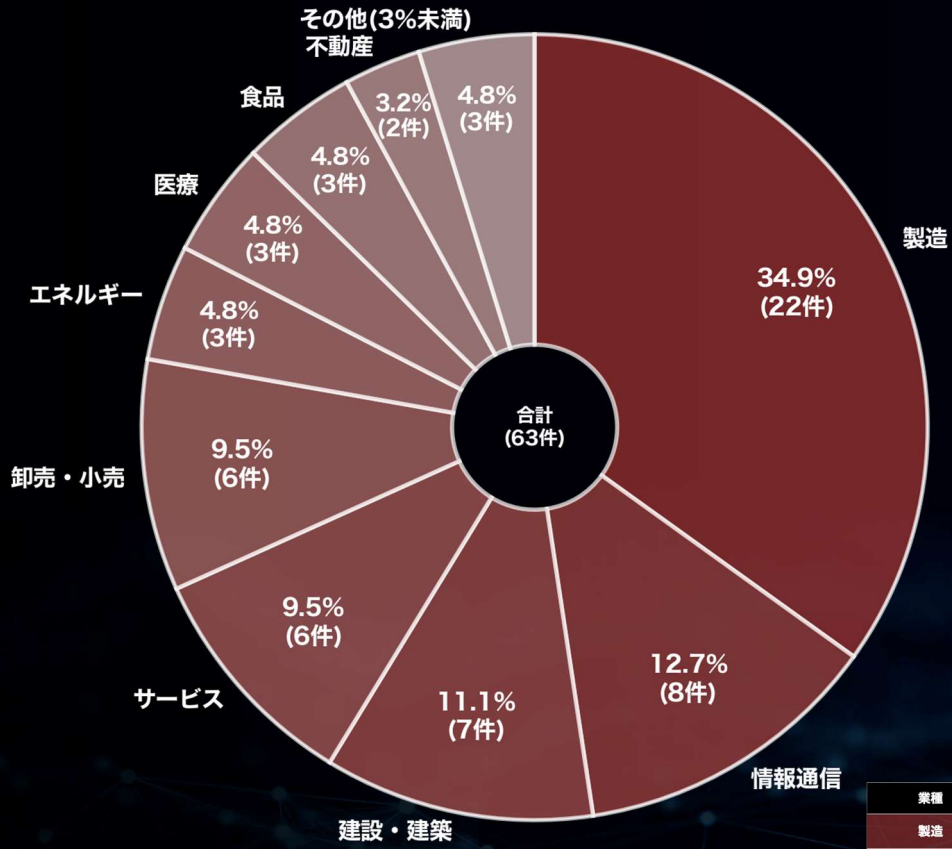
▼全体割合



※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	83 (22)	47.7 (12.6)
情報通信	15 (8)	8.6 (4.6)
サービス	13 (6)	7.5 (3.4)
卸売・小売	12 (6)	6.9 (3.4)
建設・建築	10 (7)	5.7 (4.0)
教育	9	5.2
医療	6 (3)	3.4 (1.7)
食品	6 (3)	3.4 (1.7)
その他(3%未満)	20 (8)	11.5 (4.6)

▼中小企業のみの割合



業種	件数	割合(%)
製造	22	34.9
情報通信	8	12.7
建設・建築	7	11.1
サービス	6	9.5
卸売・小売	6	9.5
エネルギー	3	4.8
医療	3	4.8
食品	3	4.8
不動産	2	3.2
その他(3%未満)	3	4.8

過去1年間の業種別分析においては、中小企業のみに抜粋すると、
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

※ 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

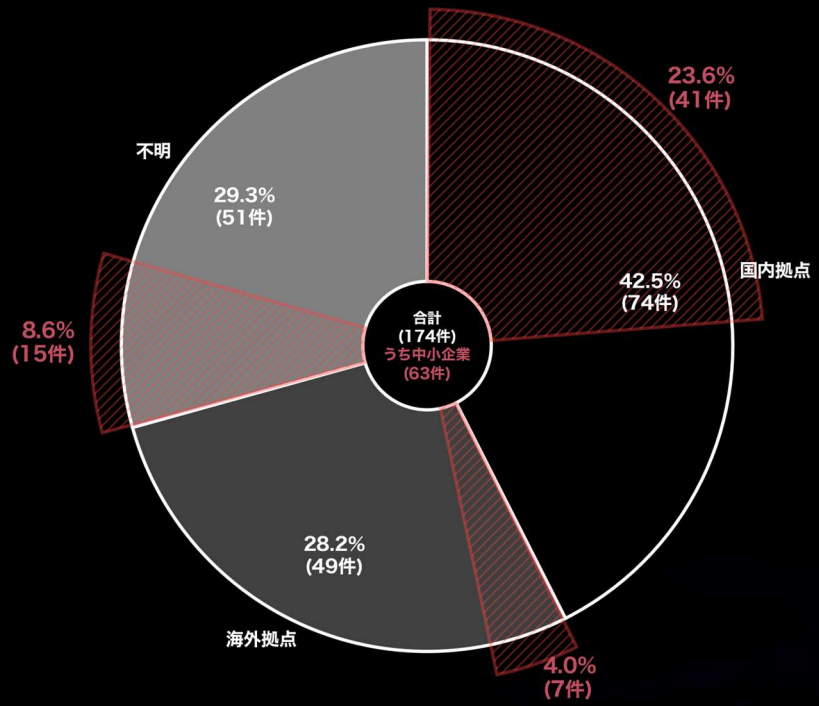
（※本ページの表／グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している）

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）

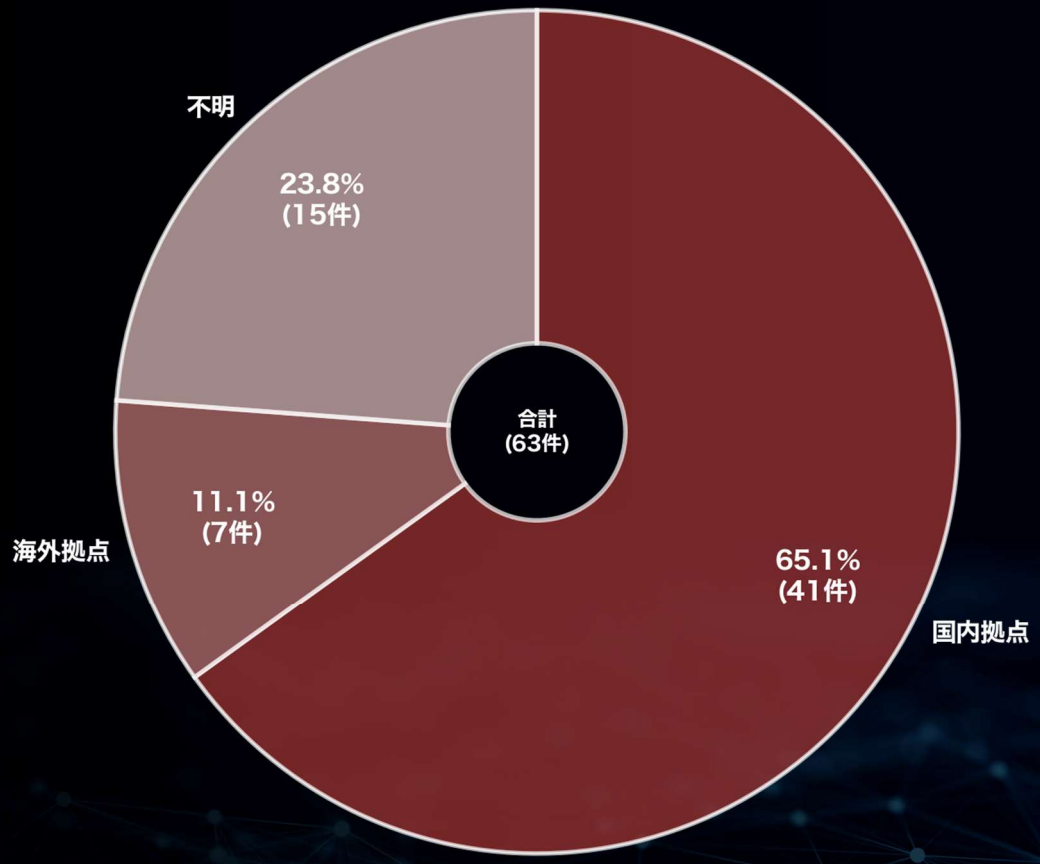
（過去1年間／2025年2月～2026年1月）

赤色は中小企業を示す

▼全体割合



▼中小企業のみの割合



※
「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10億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	74 (41)	42.5 (23.6)
海外拠点	49 (7)	28.2 (4.0)
不明	51 (15)	29.3 (8.6)
合計	174 (63)	100 (36.2)

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	41	65.1
海外拠点	7	11.1
不明	15	23.8

※ 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2月～2026年1月）

赤色は中小企業を示す

※（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
2025/2	Qilin (Agenda)	自動車部品メーカー
2025/2	Hunters International	住宅・施設建設
2025/2	FOG	ITサービス会社
2025/2	(Unknown)	保険代理店
2025/2	LYNX	ITサービス会社
2025/2	Cicada3301	システムインテグレーター
2025/2	Hunters International	緑化・造園業者
2025/2	CL0P (CLOP)	自動車部品メーカー
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(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
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	食品物流業事業者
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
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)

（※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）

※ 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（国内-中小企業）

（過去1年間／2025年2月～2026年1月）

赤色は中小企業を示す

※（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
2025/8	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
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	各種機械鋸・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)
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)
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	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	Brain Cipher	システムインテグレーター

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状況が確認されている。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

（※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）

※ 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

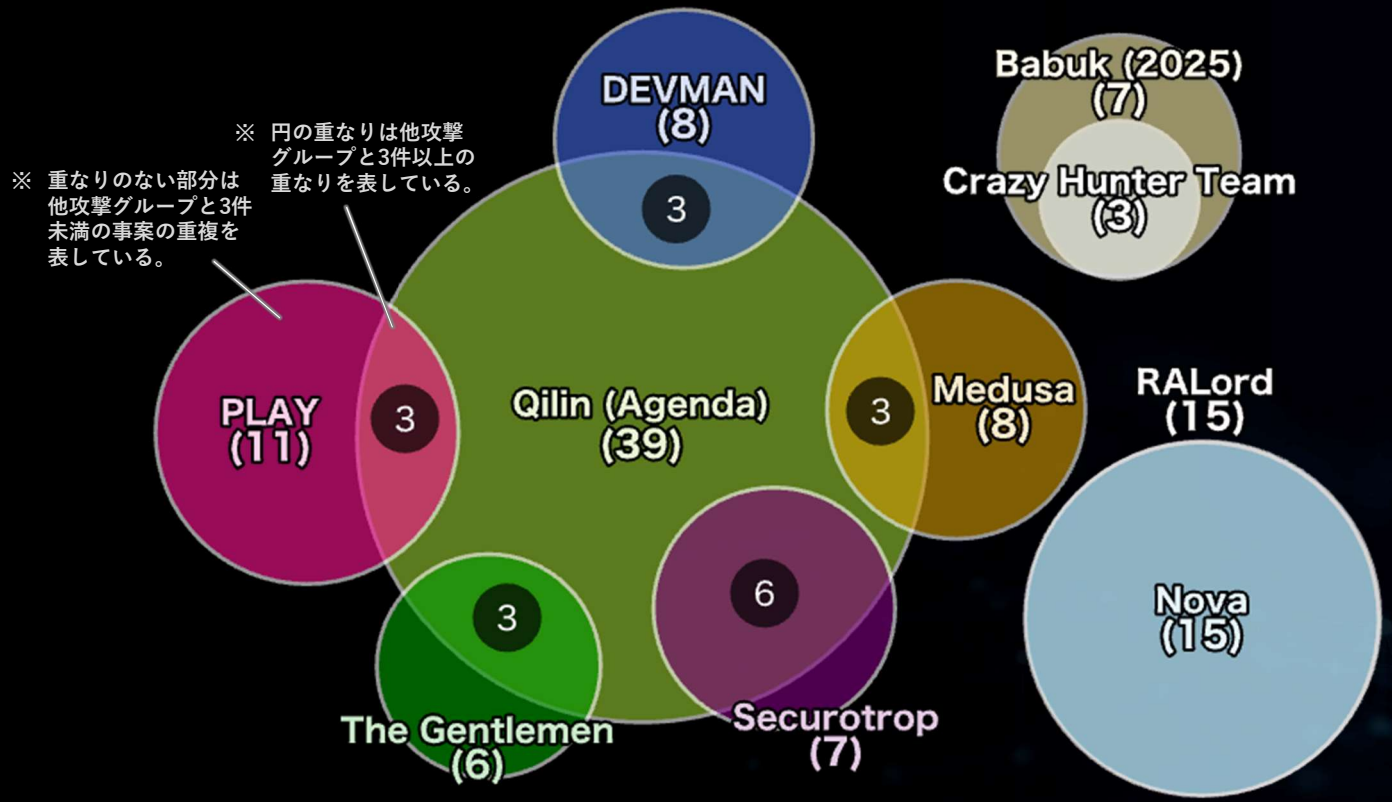
多重被害に関する分析

2026

1

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2月～2026年1月）　（累計137件）※多重被害に遭った組織数の累計



※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

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。

近年の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。

※ 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

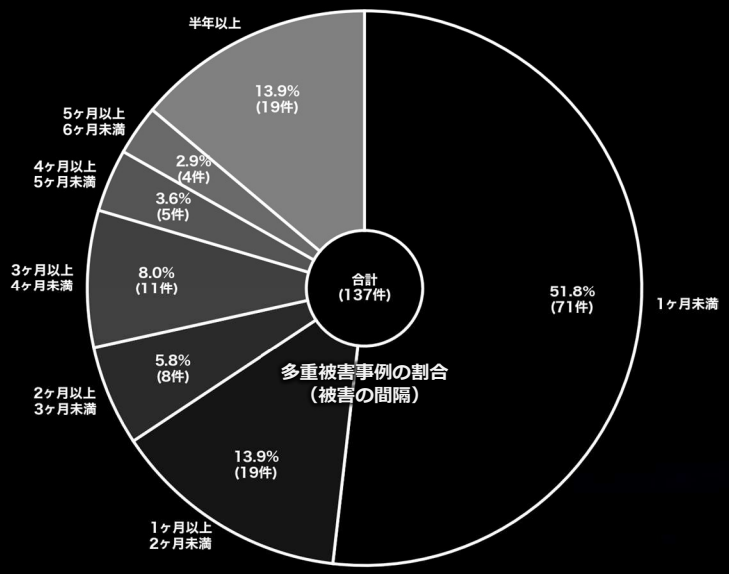
多重被害に遭った被害組織の傾向と分析（全世界）

（過去1年間／2025年2月～2026年1月）

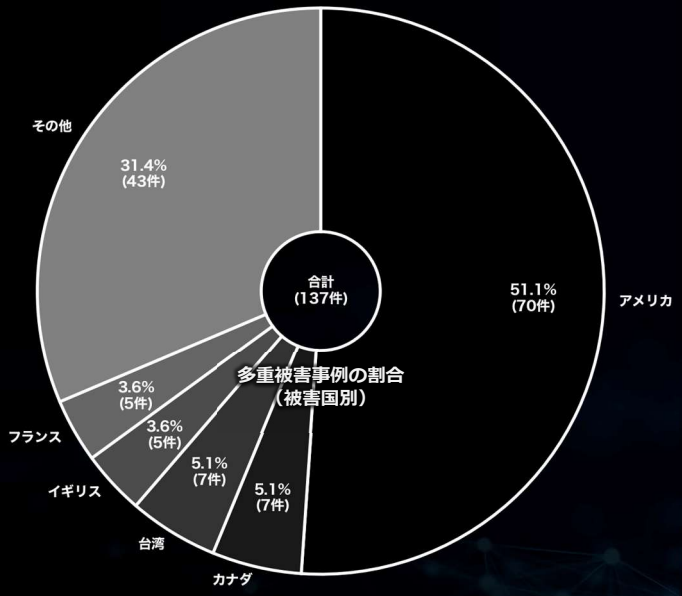
※多重被害：一度ランサムウェア攻撃の被害を受けた組織が異なる時期に異なる攻撃グループのリークサイトに再び掲載されるケース

▼被害の間隔

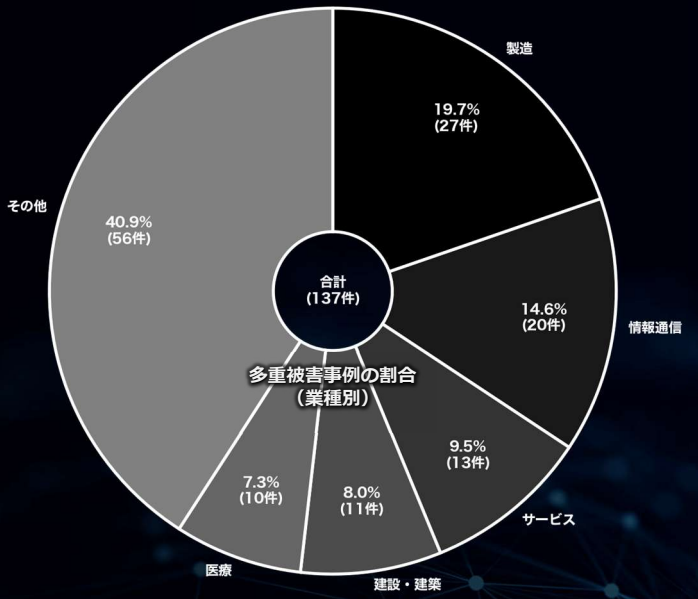
（一度目の被害から二度目の被害までの間隔）



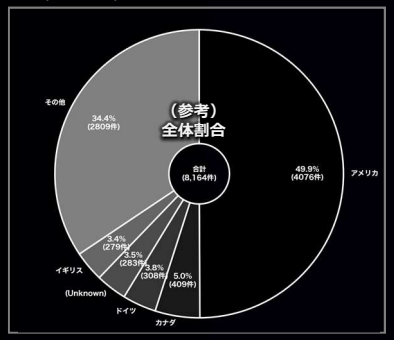
▼被害国別



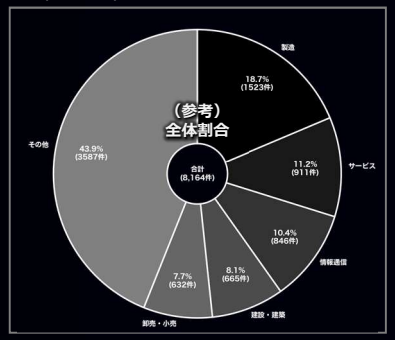
▼業種別



（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



▶多重被害に遭った組織数の累計：137件（全体8164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。

※ 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

1

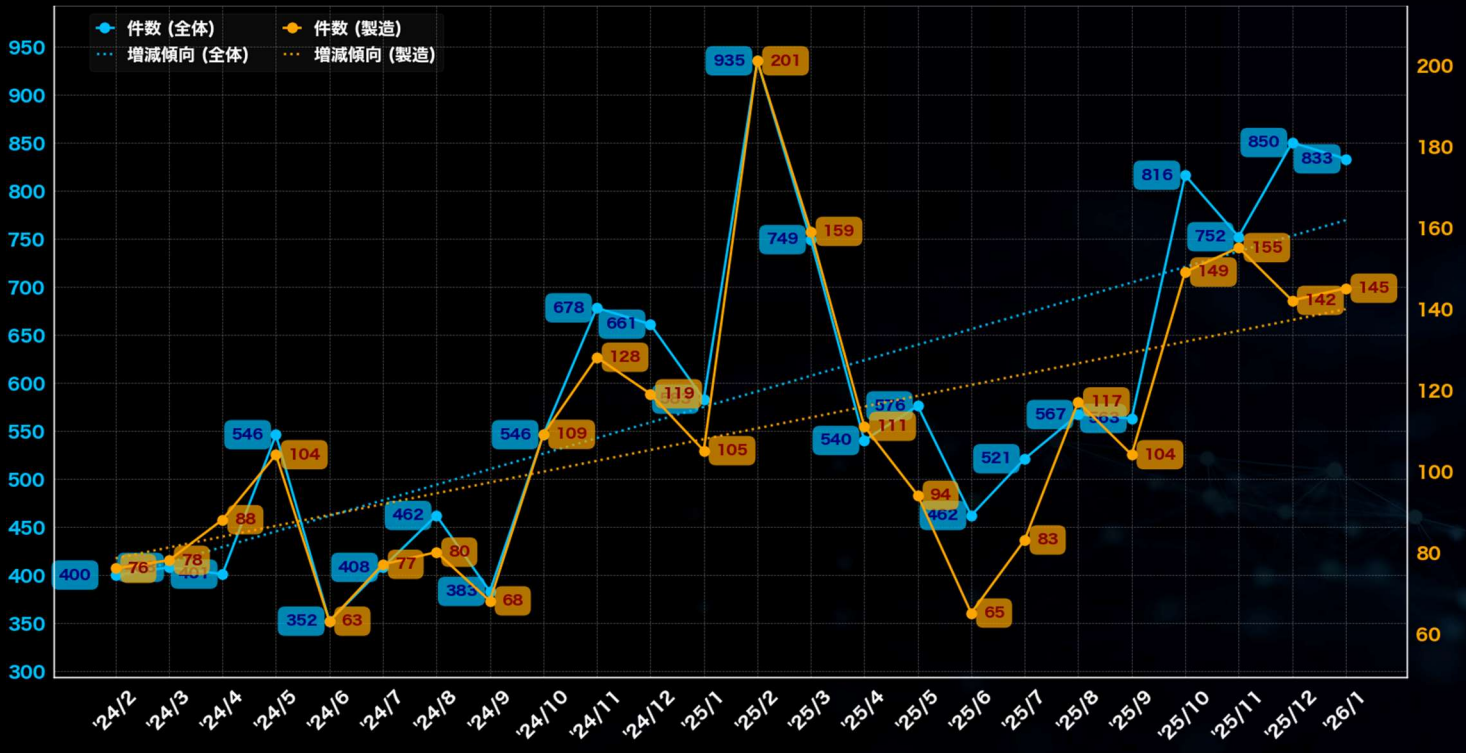
業種に関する分析

（過去2年間のリークサイト掲載上位10業種）

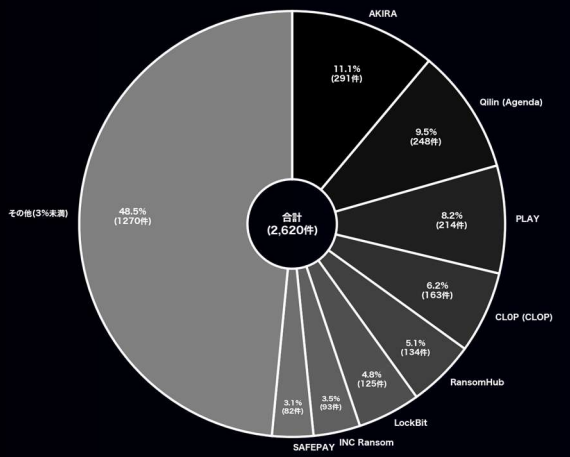
業種に関する分析（全世界）
（過去2年間／2024年2月～2026年1月）

製造

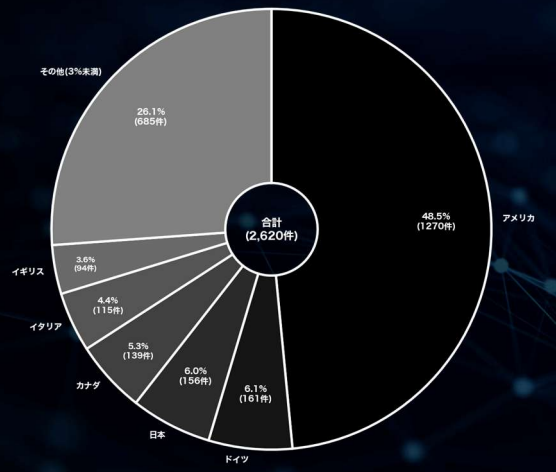
「製造」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、201件の掲載があった。一方、最も少なかった月は2024年6月で、63件であった。被害組織の所在国の割合では、アメリカが約49%と最も多く、次いでドイツと日本がそれぞれ約6%である。攻撃グループについては、少なくとも132のグループが関与しており、特に「AKIRA」が291件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「PLAY」がそれぞれ248件と214件の掲載を行っている。製造関連の件数は全体件数に対して高い割合で推移しており、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、長期に渡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



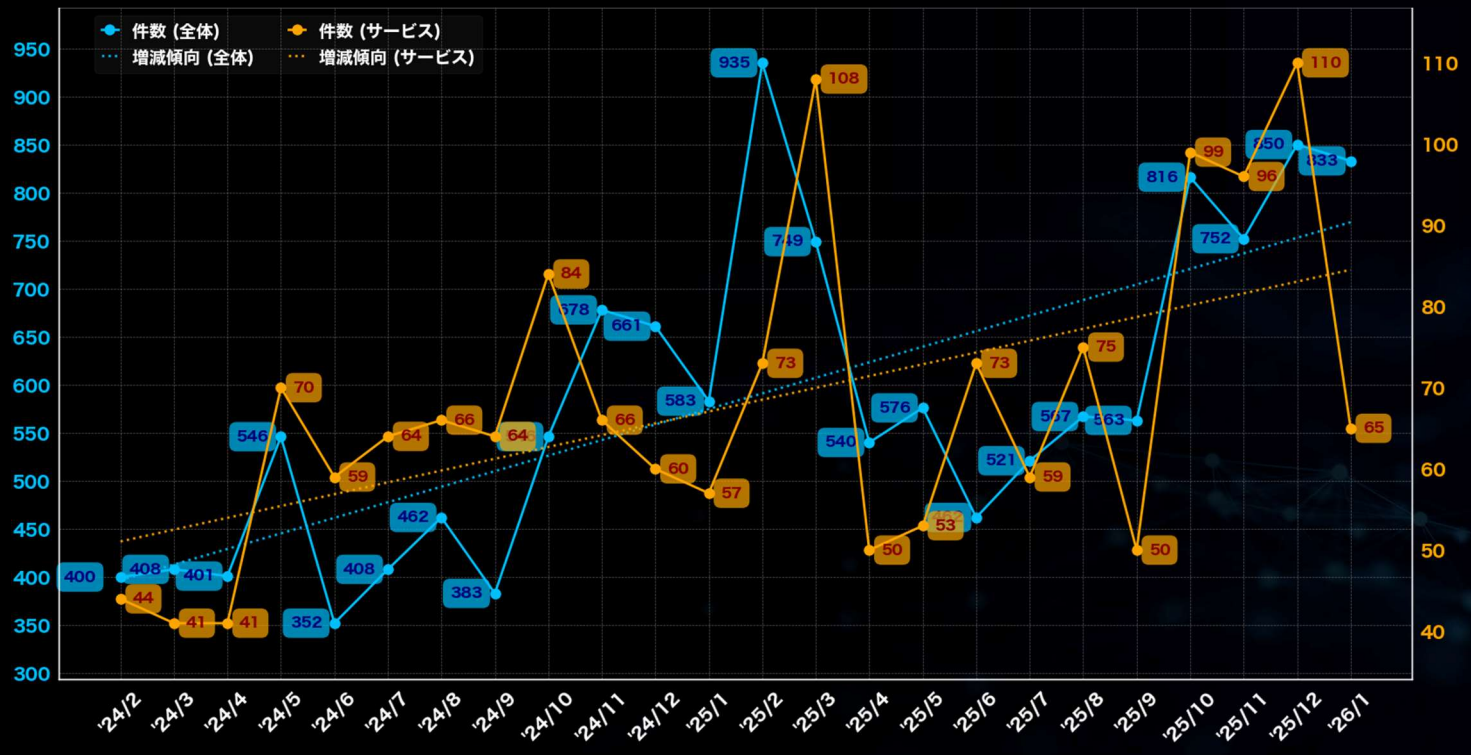
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

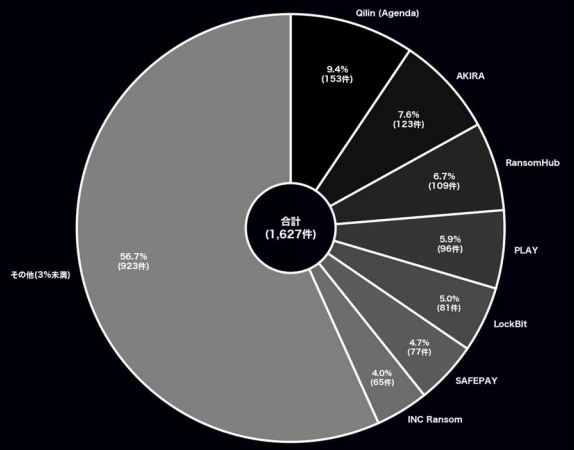
業種に関する分析（全世界）
（過去2年間／2024年2月～2026年1月）

サービス

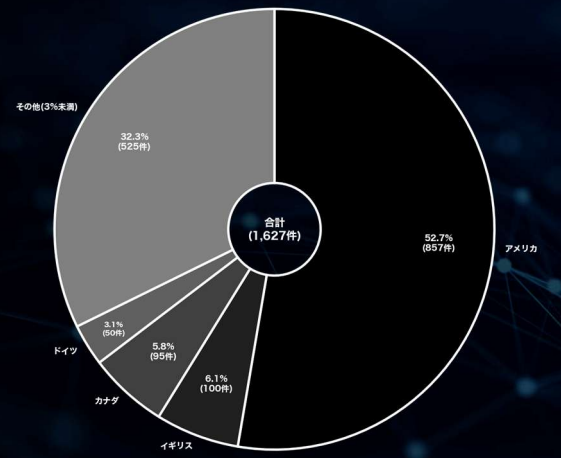
「サービス」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年12月で、110件の掲載があった。一方、最も少なかった月は2024年3月および4月で、41件であった。被害組織の所在国の割合では、アメリカが約53%と最も多く、次いでイギリスとカナダがそれぞれ約6%である。攻撃グループについては、少なくとも124のグループが関与しており、特に「Qilin (Agenda)」が153件のリークサイト掲載を実施している。次いで「AKIRA」と「RansomHub」がそれぞれ123件と109件の掲載を行っている。サービス関連の件数は製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



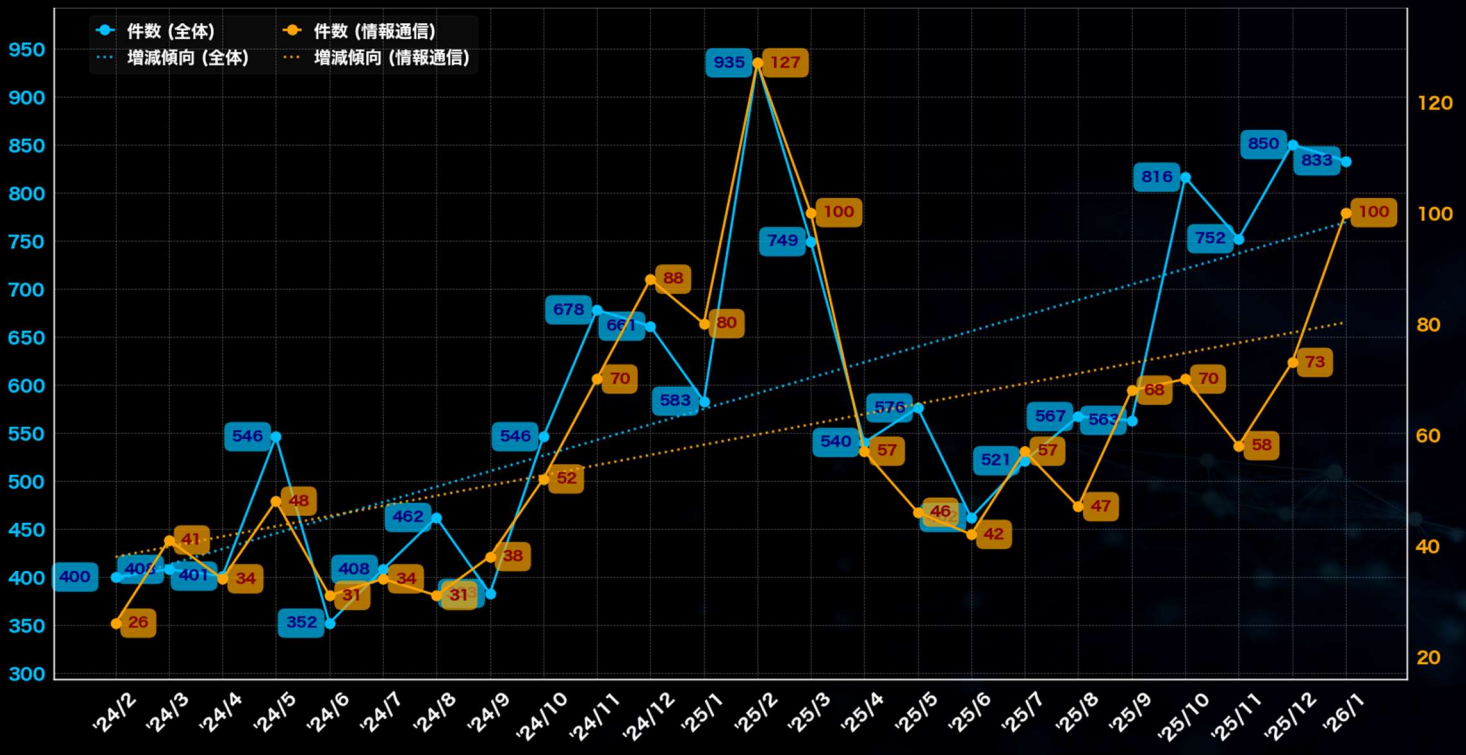
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

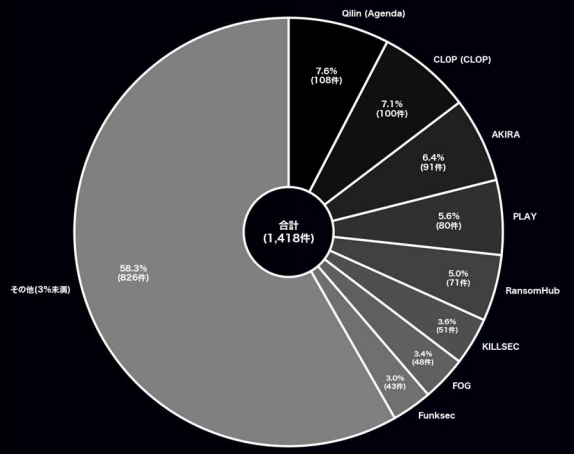
業種に関する分析（全世界）
（過去2年間／2024年2月～2026年1月）

情報通信

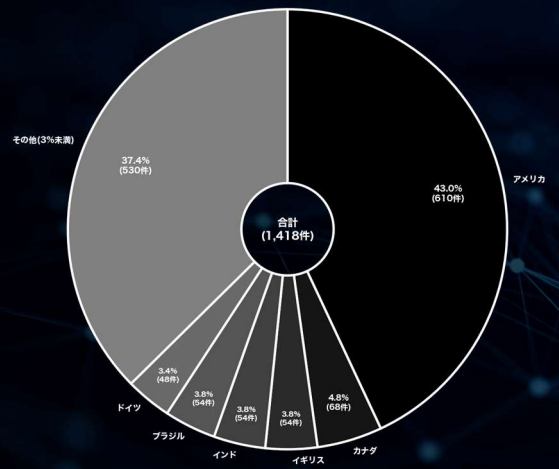
「情報通信」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、127件の掲載があった。一方、最も少なかった月は2024年2月で、26件であった。被害組織の所在国の割合では、アメリカが約43%と最も多く、次いでカナダとイギリスがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも130のグループが関与しており、特に「Qilin（Agenda）」が108件のリークサイト掲載を実施している。次いで「CL0P（CLOP）」と「AKIRA」がそれぞれ100件と91件の掲載を行っている。過去2年間におけるリークサイ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



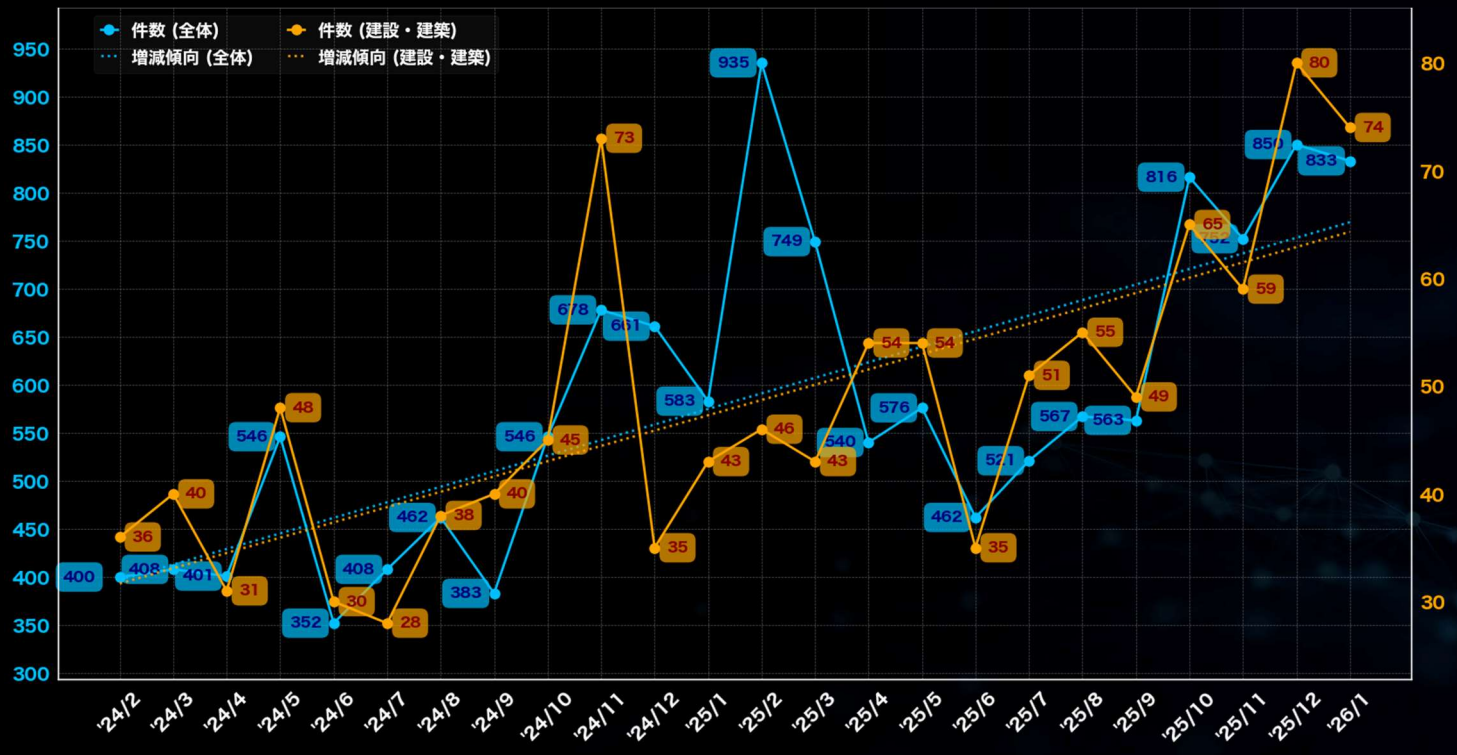
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

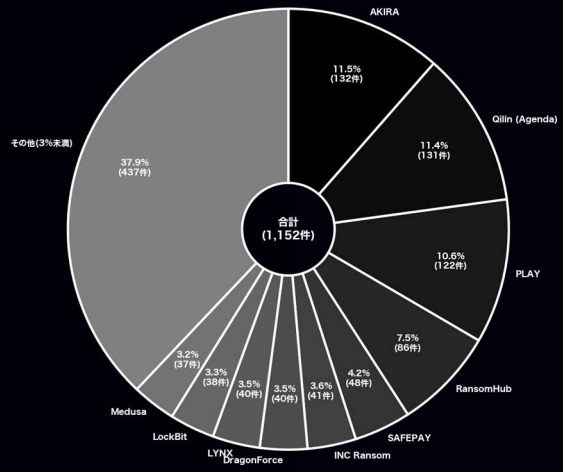
業種に関する分析（全世界）
（過去2年間／2024年2月～2026年1月）

建設・建築

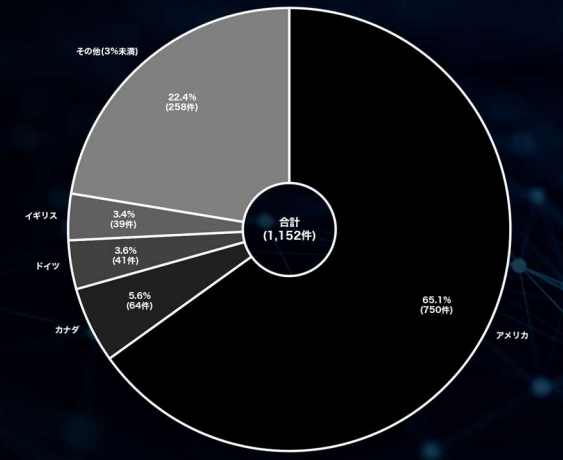
「建設・建築」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年12月で、80件の掲載があった。一方、最も少なかった月は2024年7月で、28件であった。被害組織の所在国の割合では、アメリカが約65%と最も多く、次いでカナダとドイツがそれぞれ約6%と約4%である。攻撃グループについては、少なくとも99のグループが関与しており、特に「AKIRA」が132件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「PLAY」がそれぞれ131件と122件の掲載を行っている。製造関連などと比べると件数は少ないものの、明確な増加傾向にある。



▼攻撃グループ別



▼国別



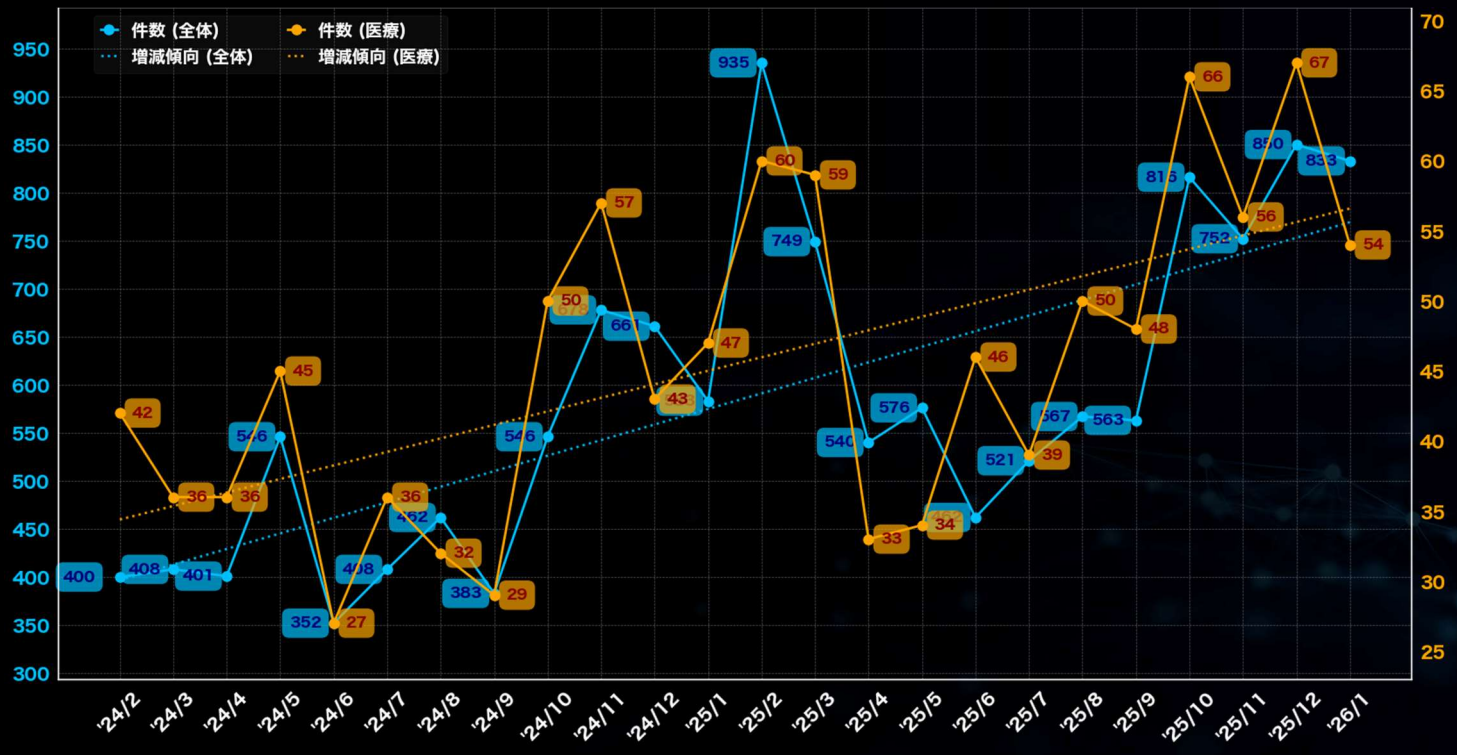
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

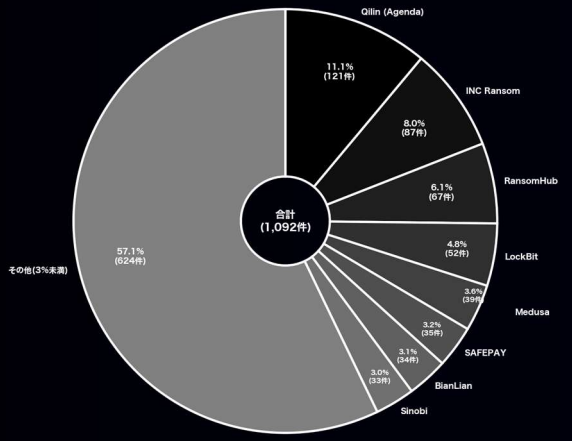
業種に関する分析（全世界）
（過去2年間／2024年2月～2026年1月）

医療

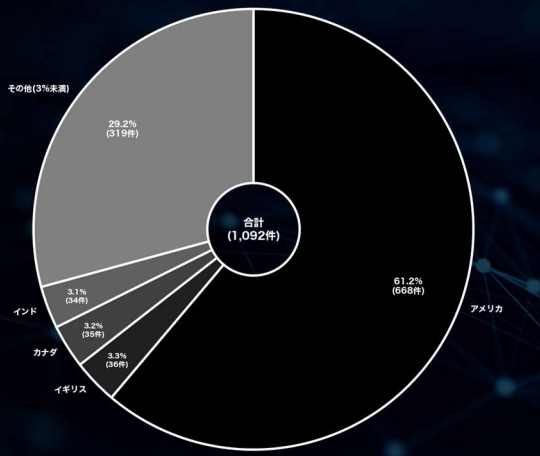
「医療」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年12月で、67件の掲載があった。一方、最も少なかった月は2024年6月で、27件であった。被害組織の所在国の割合では、アメリカが約61%と最も多く、次いでイギリス、カナダがそれぞれ約3%である。攻撃グループについては、少なくとも114のグループが関与しており、特に「Qilin (Agenda)」が121件のリークサイト掲載を実施している。次いで「INC Ransom」と「RansomHub」がそれぞれ87件と67件の掲載を行っている。かつては低水準だった医療関連の被害数は2023年3月頃に増加し、その後も高い水準が継続している。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



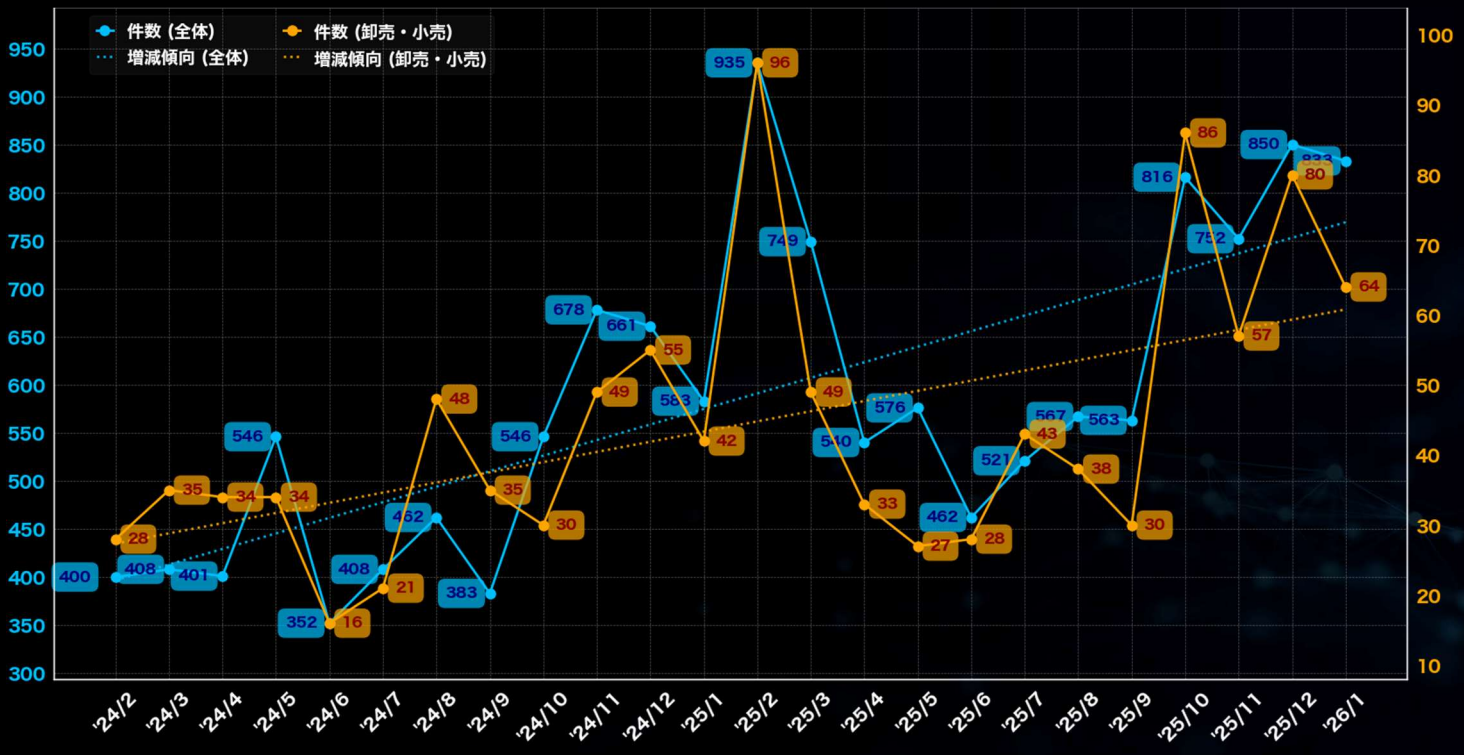
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

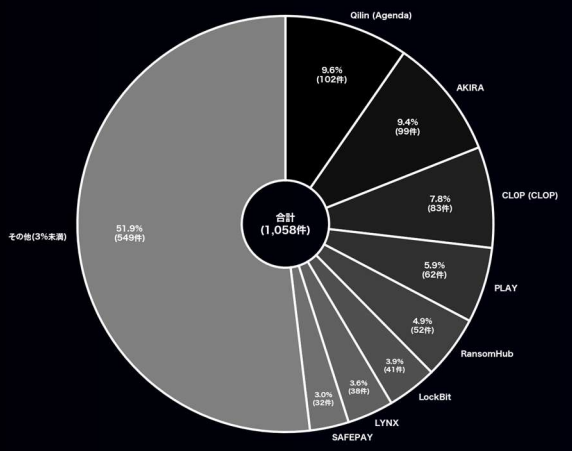
業種に関する分析（全世界）
（過去2年間／2024年2月～2026年1月）

卸売・小売

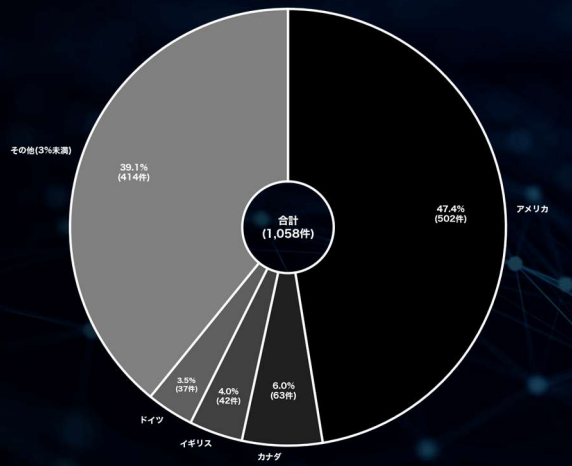
「卸売・小売」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、96件の掲載があった。一方、最も少なかった月は2024年6月で、16件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いでカナダとイギリスがそれぞれ約6%と約4%である。攻撃グループについては、少なくとも105のグループが関与しており、特に「Qilin (Agenda)」が102件のリークサイト掲載を実施している。次いで「AKIRA」と「CL0P (CLOP)」が99件と83件の掲載を行っている。卸売・小売関連は大きな増減の波があるものの、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



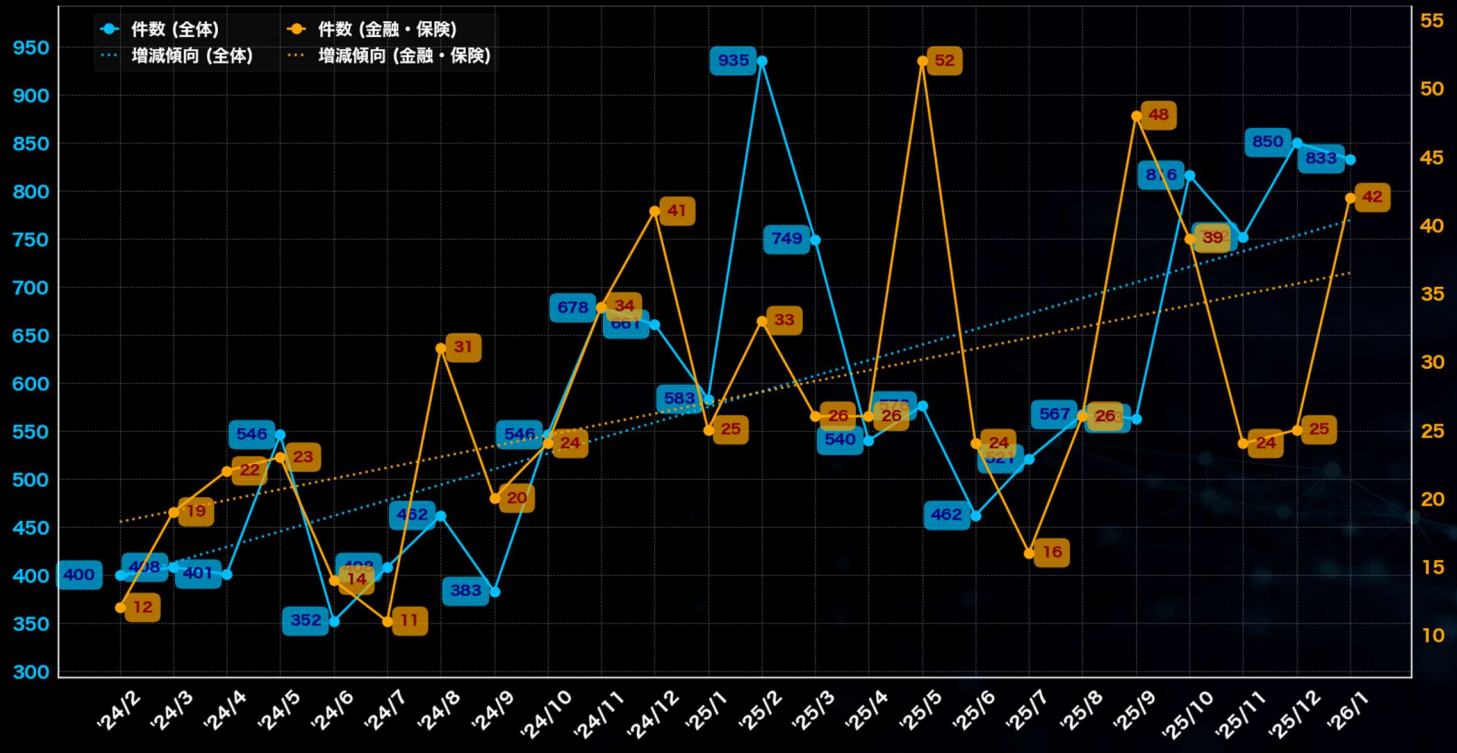
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

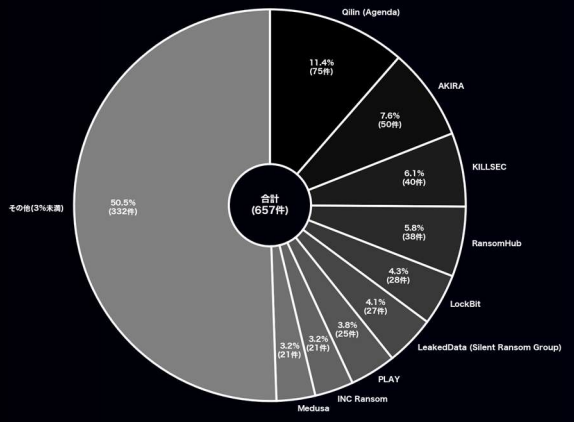
業種に関する分析（全世界）
（過去2年間／2024年2月～2026年1月）

金融・保険

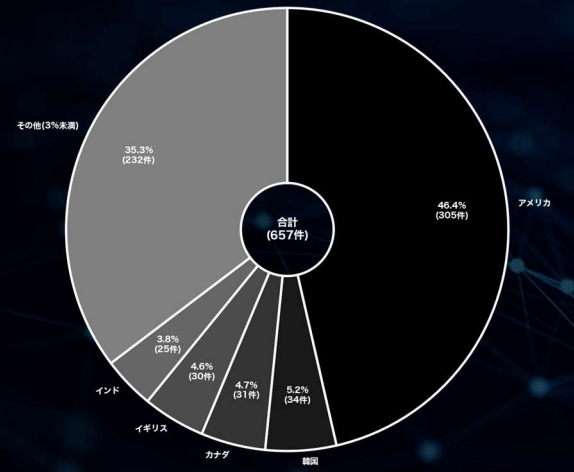
「金融・保険」業界に対するランサムウェア攻撃のリークサイト掲載件数は、最も多かった月が2025年5月で、52件の掲載があった。一方、最も少なかった月は2024年7月で、11件であった。被害組織の所在国の割合では、アメリカが約46%と最も多く、次いで韓国とカナダがそれぞれ約5%である。攻撃グループについては、少なくとも102のグループが関与しており、特に「Qilin (Agenda)」が75件のリークサイト掲載を実施している。次いで「AKIRA」と「KILLSEC」がそれぞれ50件と40件の掲載を行っている。金融・保険関連は全体件数に対する割合は低いものの明確な増加傾向にある。



▼攻撃グループ別



▼国別



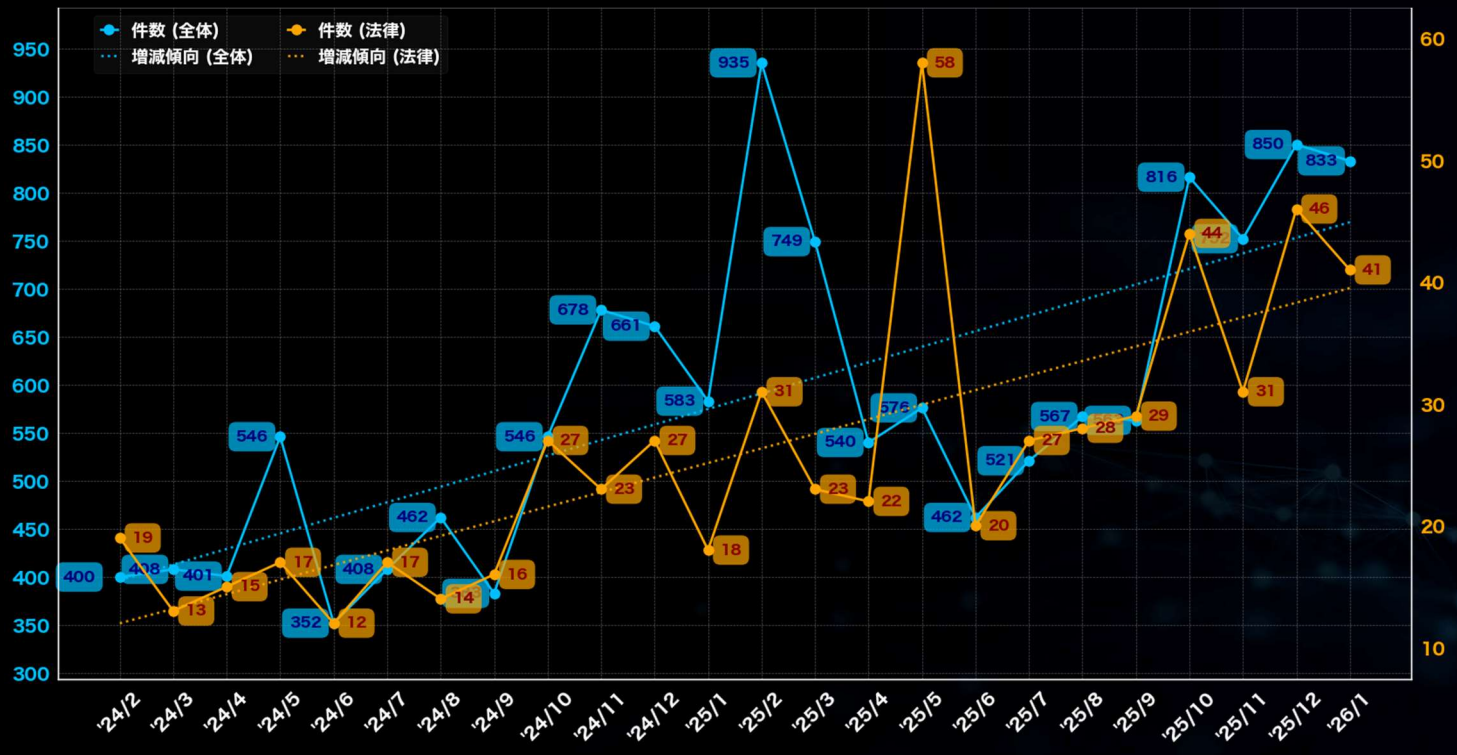
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

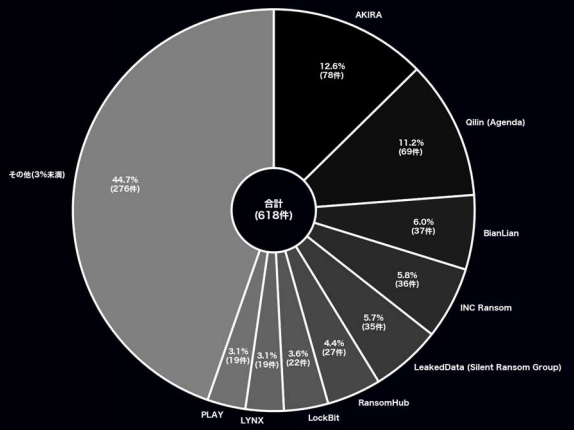
業種に関する分析（全世界）
（過去2年間／2024年2月～2026年1月）

法律

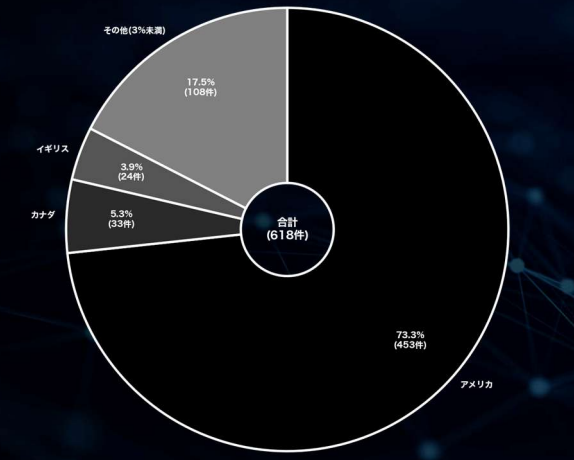
「法律」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年5月で、58件の掲載があった。一方、最も少なかった月は2024年6月で、12件であった。被害組織の所在国の割合では、アメリカが約73%と最も多く、次いでカナダとイギリスがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも84のグループが関与しており、特に「AKIRA」が78件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「BianLian」がそれぞれ69件と37件の掲載を行っている。法律関連は2023年末以降、減少傾向が見られたが、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



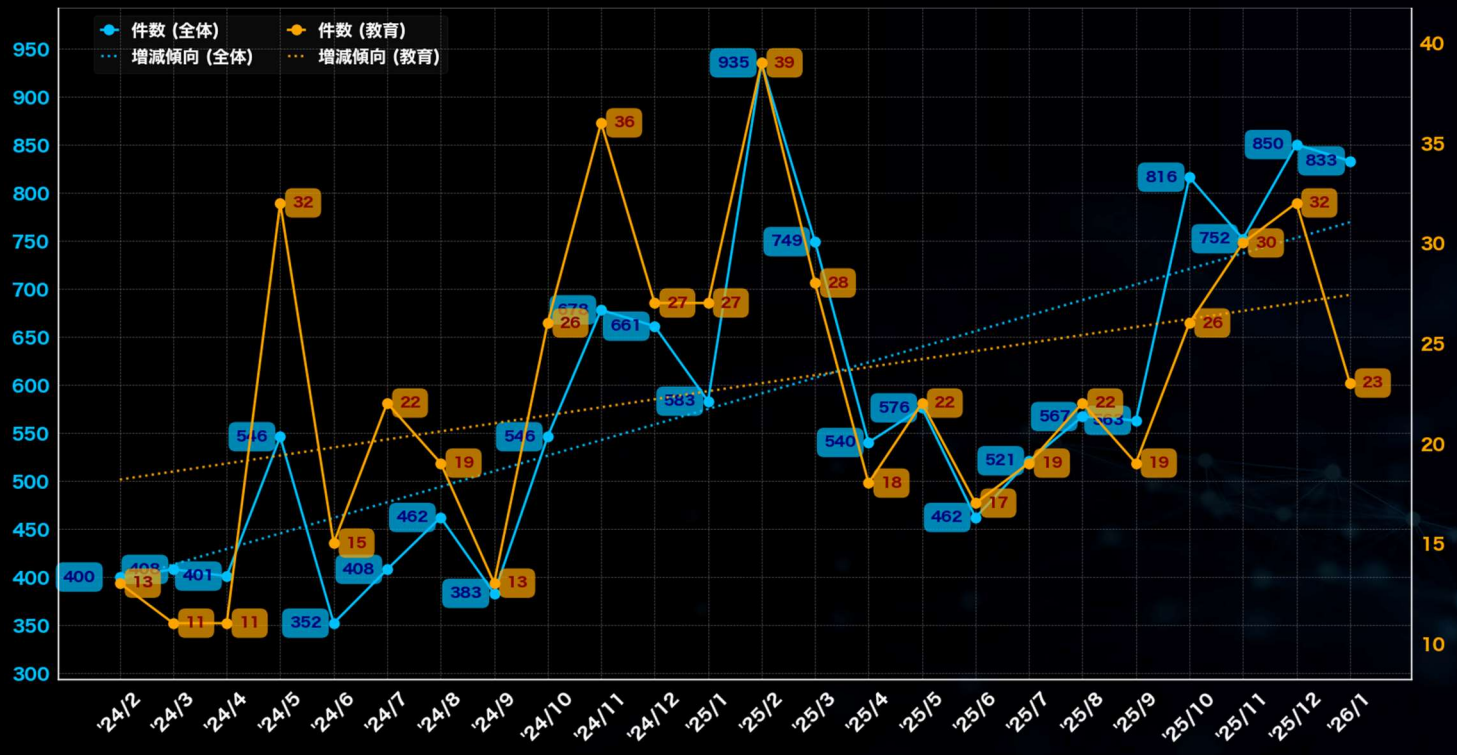
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて
国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

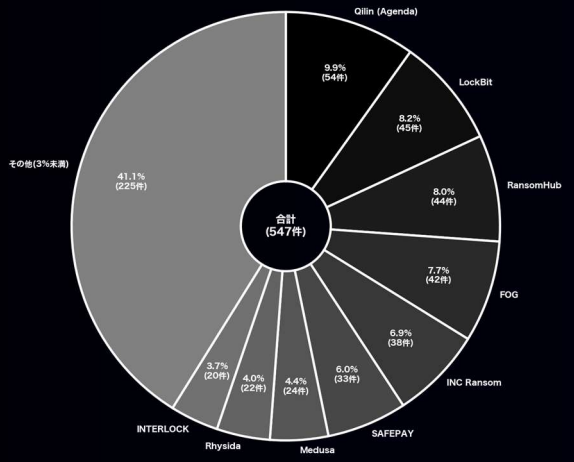
業種に関する分析（全世界）
（過去2年間／2024年2月～2026年1月）

教育

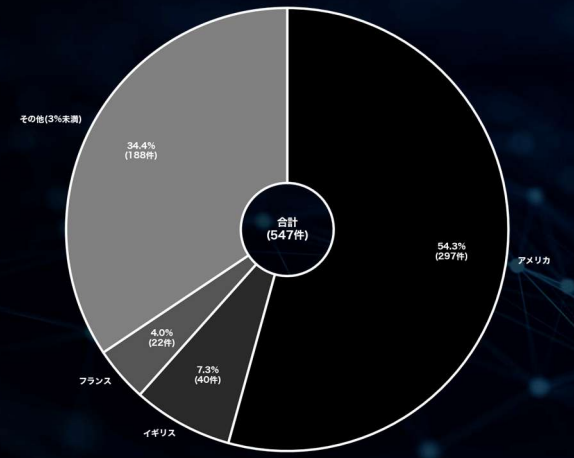
「教育」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、39件の掲載があった。一方、最も少なかった月は2024年3月と4月で、11件であった。被害組織の所在国の割合では、アメリカが約54%と最も多く、次いでイギリスとフランスがそれぞれ約7%と約4%である。攻撃グループについては、少なくとも86のグループが関与しており、特に「Qilin (Agenda)」が54件のリークサイト掲載を実施している。次いで「LockBit」と「RansomHub」がそれぞれ45件と44件の掲載を行っている。過去2年間の推移は緩やかな増加傾向となっている。



▼攻撃グループ別



▼国別



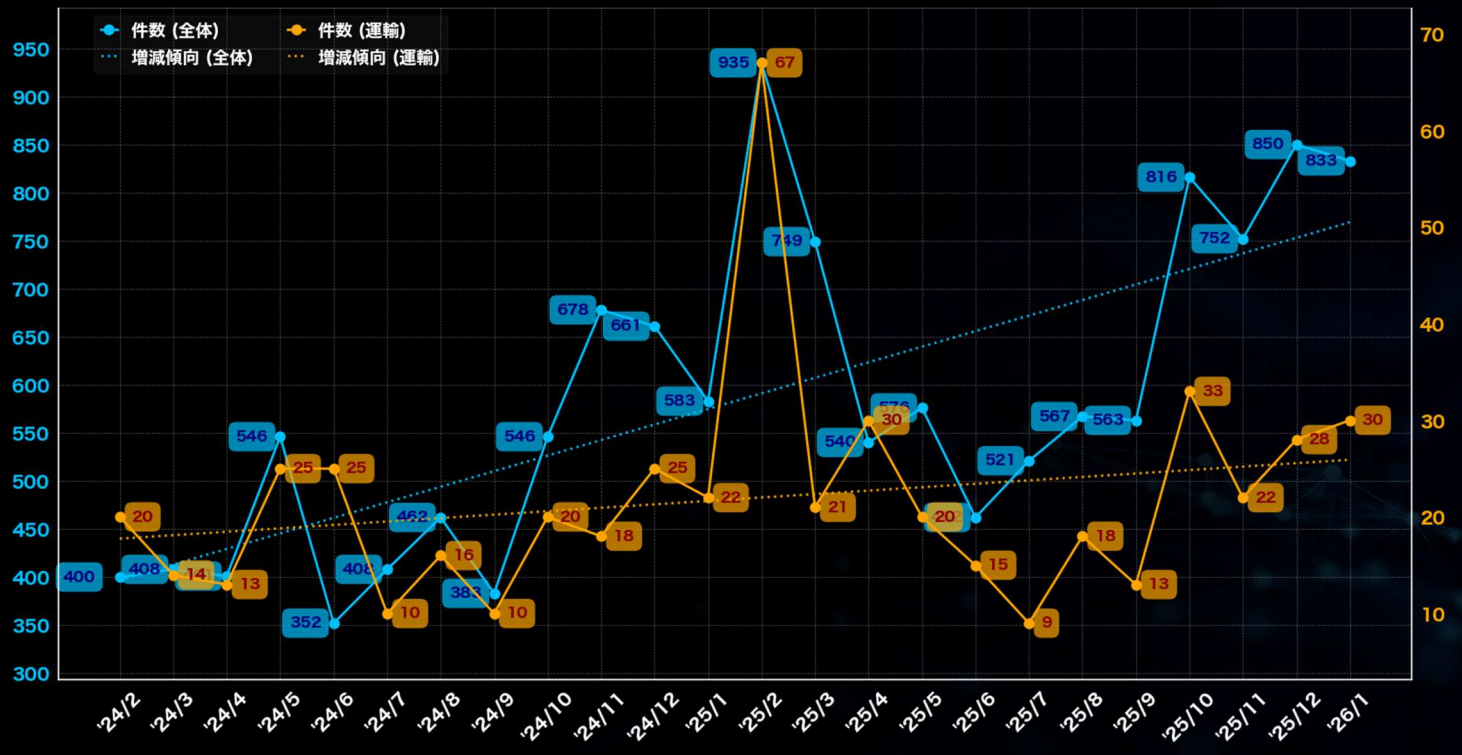
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

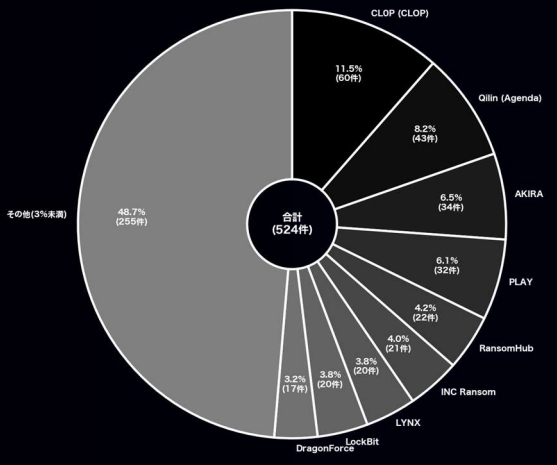
業種に関する分析（全世界）
（過去2年間／2024年2月～2026年1月）

運輸

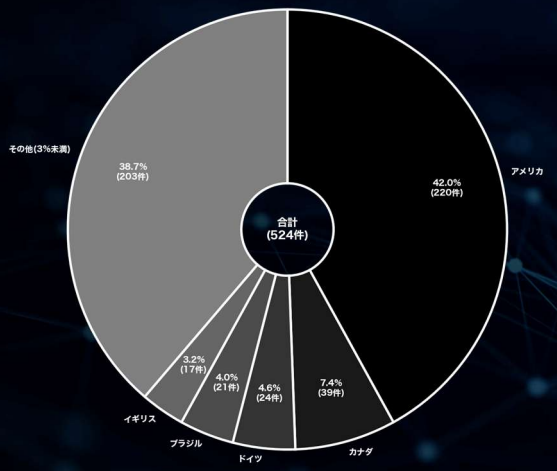
「運輸」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、67件の掲載があった。一方、最も少なかった月は2025年7月で、9件であった。被害組織の所在国の割合では、アメリカが約42%と最も多く、次いでカナダとドイツがそれぞれ約7%と約5%である。攻撃グループについては、少なくとも91のグループが関与しており、特に「CL0P (CLOP)」が60件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「AKIRA」がそれぞれ43件と34件の掲載を行っている。運輸関係は全体件数に対する割合こそ低く、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。

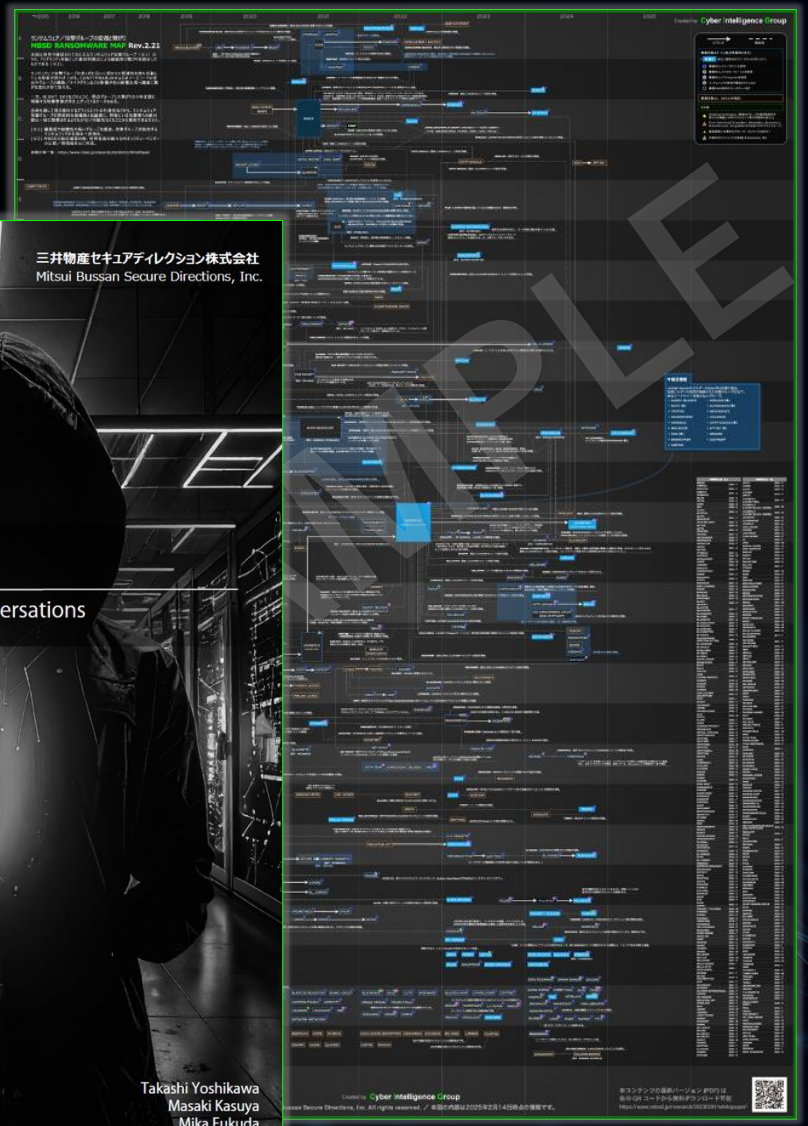
● ランサムウェア／攻撃グループの変遷と繋がり（MBSD RANSOMWARE MAP）：
https://www.mbsd.jp/research/20230201/whitepaper/

● 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

※ 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。

・ これらはあ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ありません。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/

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

Cyber Intelligence Group