CIG
Cyber Intelligence Group

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5月号 Rev 1.00
(2026年4月分)

2026
4

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

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

2026

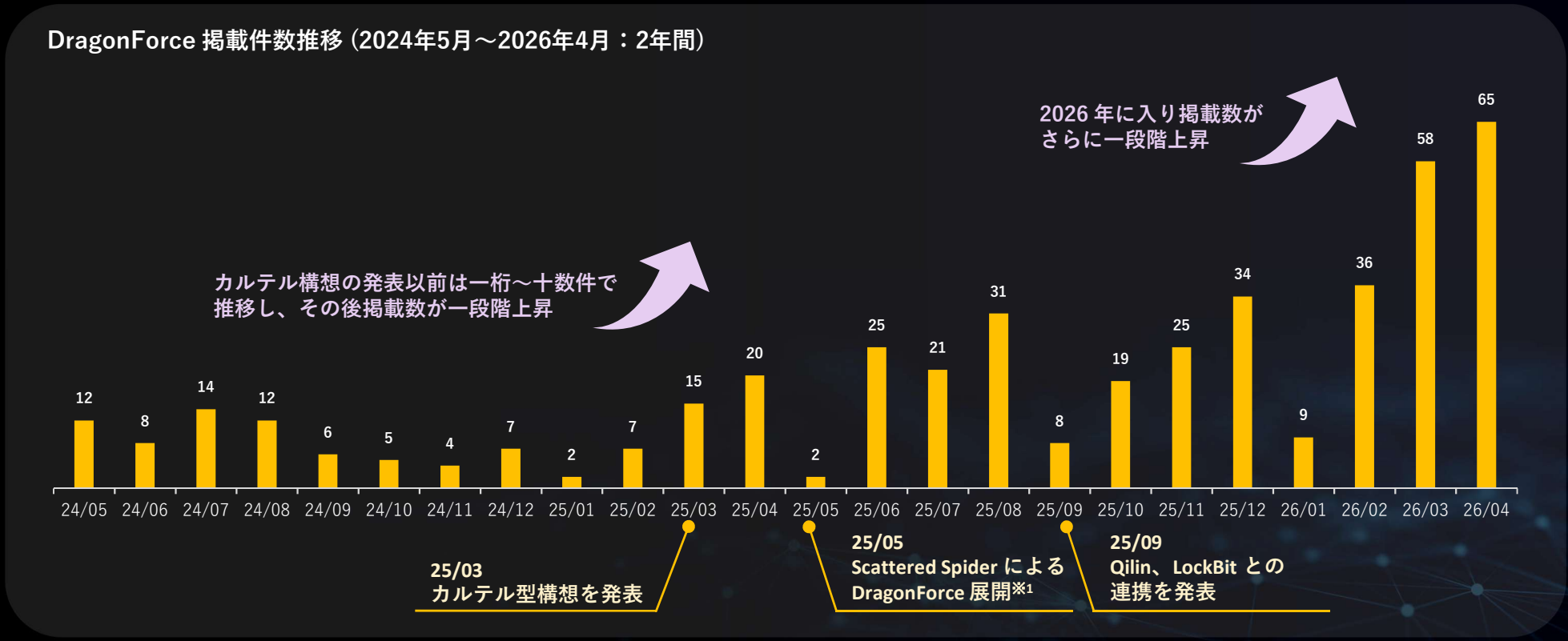
4

総括と監視対象

今月のハイライト

● DragonForceの掲載数増加：カルテル型へ移行後の推移

DragonForce は2025年3月、基盤・ツール・交渉環境・リークサイトなどを提供し、参加者が DragonForce ブランドまたは独自ブランドで活動できるカルテル型モデルの運用を開始した。この運用モデルでは、攻撃主体・使用基盤・公開ブランドが必ずしも一致しないため、DragonForce としての掲載数がどう変化するかは参加者のブランド選択に左右される。以下では、DragonForce のリークサイト掲載数について、カルテル型運用への移行後の推移を確認する。



カルテル型の構想を発表後 DragonForce のリークサイト掲載数は増加傾向にあり、2026年3月・4月には攻撃グループ別の上位3位となった。リークサイトへの掲載は被害全体の一部に過ぎないが、その範囲においては、DragonForce の活発化が見て取れる。
また、主要 RaaS である Qilin・LockBit との連携に加え、初期侵入を得意とする Scattered Spider が DragonForce を展開した事例※1も報告されている。
こうした動きは、DragonForce の認知度や活用機会を高め、アフィリエイトによる DragonForce の基盤やリークサイトの利用を後押しした可能性がある。この動向からは、基盤提供型 RaaS の拡大に伴い、攻撃グループ間の関係が一層複雑化している状況が垣間見える。

※1：https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

※ 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4月15日～2026年5月6日）

【トルコ国民を標的とした新たな「JanaWare」ランサムウェア、サイバー犯罪エコシステムの分裂に伴い出現】（出典: The Record 2026/04/15）
Acronis 社 が、トルコ居住者に限定して活動する地域特化型ランサムウェア JanaWare を報告。トルコ限定の実行条件を持ち、Adwind RAT とフィッシングメール経由で家庭や中小企業から少額身代金を要求。
https://therecord.media/new-janaware-ransomware-targeting-turkey

【Payouts King ランサムウェアが QEMU VM でエンドポイントセキュリティを回避】（出典: Sophos 2026/04/16）
Sophos が、オープンソースのエミュレータ QEMU を悪用し仮想化環境内に攻撃ツールを隠蔽する手法について報告。実際にランサムウェアグループ Payouts King のキャンペーンでの使用が確認されている。
https://www.sophos.com/en-us/blog/qemu-abused-to-evade-detection-and-enable-ransomware-delivery

【The Gentlemen ランサムウェアが、ボットネット「SystemBC」を利用した新たな攻撃手法を採用】（出典: BleepingComputer 2026/04/20）
The Gentlemen ランサムウェアは、SystemBC ボットネットをプロキシインフラとして利用し、人手による侵入・横展開に組み込むことで、ネットワーク上の Windows / Linux / ESXi 環境の短時間暗号化を実現。
https://www.bleepingcomputer.com/news/security/the-gentlemen-ransomware-now-uses-systembc-for-bot-powered-attacks/

【議員ら、病院を標的としたランサムウェア攻撃に対するテロ行為認定や殺人罪適用の可能性を検討】（出典: CyberScoop 2026/04/21）
米下院公聴会で、病院へのランサムウェア攻撃をテロ指定や連邦殺人罪の対象とする案が議論。医療機関への攻撃は2024年から2025年で倍増しており、抑止力強化と法的枠組み拡張への動きが顕在化している。
https://cyberscoop.com/lawmakers-ponder-terrorism-designations-homicide-charges-over-hospital-ransomware-attacks/

【RAMP の内部を暴く:流出したデータベースが明かすロシアのランサムウェア市場の実態】（出典: Comparitech 2026/04/22）
Comparitech 社 が RAMP フォーラムの流出データベースを分析。ロシア系ランサムウェア市場が売り手・買い手・ブローカー・採用担当に分業化したプラットフォームとして機能していた実態が示された。
https://www.comparitech.com/news/inside-ramp-what-a-leaked-database-reveals-about-russias-ransomware-marketplace/

【Kyber ランサムウェアが Windows でポスト量子暗号を試用】（出典: BleepingComputer 2026/04/22）
Rapid7 が Kyber ランサムウェアの Windows および VMware ESXi 向け亜種を確認。Windows 版ではキー保護に Kyber1024 ポスト量子暗号を導入し、ESXi 版は同様の宣伝に反し ChaCha8 と RSA-4096 を使用。
https://www.bleepingcomputer.com/news/security/kyber-ransomware-gang-toys-with-post-quantum-encryption-on-windows/

【Trigona グループ、データ窃取を効率化するため独自の情報流出ツールを展開】（出典: SECURITY.COM (Broadcom/Symantec) 2026/04/23）
Trigona ランサムウェアを用いた今年3月の侵害では、並列転送や拡張子フィルタ、通信ローテーション機能を備えた独自のデータ窃取ツールの使用が確認。公開ツールよりも秘匿性と効率性を向上させている。
https://www.security.com/threat-intelligence/trigona-exfiltration-custom

【Vect 2.0 ランサムウェア、設計上の欠陥によりワイパー化】（出典: Dark Reading 2026/04/30）
Check Point Research が VECT 2.0 の欠陥について指摘。サイズが128KB超のファイルは復号に必要な nonce を破棄する実装の欠陥により、攻撃者でも復号不能となり、実質ワイパー化していると指摘。
https://www.darkreading.com/threat-intelligence/vect-ransomware-wiper-design-error

【ロシア発の大規模ランサムウェアグループの構成員が実刑判決を受ける】（出典: 米司法省 2026/05/04）
米連邦裁は、 Conti 元幹部主導のランサムウェアグループ Karakurt などで交渉役を務めたラトビア国籍のDeniss Zolotarjovs 被告に対し、102か月の実刑判決を下した。同被告は少なくとも54社への恐喝に関与。
https://www.justice.gov/opa/pr/member-prolific-russian-ransomware-group-sentenced-prison

【痕跡の撹乱: Chaos ランサムウェアの背後に潜む国家支援型の影】（出典: Rapid7 2026/05/06）
Rapid7 は、Chaos グループに見せかけた攻撃を、コード署名証明書や C2 基盤からイラン MOIS 配下 APT MuddyWater の偽旗型サイバー攻撃と中程度の確度で関連付け、資格情報窃取と永続化手口を分析した。
https://www.rapid7.com/blog/post/tr-muddying-tracks-state-sponsored-shadow-behind-chaos-ransomware/

※ 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）：324（※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：63

※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）

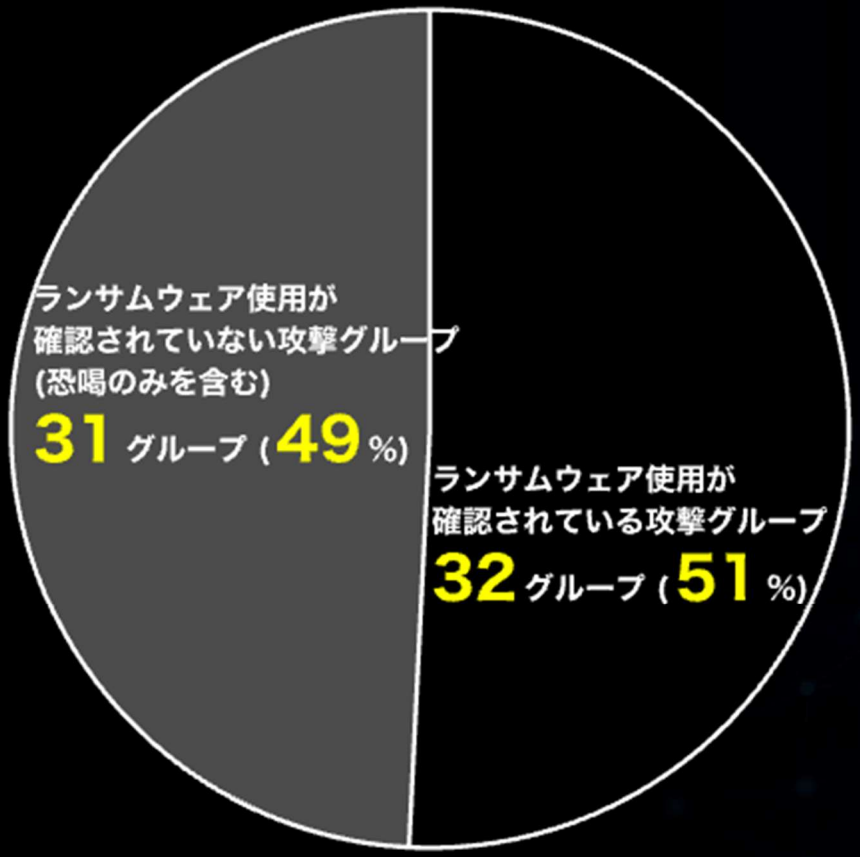
0APT
0mega (Omega)
8BASE
Abyss
AiLock
AKIRA
AKO
ALP-001
Alpha (MYDATA)
AlphV (BlackCat)
Anubis
Apos Security
APT73 (Eraleig)
ARACHNA
ARCUS MEDIA
Argonauts
Arkana
ArvinClub
Astro (Astra)
Atomsilo
● AUDIT
● Aur0ra
Avaddon
AvosLocker
AWARE
Axxes
AzzaSec
Babuk
Babuk (2025)
BASHE
BEAST
Benzona
BERT
BianLian
BL0ODY (BLOODY)
Bl4ckt0r (BlackTor)
Black Basta
BlackByte
BlackDolphin
BlackField
BlackLock
BlackMatter
Black Nevas
Blackout
BLACKSHRANTAC
BlackSuit
● BLACKWATER
BLUEBOX
BLUESKY
BQTLOCK
Brain Cipher
BRAVOX
Brotherhood
BULLY
Business Data Leaks
CACTUS
Cephalus
CHAOS (2025)
CHEERS
ChileLocker (Arcrypter)
CHORT
Cicada3301
CiphBit
CipherForce
CipherLocker
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
EXITIUM
FOG
Frag
FSOCIETY / FLOCKER
FSTeam
FulcrumSec
Funksec
GD LockerSec
Genesis
GLOBAL
Grief
Groove
Gunra / Fresh Gunra
HANDARA [Hacktivist]
Haron
HELLCAT
Helldown
HelloGookie
Hitler (AGL0BGVYCG)
Hive
HolyGhost
Hotarus
Hunters International
● HYFLOCK
ICEFIRE
IMN Crew
INC Ransom
Insane
INSOMNIA
INTERLOCK
J GROUP
KAIROS
Karakurt
Karma
Kawa4096
Kazu
KILLSEC
Kittykatkrew
Knight
Kraken (HelloKitty)
● KRYBIT
Kryptos
Kyber
● LAMASHTU
LAMBDA
La Piovra
LAPSUS$
LAPSUS$ Group
LeakedData (Silent Ransom Group)
LEAKNET
LILITH
Linkc
LockBit
LOKI
Lorenz
LostTrust
LunaLock
LV
LYNX
● M3RX
MADCAT
MAD LIBERATOR
MALAS
MalekTeam
Mallox
Mamona RIP
MBC
Medusa
MEDUZA LOCKER
MEOW
Metaencryptor
Midas
MIGA
Mindware
Minteye
● MNT6
Mogilevich [fraud]
MOISHA
Money Message
Monti
Morpheus
Mount Locker
MS13-089
N3tw0rm (NetWorm)
N4UGHTYSEC (NAUGHTYSEC)
NASIR SECUTRIY
Nefilim
NetRunner
Nevada
NightSky
NightSpire
NITROGEN
NoEscape
Nokoyawa
NONAME (VFOKX)
NONAME [2023年確認]
Nova
NULLBULGE
Obscura
Obscura 2.0
Onyx
Orca
Orion Leaks
OSIRIS PROJECT
Pandora
Pay2Key
Payload
Payload.bin
Payouts King
PEAR
PLAY
PLAYBOY
● PRINZ EUGEN
Prometheus
PRYX
PUTIN TEAM
Pysa / Mespinoza
Qilin (Agenda)
QIULONG
Quantum
RABBIT HOLE
RADAR
RADIANT
Ragnar Locker
Ragnarok
RA GROUP
RALord
Rancoz
RansomBay
Ransom Cartel
Ransom Corp
RANSOMCORTEX
Ransomed.vc
Ransom EXX
RansomHouse
RansomHub
Ransomware Blog
Ranzy
RA WORLD
Raznatovic
RedAlert (N13V)
Red Ransomware Group (Red CryptoApp)
Relic
Revil (Sodinokibi)
Reynolds
Rhysida
Risen
ROOK
root
Royal
Rransom
RunSomeWares
Rusty Locker
Sabbath (54bb47h)
SAFEPAY
SARCOMA
SATAN LOCK
SATANLOCK V2
Scattered LAPSUS$ Hunters
Secp0
Securotrop
SenSayQ
SHADOWBYT3$
shaoleaks
SHINYHUNTERS
Sicarii
SIEGEDSEC
Silent
Sinobi
SKIRA TEAM
SLUG
Snatch
Solidbit
Space Bears
Sparta
Spook
STORMOUS
Sugar
Suncrypt
SynACK
TeamXXX
TENGU
Termite
The Gentlemen
THE GREEN BLOOD GROUP
ThreeAM (3AM)
● TIMC
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
XP95
Yanluowang
Yurei
Zeon
Zero Tolerance

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

監視中のランサムウェア攻撃グループ情報
（ランサムウェア使用の割合）

●現在活動中の攻撃グループにおけるランサムウェア使用の割合（2026年 4月）

（※当月にリークサイト掲載を確認した攻撃グループ全 63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4月に活動中である事が確認された全63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

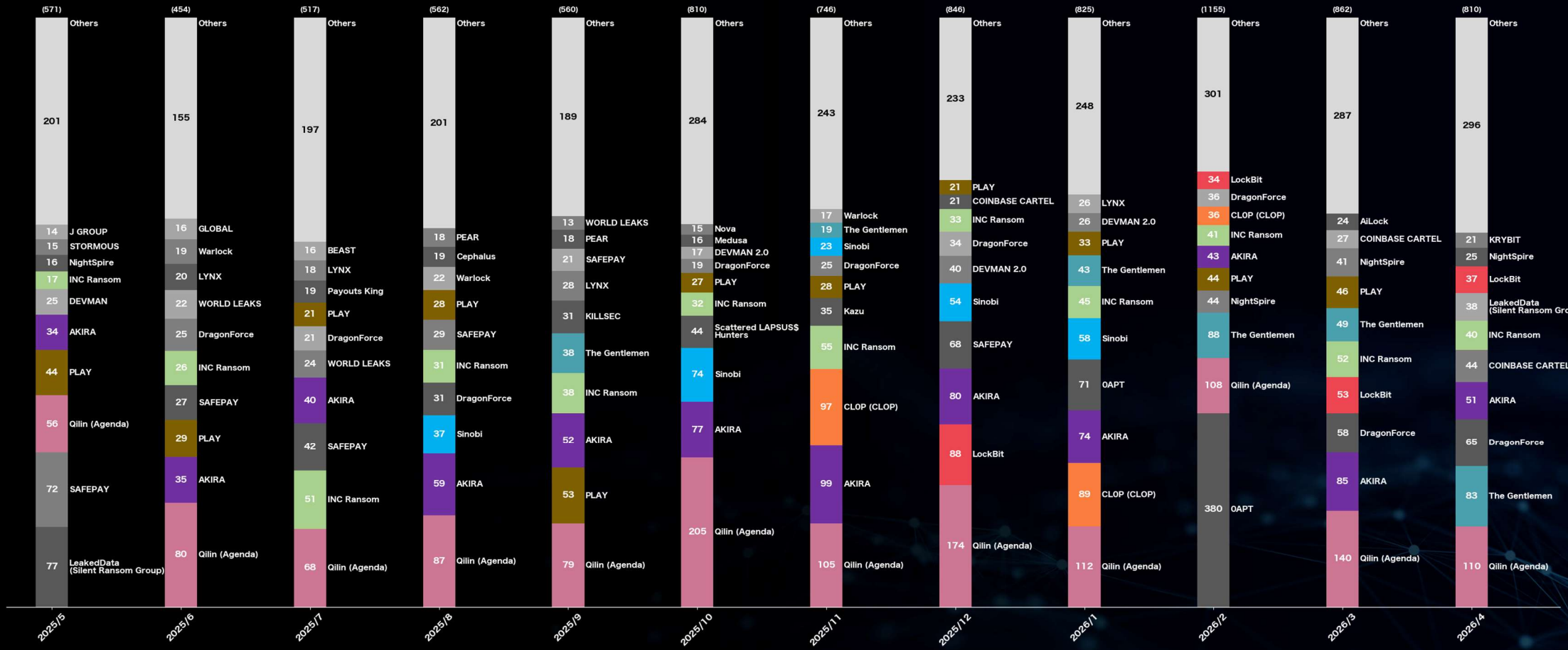
年間 統計
（全世界）

2026

4

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5月～2026年4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

4

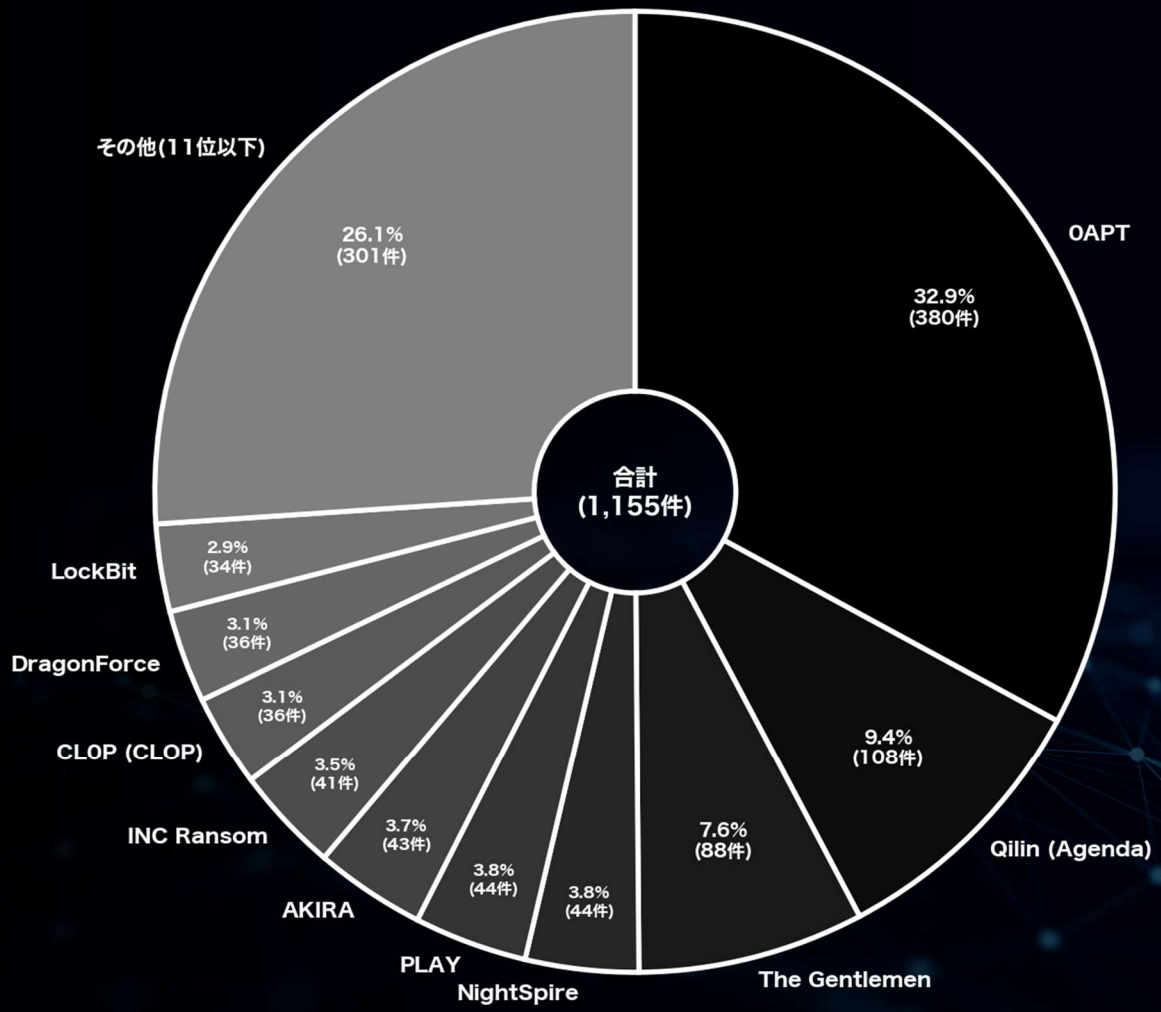
月別内訳 攻撃グループ TOP10（全世界）

（2026年 2 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)
0APT	380	32.9	+ 309
Qilin (Agenda)	108	9.4	- 4
The Gentlemen	88	7.6	+ 45
NightSpire	44	3.8	+ 23
PLAY	44	3.8	+ 11
AKIRA	43	3.7	- 31
INC Ransom	41	3.5	- 4
CL0P (CLOP)	36	3.1	- 53
DragonForce	36	3.1	+ 27
LockBit	34	2.9	+ 23

▼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

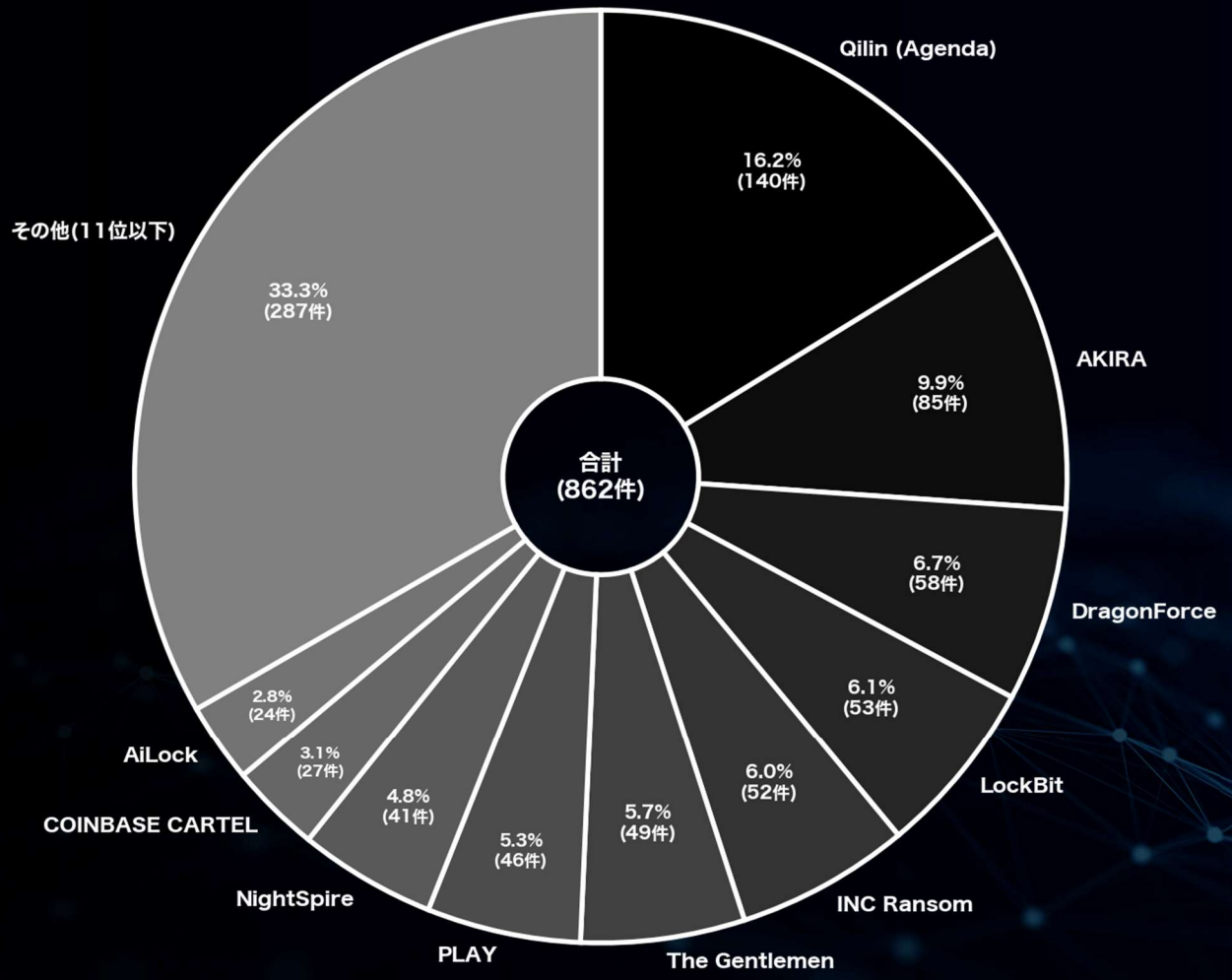
月別内訳 攻撃グループ TOP10（全世界）

（2026年 3 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)	140	16.2	+ 32
AKIRA	85	9.9	+ 42
DragonForce	58	6.7	+ 22
LockBit	53	6.1	+ 19
INC Ransom	52	6.0	+ 11
The Gentlemen	49	5.7	- 39
PLAY	46	5.3	+ 2
NightSpire	41	4.8	- 3
COINBASE CARTEL	27	3.1	+ 17
AiLock	24	2.8	+ 24

▼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

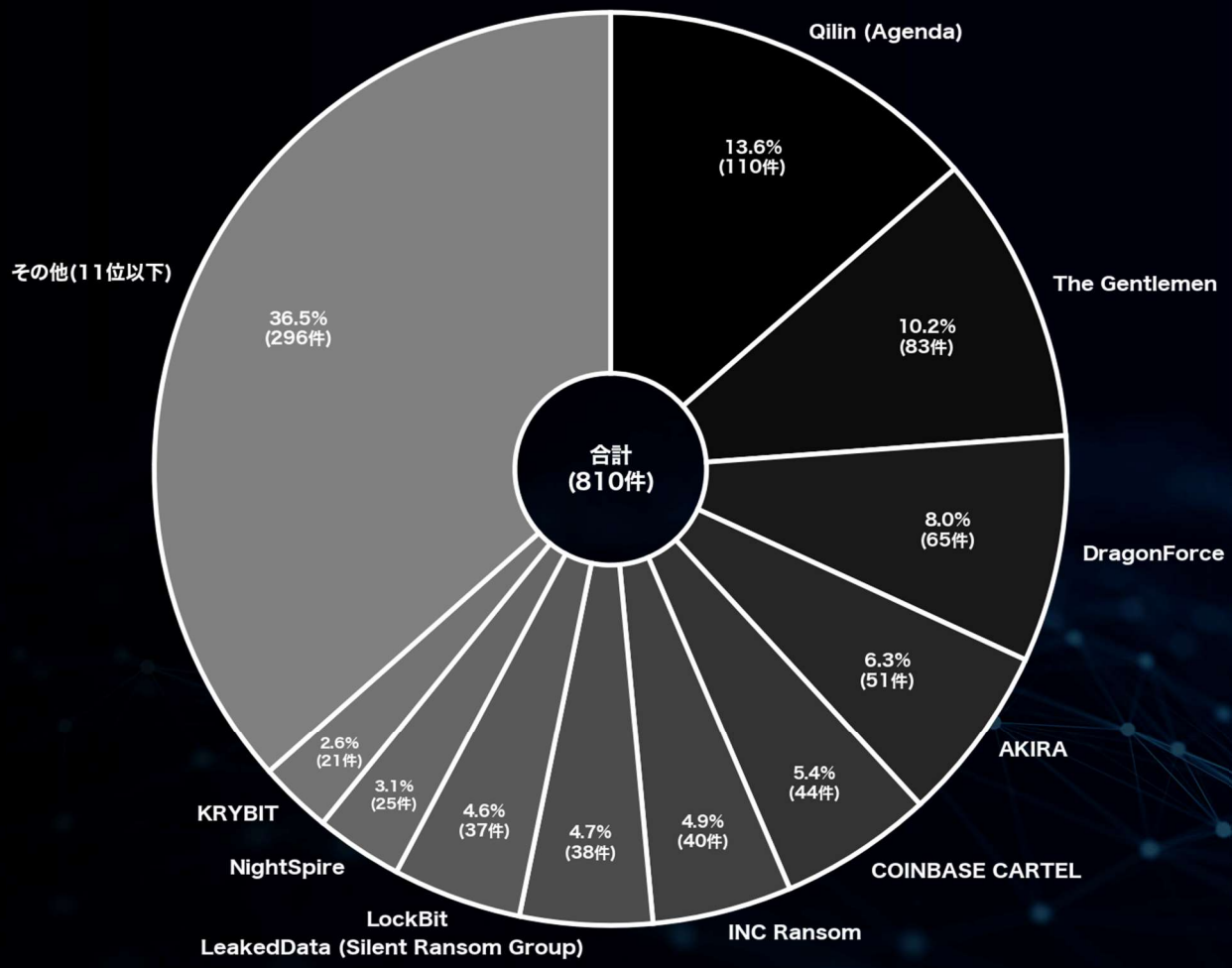
月別内訳 攻撃グループ TOP10（全世界）

（2026年 4 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)	110	13.6	- 30
The Gentlemen	83	10.2	+ 34
DragonForce	65	8.0	+ 7
AKIRA	51	6.3	- 34
COINBASE CARTEL	44	5.4	+ 17
INC Ransom	40	4.9	- 12
LeakedData (Silent Ransom Group)	38	4.7	+ 23
LockBit	37	4.6	- 16
NightSpire	25	3.1	- 16
KRYBIT	21	2.6	+ 21

▼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

4

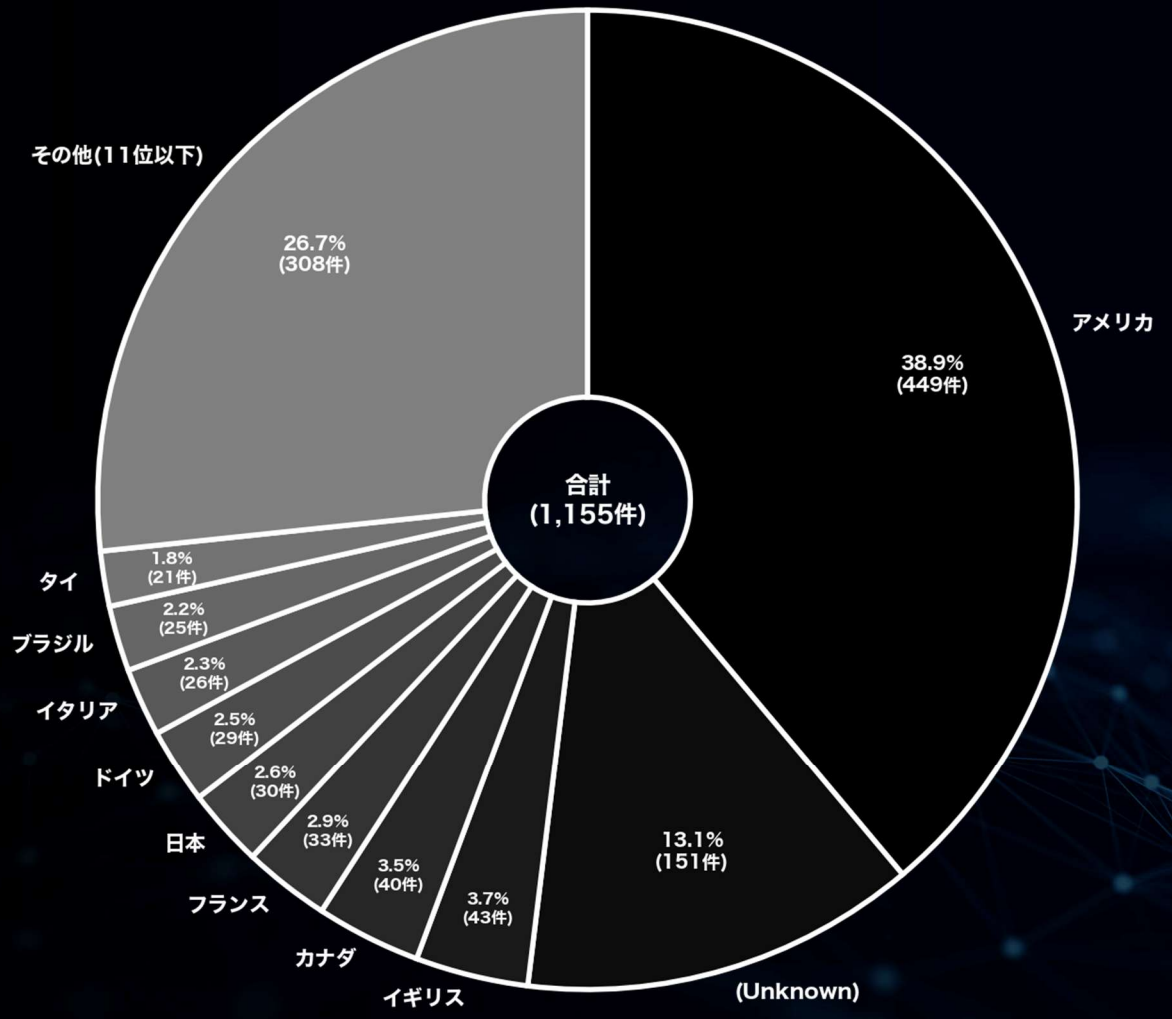
月別内訳 被害国TOP10（全世界）

（2026年 2 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	449	38.9	+ 55
(Unknown)	151	13.1	+ 109
イギリス	43	3.7	- 1
カナダ	40	3.5	± 0
フランス	33	2.9	+ 19
日本	30	2.6	+ 25
ドイツ	29	2.5	+ 4
イタリア	26	2.3	+ 4
ブラジル	25	2.2	+ 13
タイ	21	1.8	+ 11

▼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

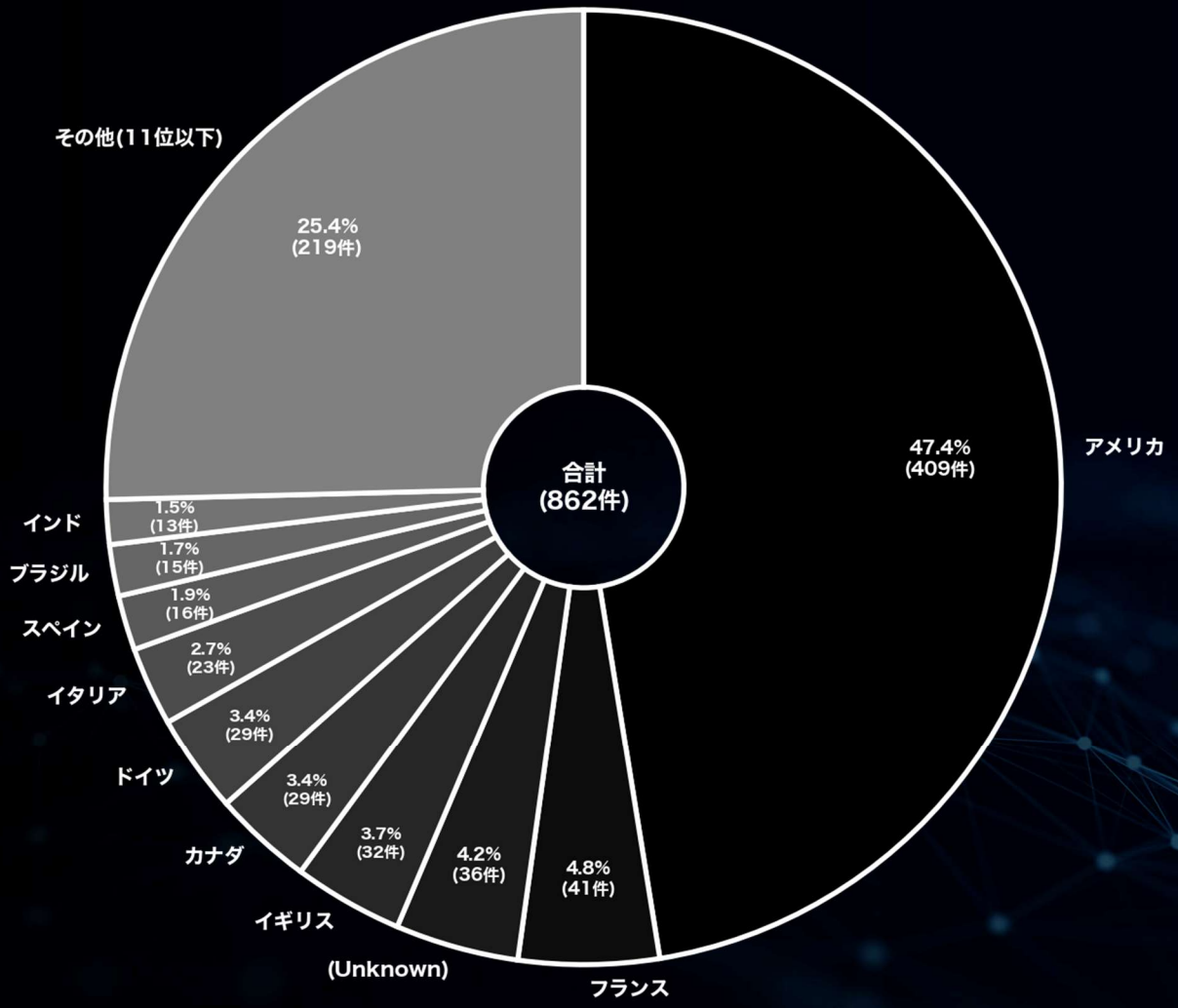
月別内訳 被害国TOP10（全世界）

（2026年 3 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	409	47.4	- 40
フランス	41	4.8	+ 8
(Unknown)	36	4.2	- 115
イギリス	32	3.7	- 11
カナダ	29	3.4	- 11
ドイツ	29	3.4	± 0
イタリア	23	2.7	- 3
スペイン	16	1.9	+ 3
ブラジル	15	1.7	- 10
インド	13	1.5	- 4

▼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

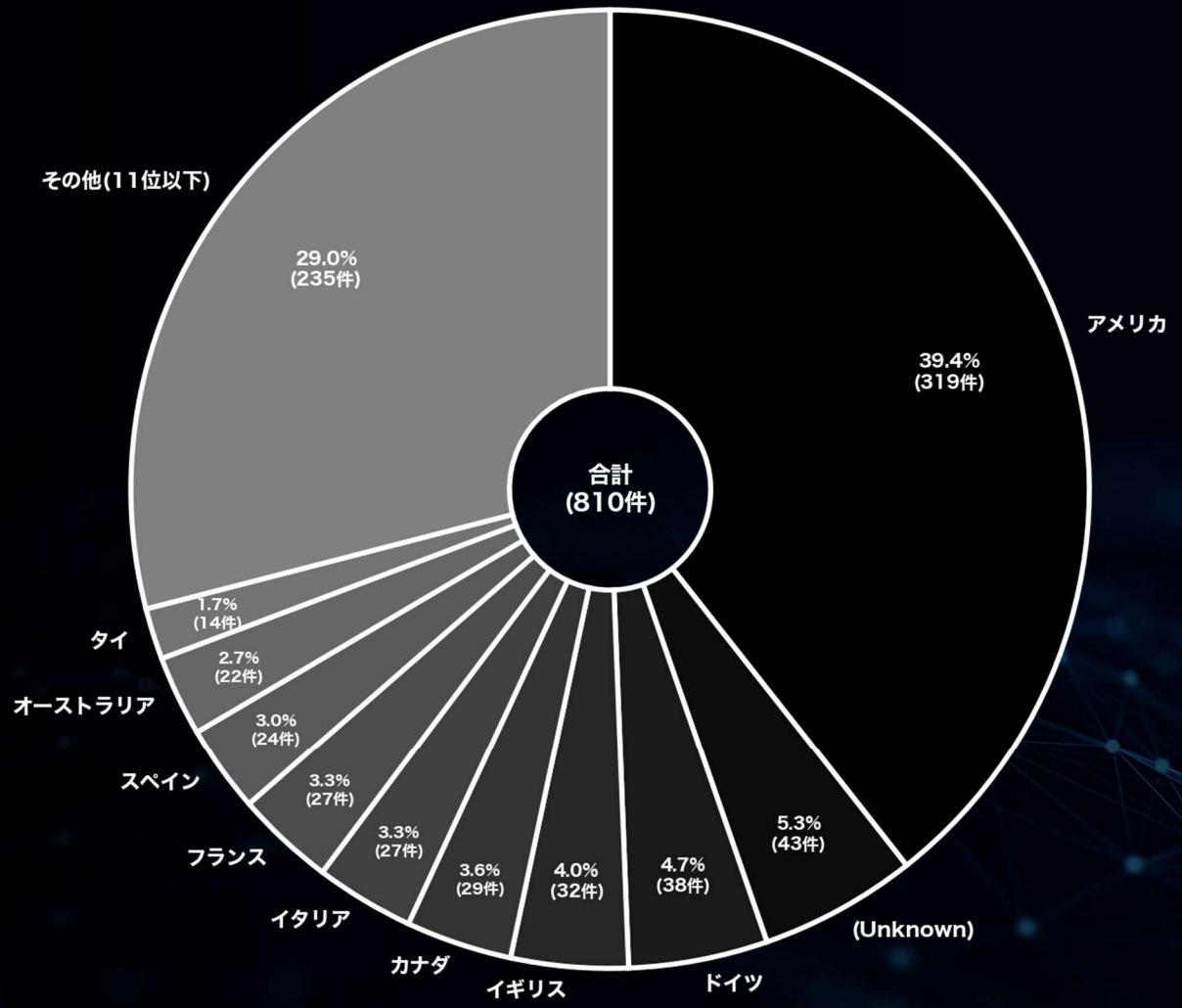
月別内訳 被害国TOP10（全世界）

（2026年 4 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	319	39.4	- 90
(Unknown)	43	5.3	+ 7
ドイツ	38	4.7	+ 9
イギリス	32	4.0	± 0
カナダ	29	3.6	± 0
イタリア	27	3.3	+ 4
フランス	27	3.3	- 14
スペイン	24	3.0	+ 8
オーストラリア	22	2.7	+ 12
タイ	14	1.7	+ 4

▼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

4

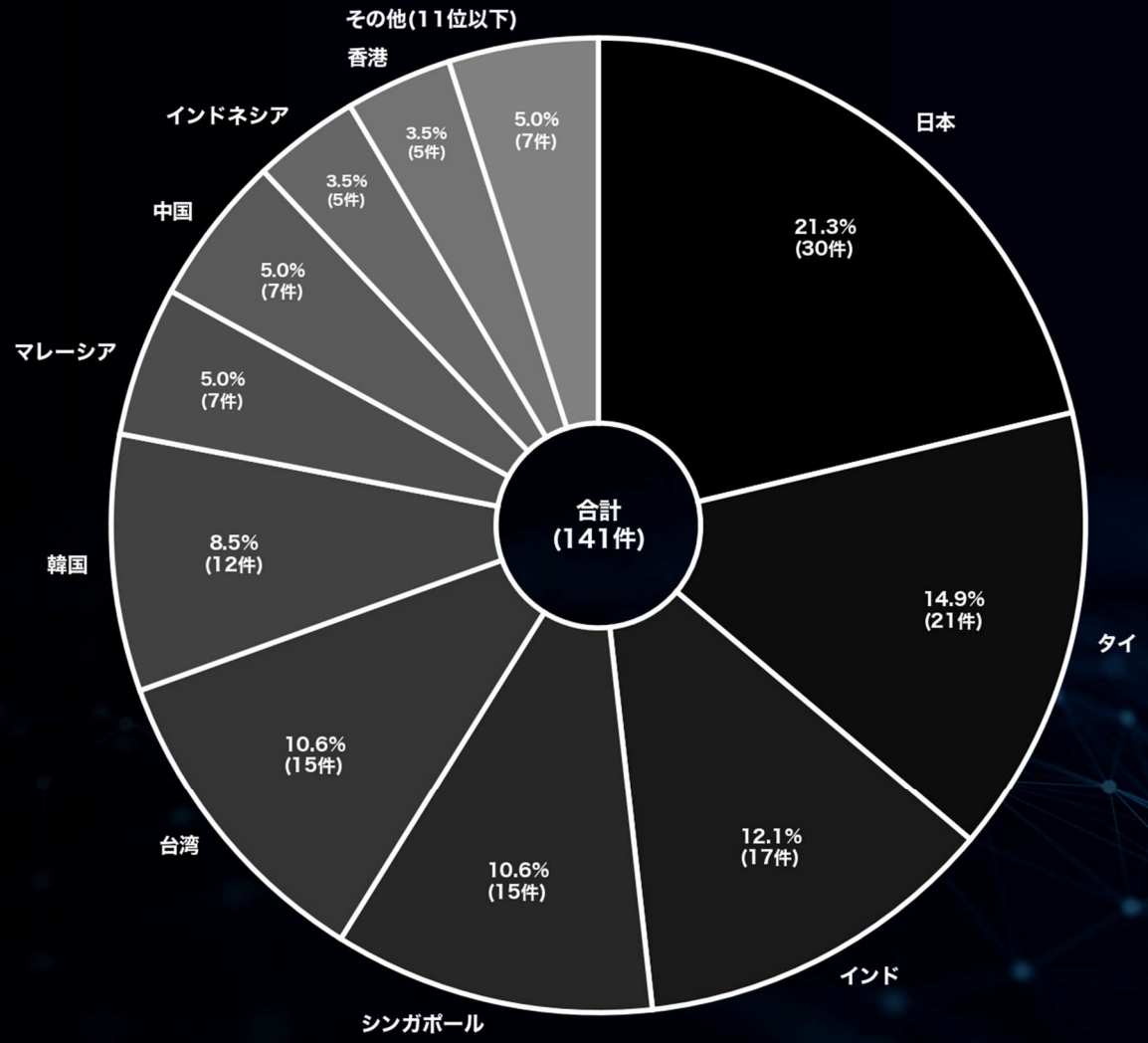
月別内訳 被害国TOP10（アジア）

（2026年 2 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)
日本	30	21.3	+ 25
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	12	8.5	+ 10
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

▼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

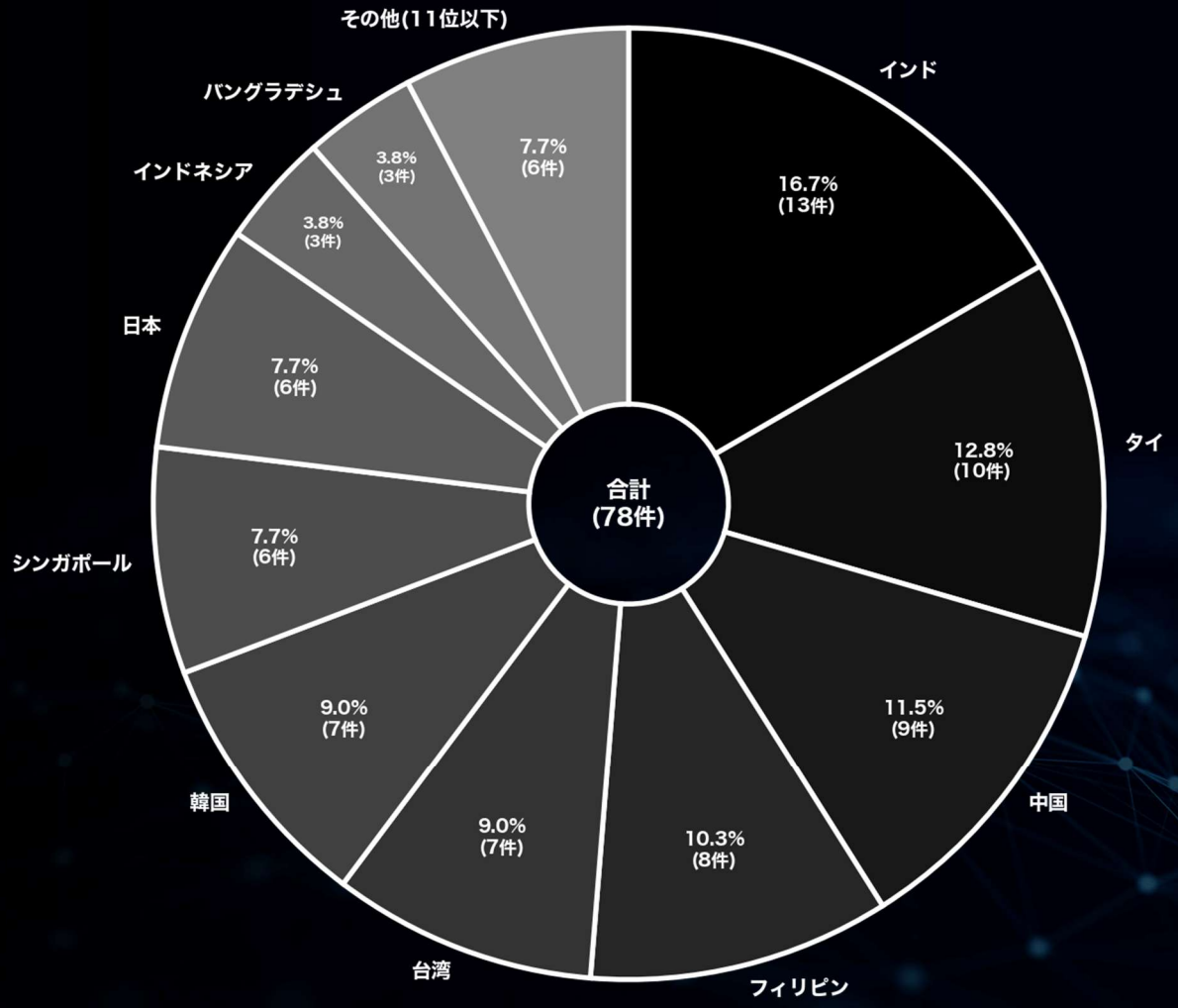
月別内訳 被害国TOP10（アジア）

（2026年 3 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	13	16.7	- 4
タイ	10	12.8	- 11
中国	9	11.5	+ 2
フィリピン	8	10.3	+ 5
台湾	7	9.0	- 8
韓国	7	9.0	- 5
シンガポール	6	7.7	- 9
日本	6	7.7	- 24
インドネシア	3	3.8	- 2
バングラデシュ	3	3.8	+ 3

▼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

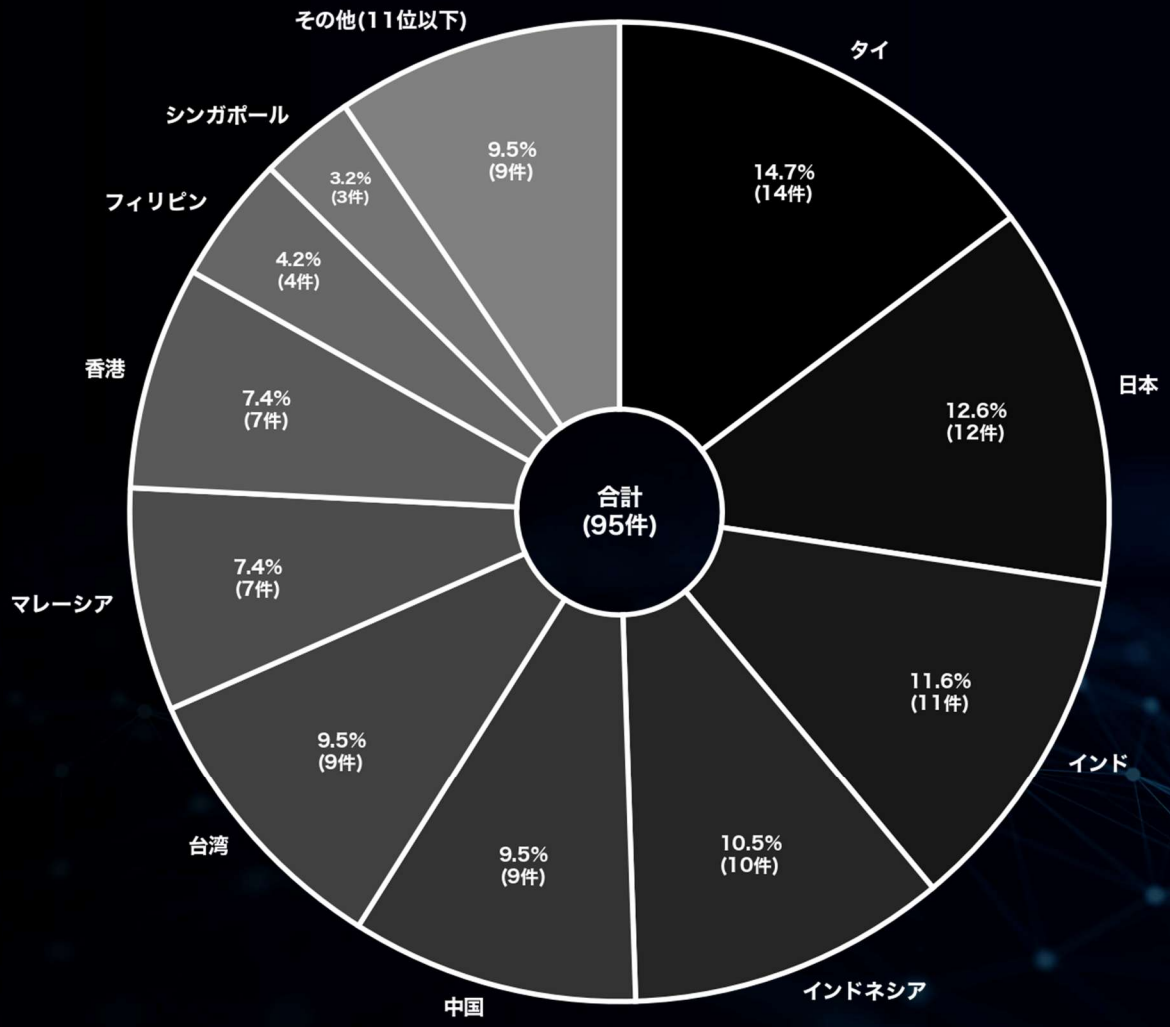
月別内訳 被害国TOP10（アジア）

（2026年 4 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)
タイ	14	14.7	+ 4
日本	12	12.6	+ 6
インド	11	11.6	- 2
インドネシア	10	10.5	+ 7
中国	9	9.5	± 0
台湾	9	9.5	+ 2
マレーシア	7	7.4	+ 5
香港	7	7.4	+ 5
フィリピン	4	4.2	- 4
シンガポール	3	3.2	- 3

▼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（全世界） 月別統計（過去3ヶ月分）

2026

4

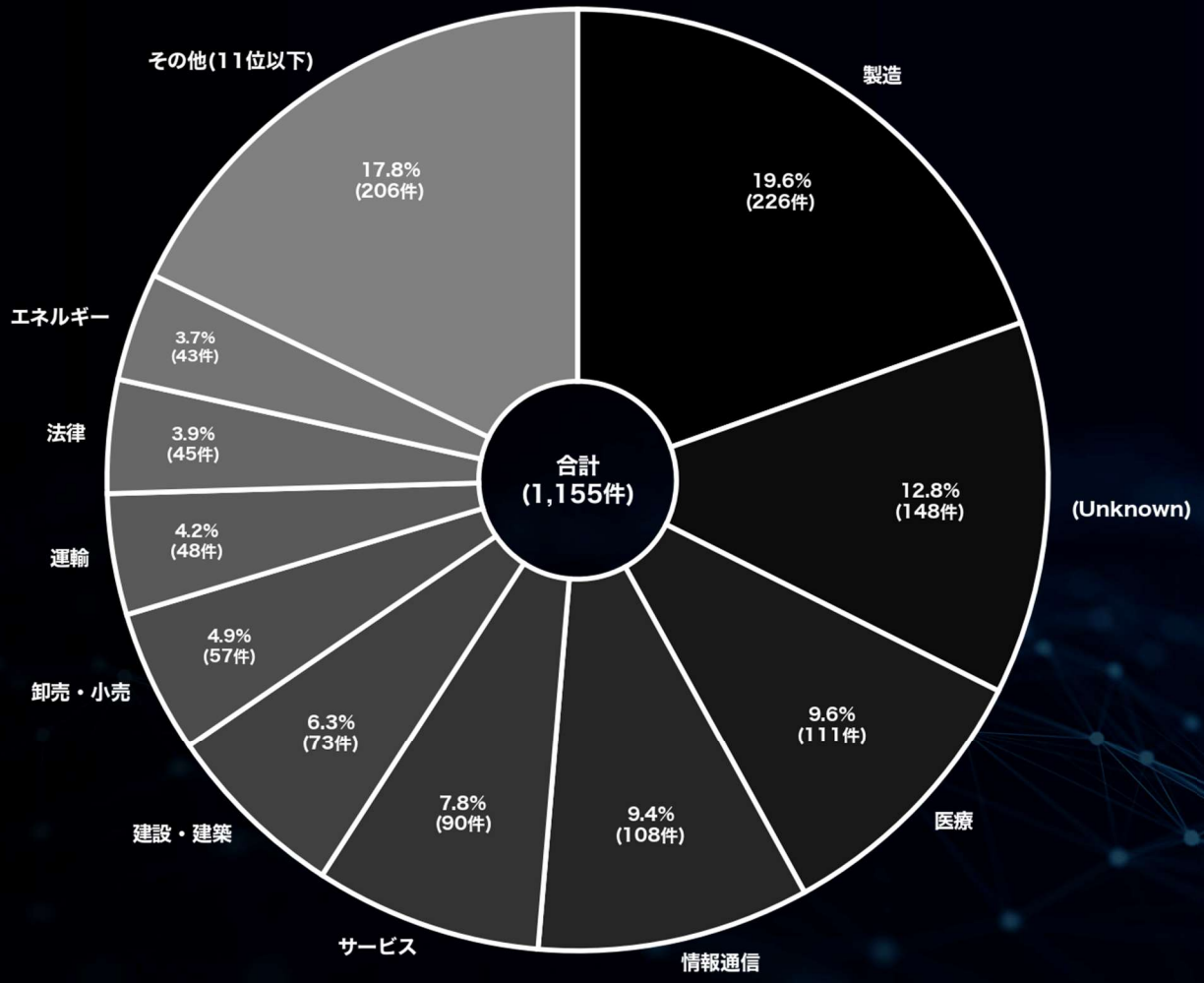
月別内訳 業種 TOP10（全世界）

（2026年 2 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	226	19.6	+ 84
(Unknown)	148	12.8	+ 105
医療	111	9.6	+ 57
情報通信	108	9.4	+ 9
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
法律	45	3.9	+ 4
エネルギー	43	3.7	+ 16

▼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

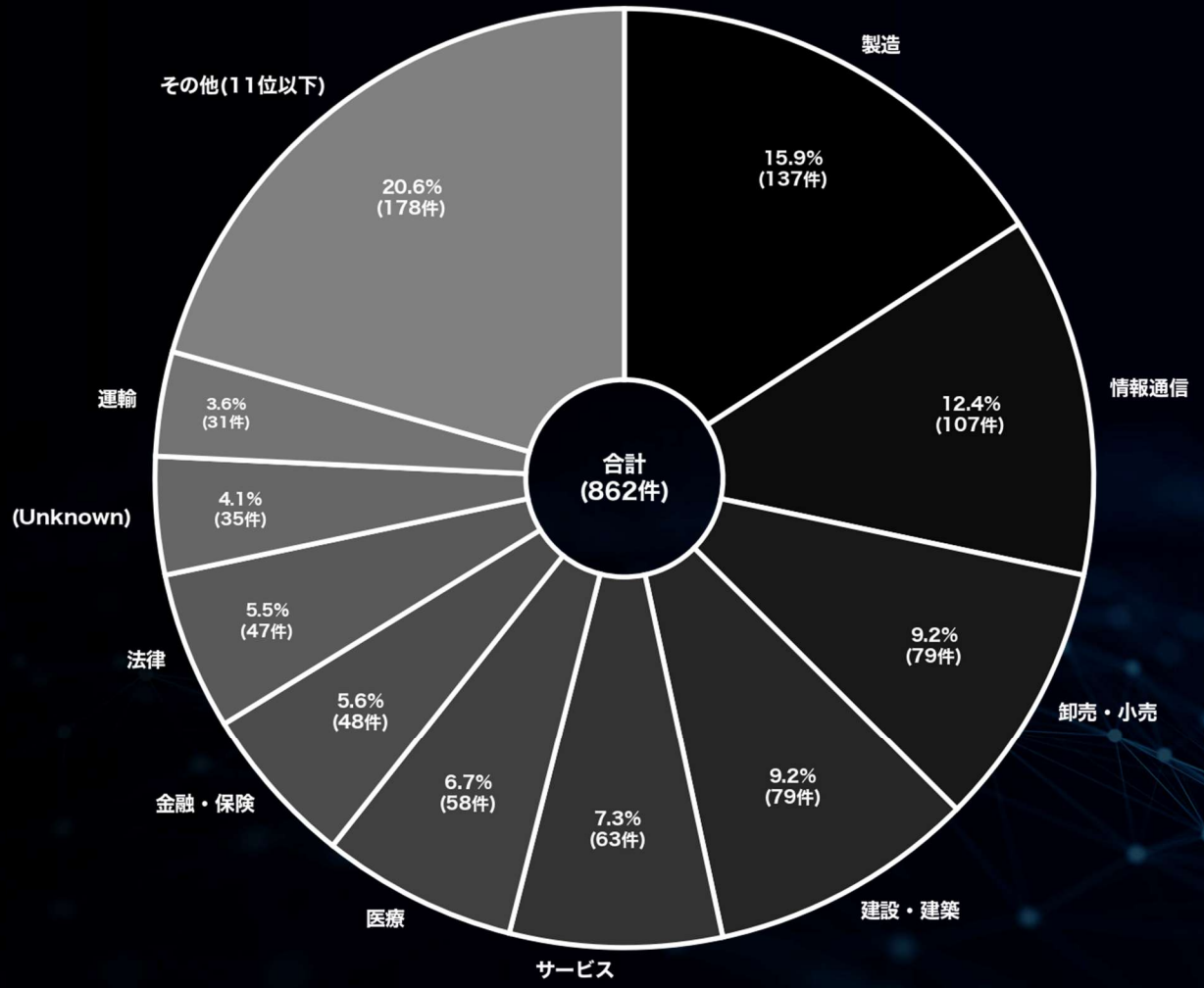
月別内訳 業種 TOP10（全世界）

（2026年 3 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	137	15.9	- 89
情報通信	107	12.4	- 1
卸売・小売	79	9.2	+ 22
建設・建築	79	9.2	+ 6
サービス	63	7.3	- 27
医療	58	6.7	- 53
金融・保険	48	5.6	+ 10
法律	47	5.5	+ 2
(Unknown)	35	4.1	- 113
運輸	31	3.6	- 17

▼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

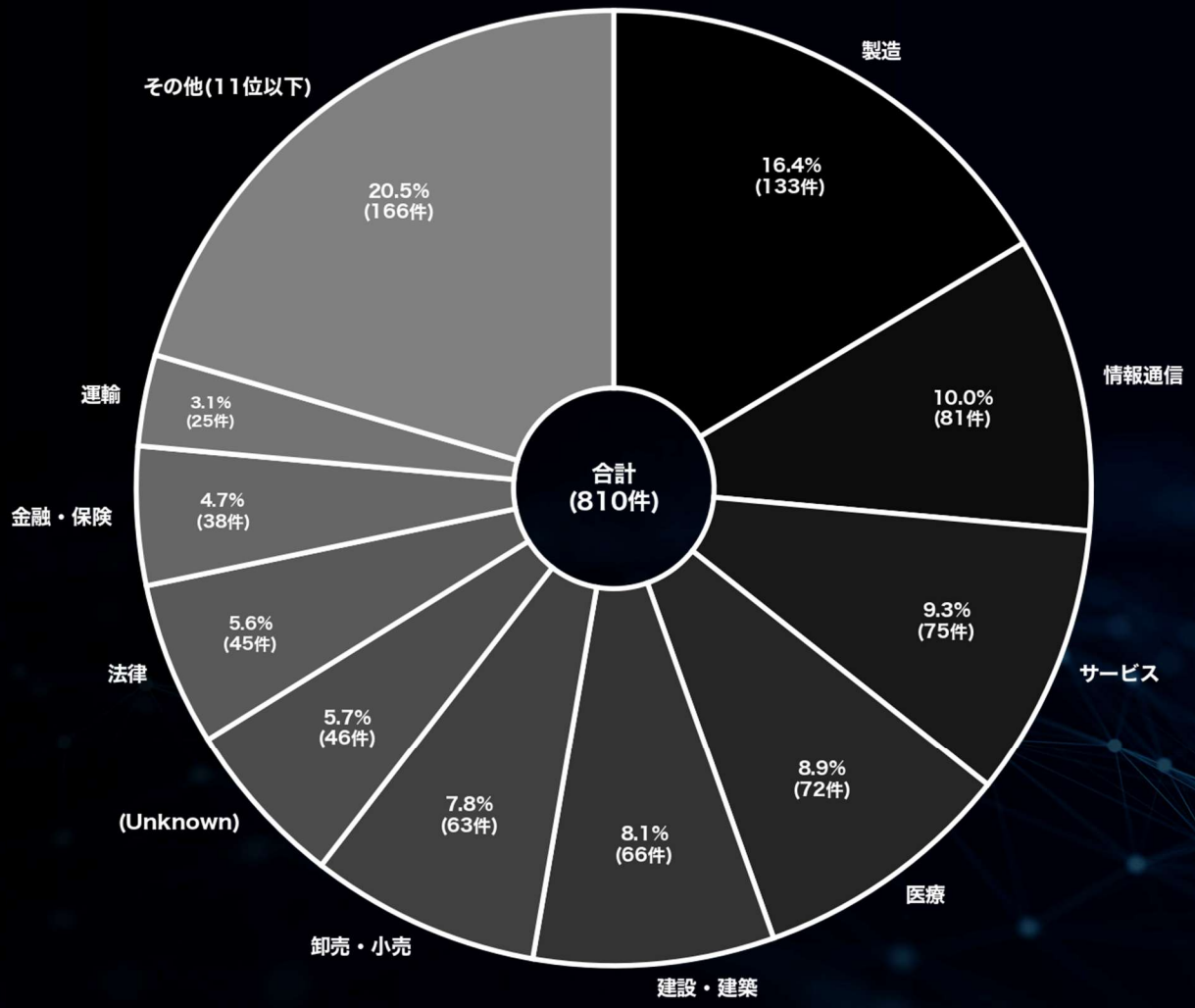
月別内訳 業種 TOP10（全世界）

（2026年 4 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	133	16.4	- 4
情報通信	81	10.0	- 26
サービス	75	9.3	+ 12
医療	72	8.9	+ 14
建設・建築	66	8.1	- 13
卸売・小売	63	7.8	- 16
(Unknown)	46	5.7	+ 11
法律	45	5.6	- 2
金融・保険	38	4.7	- 10
運輸	25	3.1	- 6

▼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

被害数の推移に関する統計
（全世界及び国内）

2026

4

被害数の推移（全世界及び国内）
（過去2年間／2024年5月～2026年4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)
2024/5	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	20	4	1
2025/4	540	21	1	0
2025/5	576	14	0	3
2025/6	460	8	0	1
2025/7	520	12	1	0
2025/8	567	16	3	0
2025/9	563	10	1	1
2025/10	814	17	2	0
2025/11	752	19	3	0
2025/12	850	20	4	0
2026/1	833	13	2	0
2026/2	1161	37	2	4
2026/3	870	14	0	2
2026/4	817	19	1	1
合計	15626	379	33	15

▼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

2026

4

資本金別の統計
（国内）

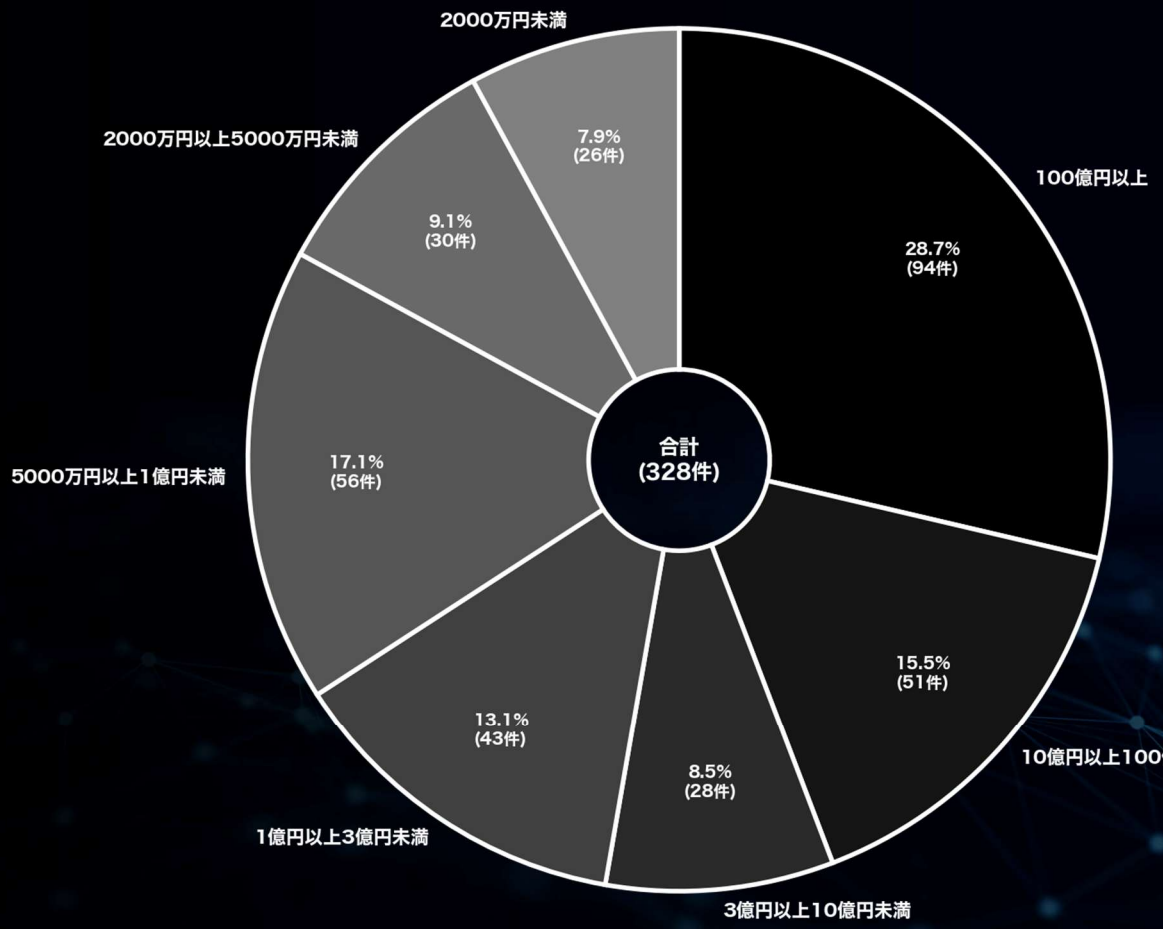
資本金別（国内）
（過去2年間／2024年5月～2026年4月）

※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	94	28.7
10億円以上100億円未満	51	15.5
3億円以上10億円未満	28	8.5
1億円以上3億円未満	43	13.1
5000万円以上1億円未満	56	17.1
2000万円以上5000万円未満	30	9.1
2000万円未満	26	7.9

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

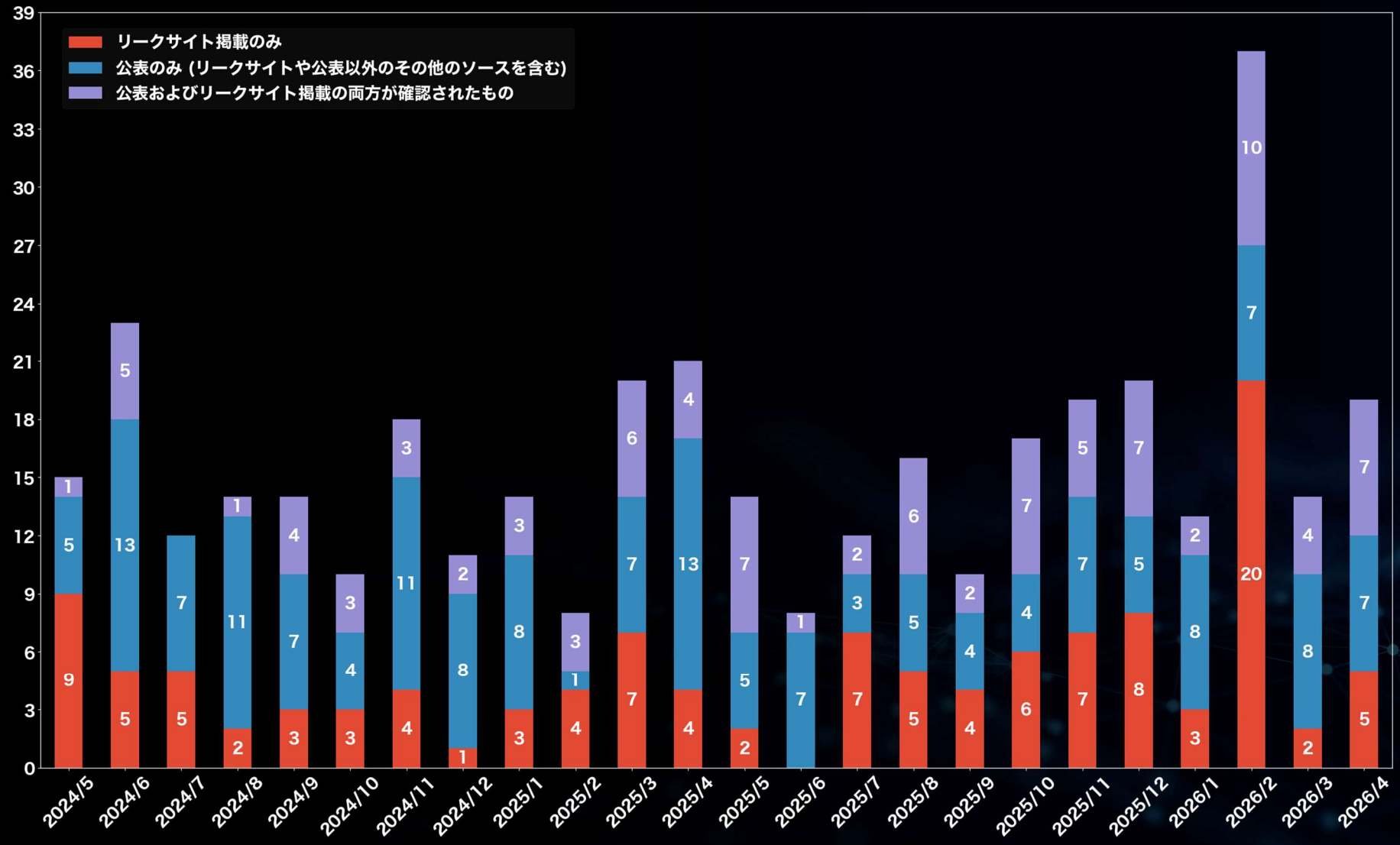
2026

4

公表と暴露に関する統計
（国内）

公表割合 月別内訳（国内）
（過去2年間／2024年5月～2026年4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

4

公となった国内被害組織概要一覧（国内）

（過去1年間／2025年5月～2026年4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
2025/5	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)
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
2025/11	(Unknown)	国際総合検定機関
2025/12	(Unknown)	エレクトロニクス専門商社(海外拠点)
2025/12	(Unknown)	教育系ITサービス提供
2025/12	AKIRA	食用油脂メーカー(海外拠点)
2025/12	Payouts King	プラスチック精密工業部品メーカー(海外拠点)

（※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5月～2026年4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
2025/12	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	(Unknown)	不動産管理
2026/1	Orion Leaks	タイヤメーカー(海外拠点)
2026/1	(Unknown)	飲料メーカー
2026/1	(Unknown)	スポーツ教室
2026/1	The Gentlemen	産業廃棄物処理
2026/1	Brain Cipher	システムインテグレーター
2026/2	Qilin (Agenda)	特殊金属材料・製造
2026/2	Everest	機械器具製造
2026/2	Everest	金属加工メーカー
2026/2	(Unknown)	大手化学素材メーカー(海外拠点)

被害月	攻撃グループ	業種概要
2026/2	0APT	大手電気機器メーカー
2026/2	0APT	大手テクノロジー企業
2026/2	0APT	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	0APT	医療機器メーカー
2026/2	0APT	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	0APT	タイヤメーカー
2026/2	0APT	総合電機メーカー
2026/2	0APT	大手自動車メーカー
2026/2	0APT	建設機械メーカー
2026/2	0APT	総合電機メーカー
2026/2	(Unknown)	ソフトウェア開発
2026/2	Qilin (Agenda)	総合デベロッパー
2026/2	NetRunner	総合病院
2026/2	(Unknown)	ホテル業・飲食店業
2026/2	0APT	鉄道会社
2026/2	0APT	地方自治体
2026/2	0APT	電力会社
2026/2	0APT	地方自治体
2026/2	Qilin (Agenda)	種苗メーカー兼商社(海外拠点)
2026/2	NightSpire	繊維・衣料関連卸売業
2026/2	(Unknown)	半導体試験装置メーカー
2026/2	NetRunner	総合病院
2026/2	LockBit	機械・工具メーカー(海外拠点)
2026/2	BLACKSHRANTAC	紳士服・婦人服販売
2026/2	NightSpire	モータースポーツチーム運営
2026/2	(Unknown)	印刷会社
2026/2	INC Ransom	石油製品・LPガス販売
2026/2	The Gentlemen	材料加工装置メーカー
2026/2	Everest	商用車メーカー

被害月	攻撃グループ	業種概要
2026/3	(Unknown)	市場調査・コンサルティング
2026/3	NetRunner	療養型病院
2026/3	(Unknown)	工業用ゴム・樹脂・配管資材商社
2026/3	(Unknown)	住宅・商業施設向けリペア
2026/3	(Unknown)	美容クリニック
2026/3	(Unknown)	シティホテル運営
2026/3	The Gentlemen	医療・看護専門出版社
2026/3	Space Bears	介護・カラオケ・飲食事業
2026/3	(Unknown)	光半導体デバイスメーカー(海外拠点)
2026/3	WORLD LEAKS	広告・制作
2026/3	The Gentlemen	繊維加工・食品加工メーカー
2026/3	(Unknown)	設備工事
2026/3	(Unknown)	美容室向け化粧品メーカー
2026/3	ALP-001	国立研究開発法人
2026/4	AKIRA	流体システム製品メーカー
2026/4	(Unknown)	非鉄金属・資源開発(海外拠点)
2026/4	(Unknown)	システムインテグレーター
2026/4	KRYBIT	酒類製造業
2026/4	LockBit	水処理・環境設備
2026/4	DragonForce	オフィス家具メーカー(海外拠点)
2026/4	(Unknown)	診療予約システム開発
2026/4	Qilin (Agenda)	舗装・土木工事
2026/4	The Gentlemen	電気機器メーカー
2026/4	Qilin (Agenda)	建設資材・福祉用具のレンタル・販売
2026/4	(Unknown)	ロボットシステムインテグレーター
2026/4	(Unknown)	生活協同組合
2026/4	COINBASE CARTEL	大学研究会
2026/4	Ransom EXX	ソフトウェア開発
2026/4	LockBit	電子部品(コネクタ)製造(海外拠点)
2026/4	(Unknown)	二輪用品専門チェーン
2026/4	The Gentlemen	ソフトウェア開発
2026/4	(Unknown)	紙器製造
2026/4	Qilin (Agenda)	大手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）

公となった国内被害組織における拠点割合（国内）

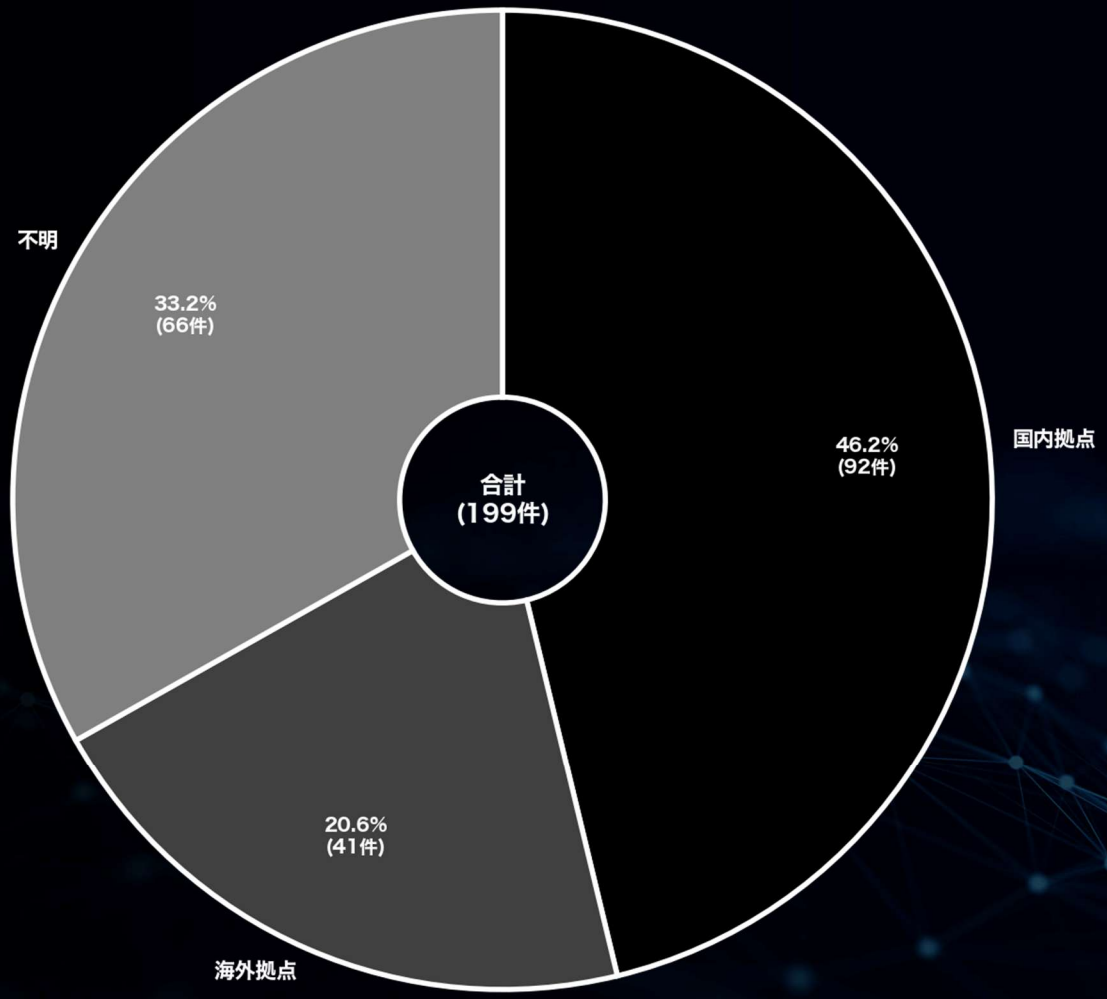
（過去1年間／2025年5月～2026年4月）

（※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	92	46.2
海外拠点	41	20.6
不明	66	33.2

▼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



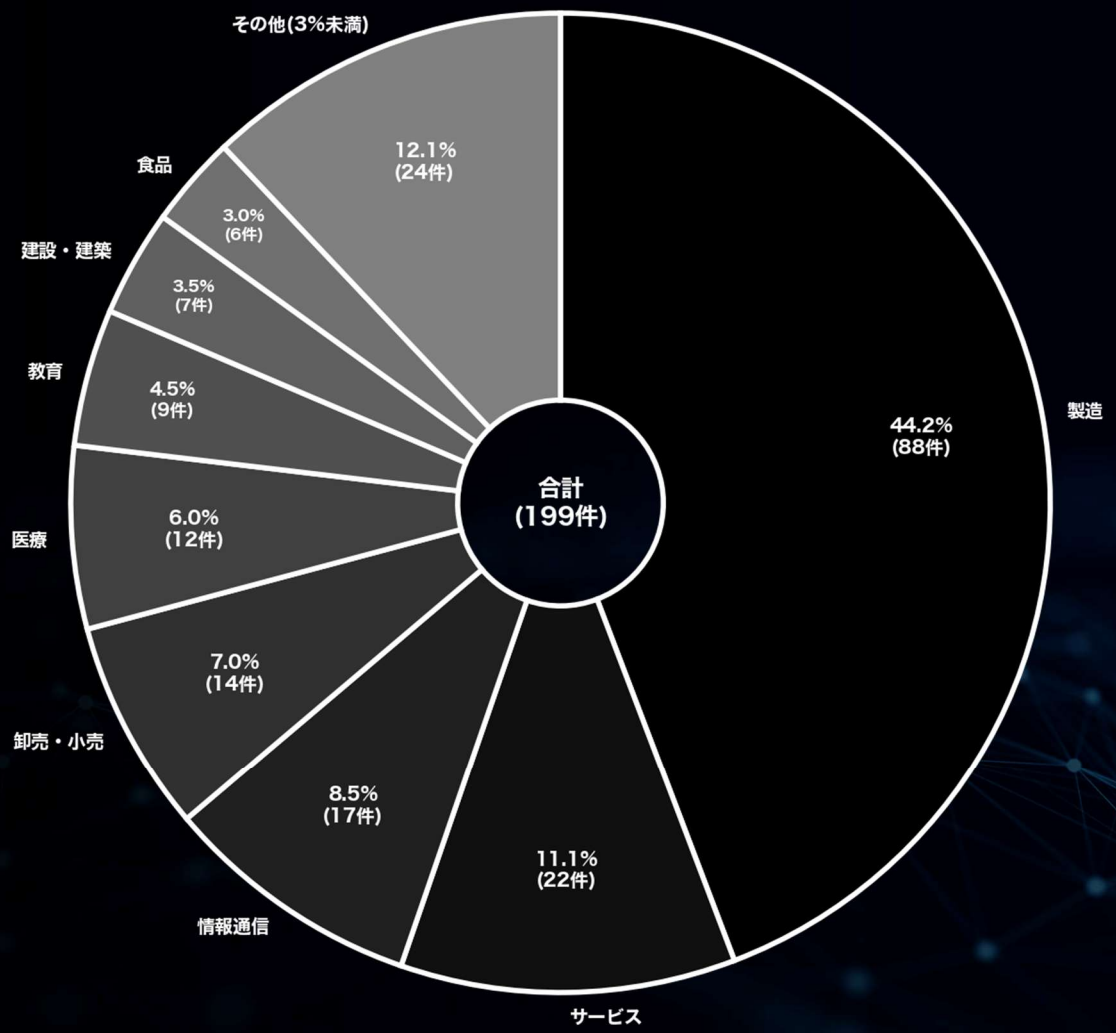
（※本ページの表／グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している）

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5月～2026年4月）

業種	件数	割合(%)
製造	88	44.2
サービス	22	11.1
情報通信	17	8.5
卸売・小売	14	7.0
医療	12	6.0
教育	9	4.5
建設・建築	7	3.5
食品	6	3.0
その他(3%未満)	24	12.1

▼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

2026

4

中小企業における被害分析
（国内）

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

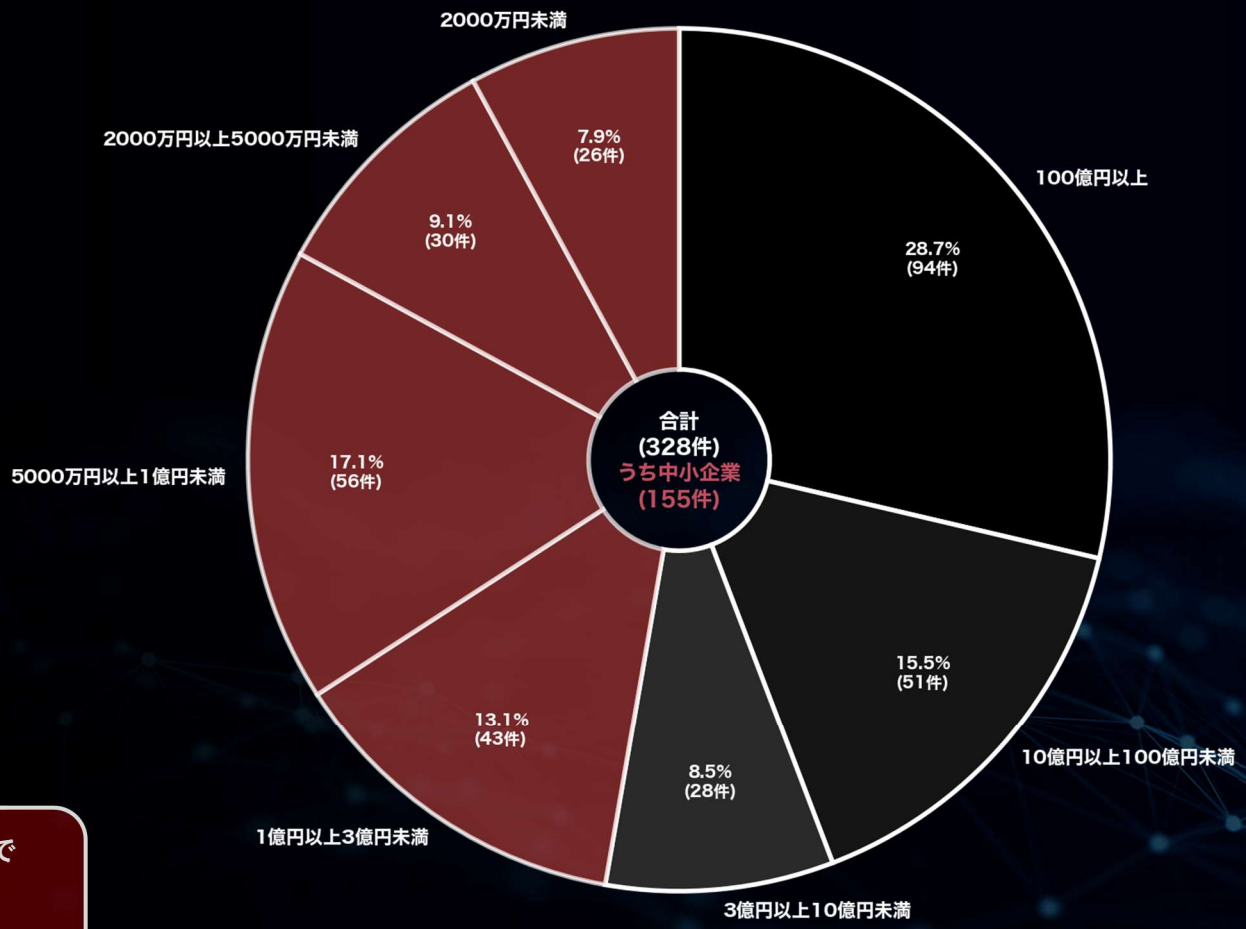
資本金別（国内-中小企業）
（過去2年間／2024年5月～2026年4月）

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	94	28.7
10億円以上100億円未満	51	15.5
3億円以上10億円未満	28	8.5
1億円以上3億円未満	43	13.1
5000万円以上1億円未満	56	17.1
2000万円以上5000万円未満	30	9.1
2000万円未満	26	7.9

▼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155件にのぼり、全体の47.3%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）

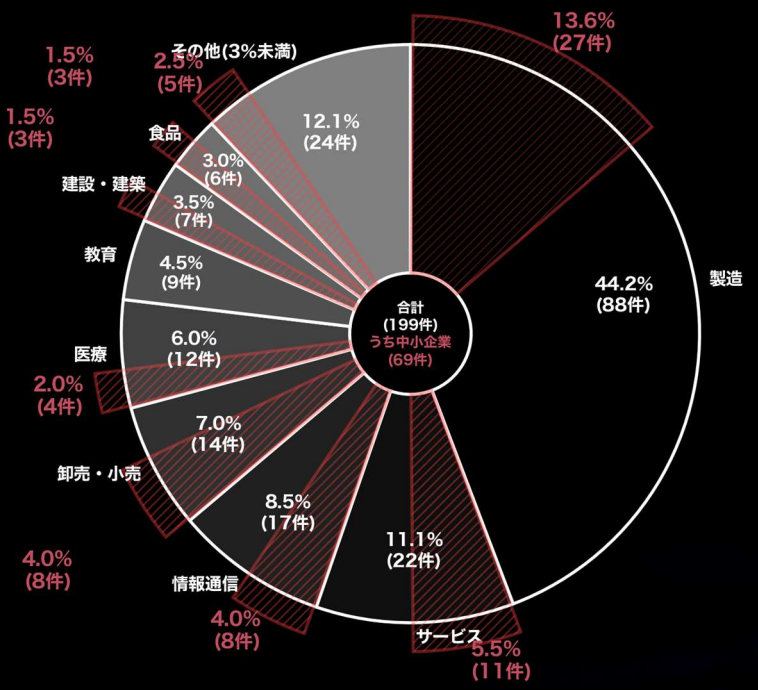
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

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5月～2026年4月）

赤色は中小企業を示す

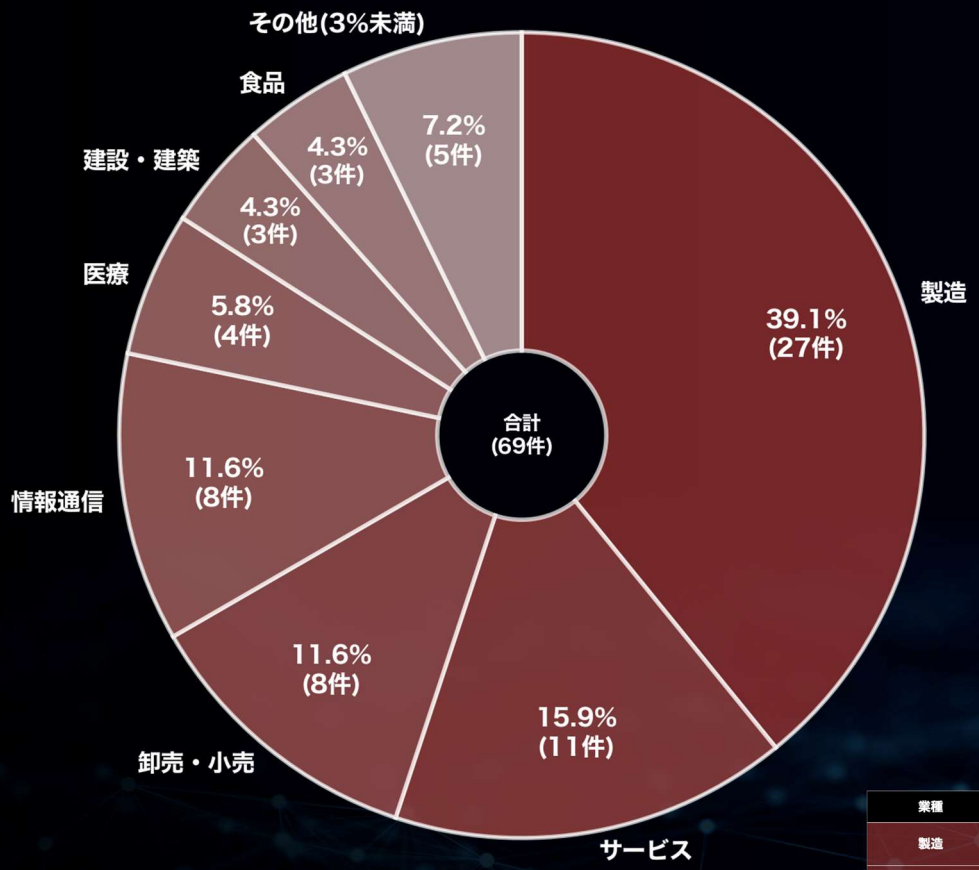
▼全体割合



※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	88 (27)	44.2 (13.6)
サービス	22 (11)	11.1 (5.5)
情報通信	17 (8)	8.5 (4.0)
卸売・小売	14 (8)	7.0 (4.0)
医療	12 (4)	6.0 (2.0)
教育	9	4.5
建設・建築	7 (3)	3.5 (1.5)
食品	6 (3)	3.0 (1.5)
その他(3%未満)	24 (5)	12.1 (2.5)

▼中小企業のみの割合



業種	件数	割合(%)
製造	27	39.1
サービス	11	15.9
卸売・小売	8	11.6
情報通信	8	11.6
医療	4	5.8
建設・建築	3	4.3
食品	3	4.3
その他(3%未満)	5	7.2

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

（※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）

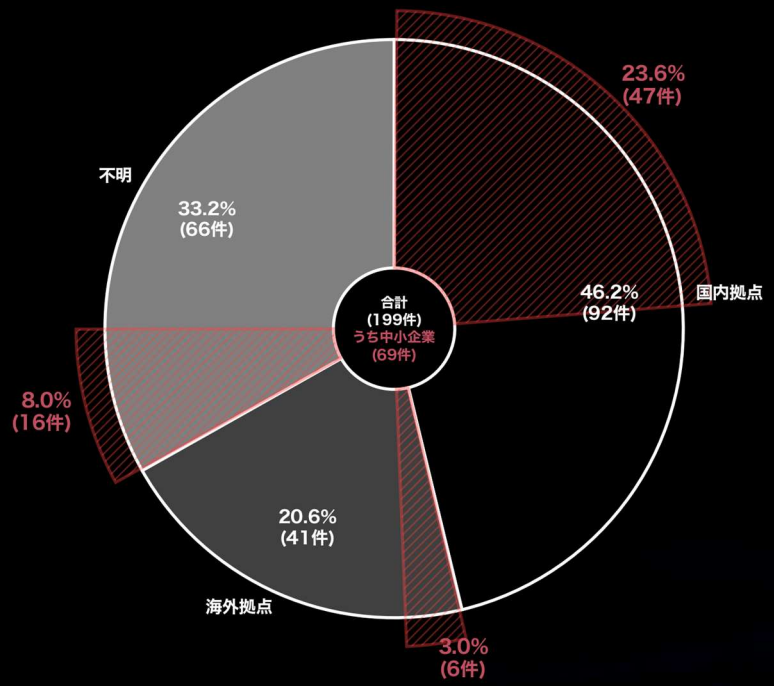
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

公となった国内被害組織における拠点割合（国内-中小企業）

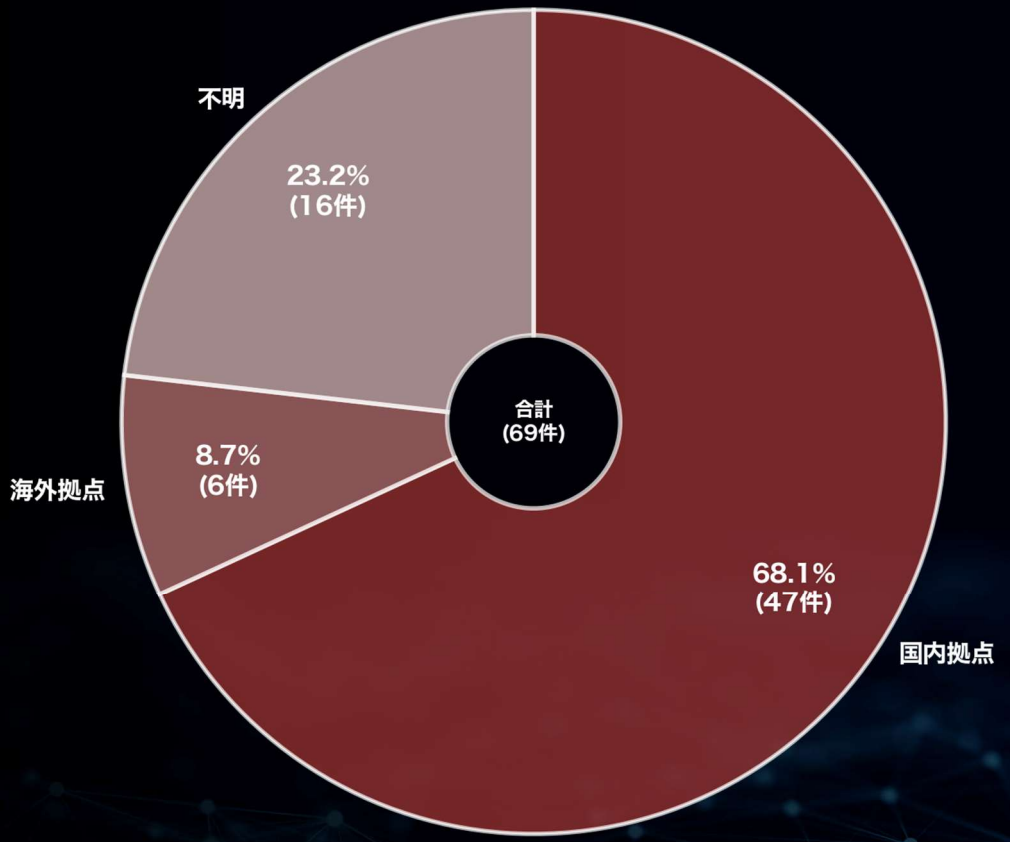
（過去1年間／2025年5月～2026年4月）

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	92 (47)	46.2 (23.6)
海外拠点	41 (6)	20.6 (3.0)
不明	66 (16)	33.2 (8.0)
合計	199 (69)	100 (34.6)

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	47	68.1
海外拠点	6	8.7
不明	16	23.2

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

※ 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5月～2026年4月）

赤色は中小企業を示す

被害月	攻撃グループ	業種概要
2025/5	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

被害月	攻撃グループ	業種概要
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
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

被害月	攻撃グループ	業種概要
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
2025/11	(Unknown)	国際総合検定機関
2025/12	(Unknown)	エレクトロニクス専門商社(海外拠点)
2025/12	(Unknown)	教育系ITサービス提供
2025/12	AKIRA	食用油脂メーカー(海外拠点)
2025/12	Payouts King	プラスチック精密工業部品メーカー(海外拠点)

※（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

※ 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5月～2026年4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
2025/12	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	(Unknown)	不動産管理
2026/1	Orion Leaks	タイヤメーカー(海外拠点)
2026/1	(Unknown)	飲料メーカー
2026/1	(Unknown)	スポーツ教室
2026/1	The Gentlemen	産業廃棄物処理
2026/1	Brain Cipher	システムインテグレーター
2026/2	Qilin (Agenda)	特殊金属材料・製造
2026/2	Everest	機械器具製造
2026/2	Everest	金属加工メーカー
2026/2	(Unknown)	大手化学素材メーカー(海外拠点)

被害月	攻撃グループ	業種概要
2026/2	0APT	大手電気機器メーカー
2026/2	0APT	大手テクノロジー企業
2026/2	0APT	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	0APT	医療機器メーカー
2026/2	0APT	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	0APT	タイヤメーカー
2026/2	0APT	総合電機メーカー
2026/2	0APT	大手自動車メーカー
2026/2	0APT	建設機械メーカー
2026/2	0APT	総合電機メーカー
2026/2	(Unknown)	ソフトウェア開発
2026/2	Qilin (Agenda)	総合デベロッパー
2026/2	NetRunner	総合病院
2026/2	(Unknown)	ホテル業・飲食店業
2026/2	0APT	鉄道会社
2026/2	0APT	地方自治体
2026/2	0APT	電力会社
2026/2	0APT	地方自治体
2026/2	Qilin (Agenda)	種苗メーカー兼商社(海外拠点)
2026/2	NightSpire	繊維・衣料関連卸売業
2026/2	(Unknown)	半導体試験装置メーカー
2026/2	NetRunner	総合病院
2026/2	LockBit	機械・工具メーカー(海外拠点)
2026/2	BLACKSHRANTAC	紳士服・婦人服販売
2026/2	NightSpire	モータースポーツチーム運営
2026/2	(Unknown)	印刷会社
2026/2	INC Ransom	石油製品・LPガス販売
2026/2	The Gentlemen	材料加工装置メーカー
2026/2	Everest	商用車メーカー

被害月	攻撃グループ	業種概要
2026/3	(Unknown)	市場調査・コンサルティング
2026/3	NetRunner	療養型病院
2026/3	(Unknown)	工業用ゴム・樹脂・配管資材商社
2026/3	(Unknown)	住宅・商業施設向けリペア
2026/3	(Unknown)	美容クリニック
2026/3	(Unknown)	シティホテル運営
2026/3	The Gentlemen	医療・看護専門出版社
2026/3	Space Bears	介護・カラオケ・飲食事業
2026/3	(Unknown)	光半導体デバイスメーカー(海外拠点)
2026/3	WORLD LEAKS	広告・制作
2026/3	The Gentlemen	繊維加工・食品加工メーカー
2026/3	(Unknown)	設備工事
2026/3	(Unknown)	美容室向け化粧品メーカー
2026/3	ALP-001	国立研究開発法人
2026/4	AKIRA	流体システム製品メーカー
2026/4	(Unknown)	非鉄金属・資源開発(海外拠点)
2026/4	(Unknown)	システムインテグレーター
2026/4	KRYBIT	酒類製造業
2026/4	LockBit	水処理・環境設備
2026/4	DragonForce	オフィス家具メーカー(海外拠点)
2026/4	(Unknown)	診療予約システム開発
2026/4	Qilin (Agenda)	舗装・土木工事
2026/4	The Gentlemen	電気機器メーカー
2026/4	Qilin (Agenda)	建設資材・福祉用具のレンタル・販売
2026/4	(Unknown)	ロボットシステムインテグレーター
2026/4	(Unknown)	生活協同組合
2026/4	COINBASE CARTEL	大学研究会
2026/4	Ransom EXX	ソフトウェア開発
2026/4	LockBit	電子部品(コネクタ)製造(海外拠点)
2026/4	(Unknown)	二輪用品専門チェーン
2026/4	The Gentlemen	ソフトウェア開発
2026/4	(Unknown)	紙器製造
2026/4	Qilin (Agenda)	大手自動車部品メーカー(海外拠点)

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

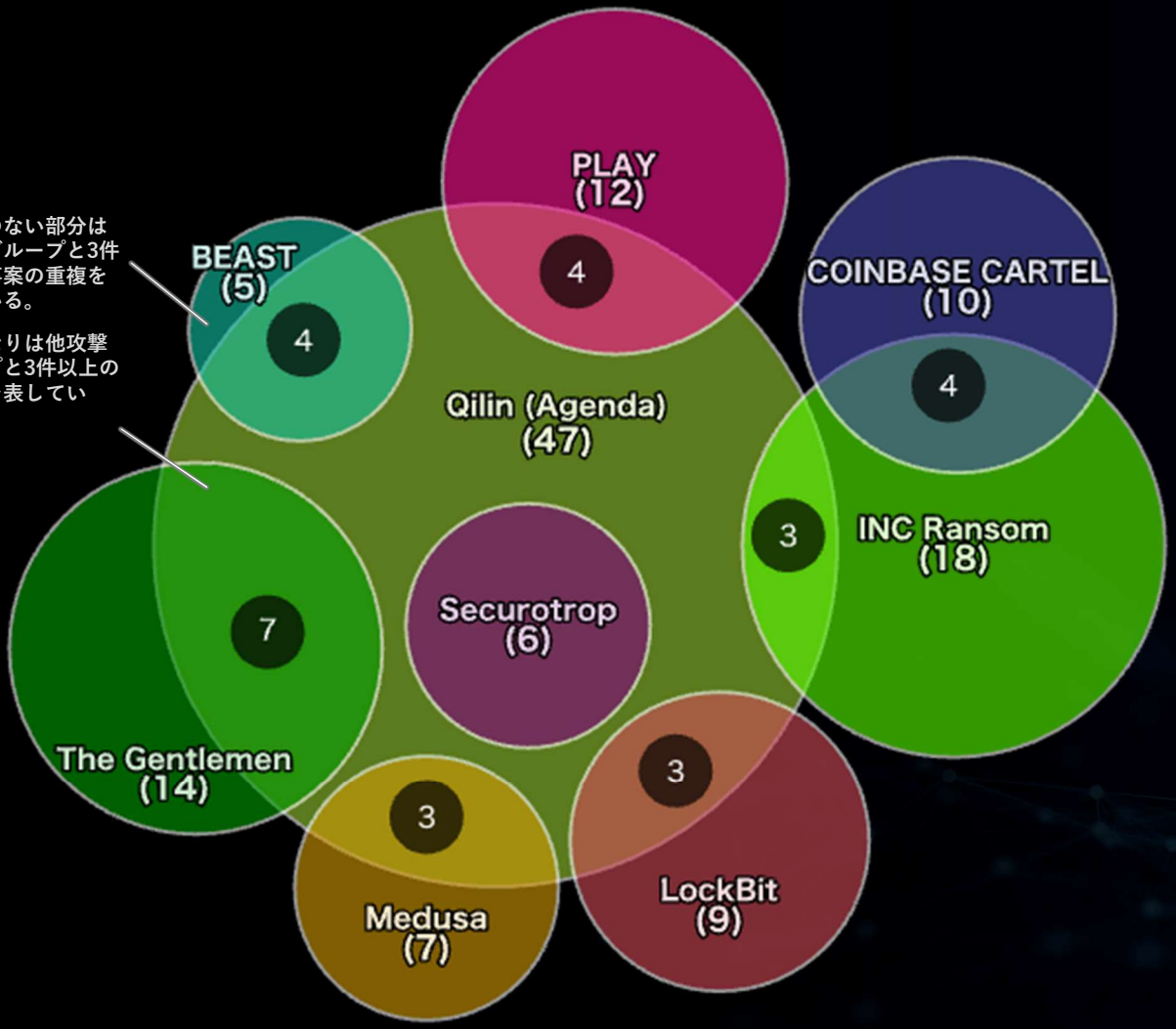
多重被害に関する分析

2026

4

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5月～2026年4月）　（累計127件）※多重被害に遭った組織数の累計



※ 重なりのない部分は他攻撃グループと3件未満の事案の重複を表している。

※ 円の重なりは他攻撃グループと3件以上の重なりを表している。

※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。

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

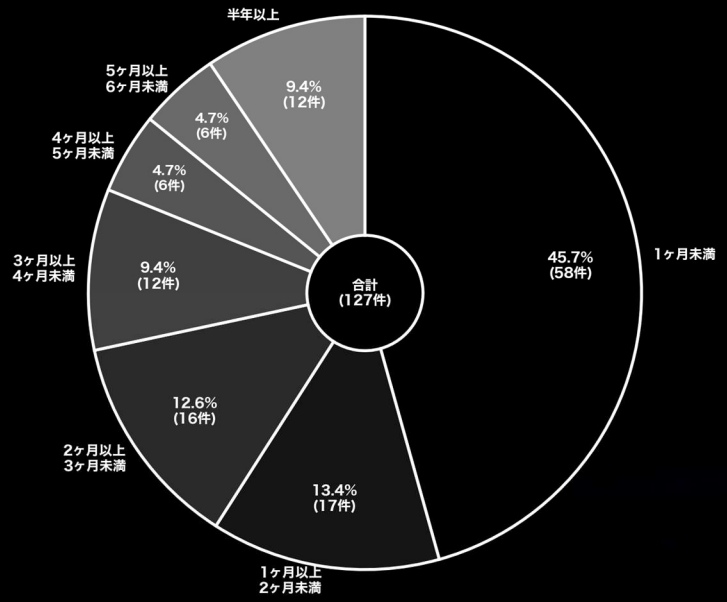
多重被害に遭った被害組織の傾向と分析（全世界）

（過去1年間／2025年5月～2026年4月）

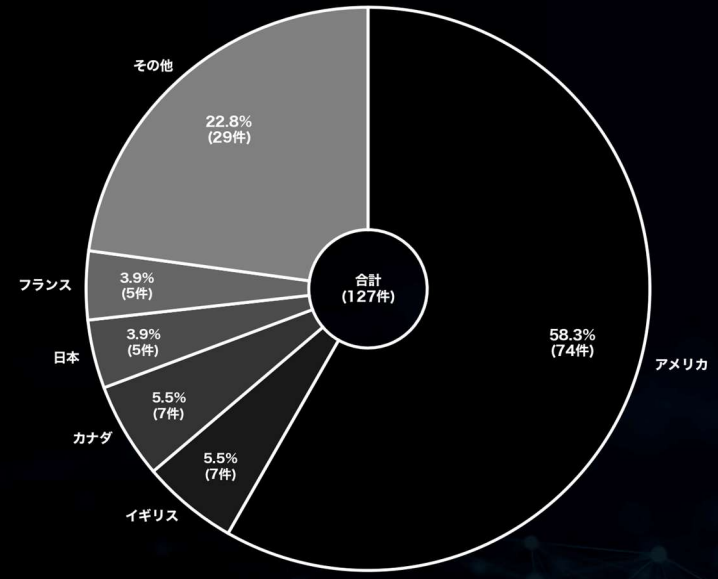
※多重被害：一度ランサムウェア攻撃の被害を受けた組織が異なる時期に異なる攻撃グループのリークサイトに再び掲載されるケース

▼被害の間隔

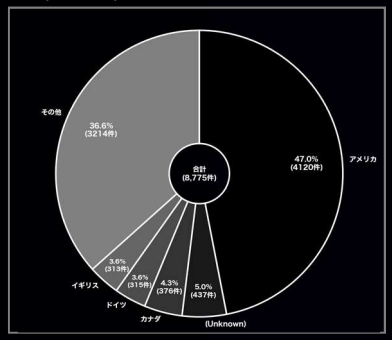
（一度目の被害から二度目の被害までの間隔）



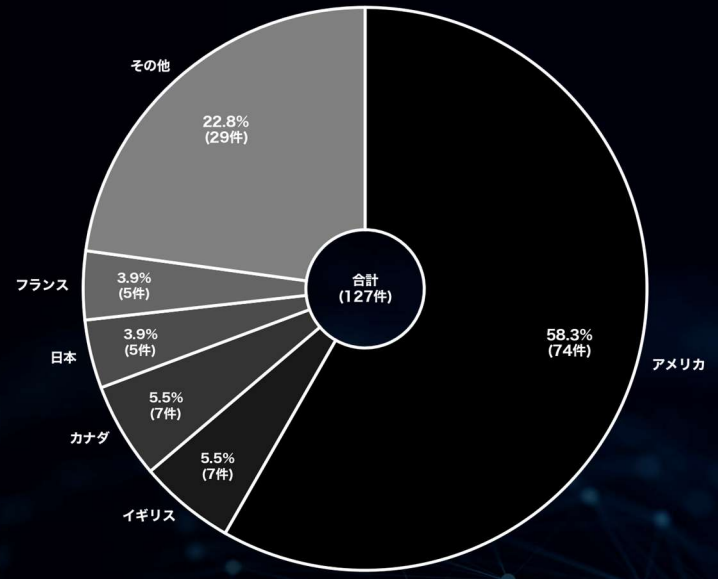
▼被害国別



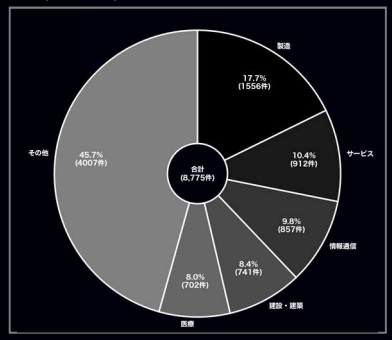
（参考比較）同期間の全データにおける割合



▼業種別



（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：127件（全体8775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。

2026

4

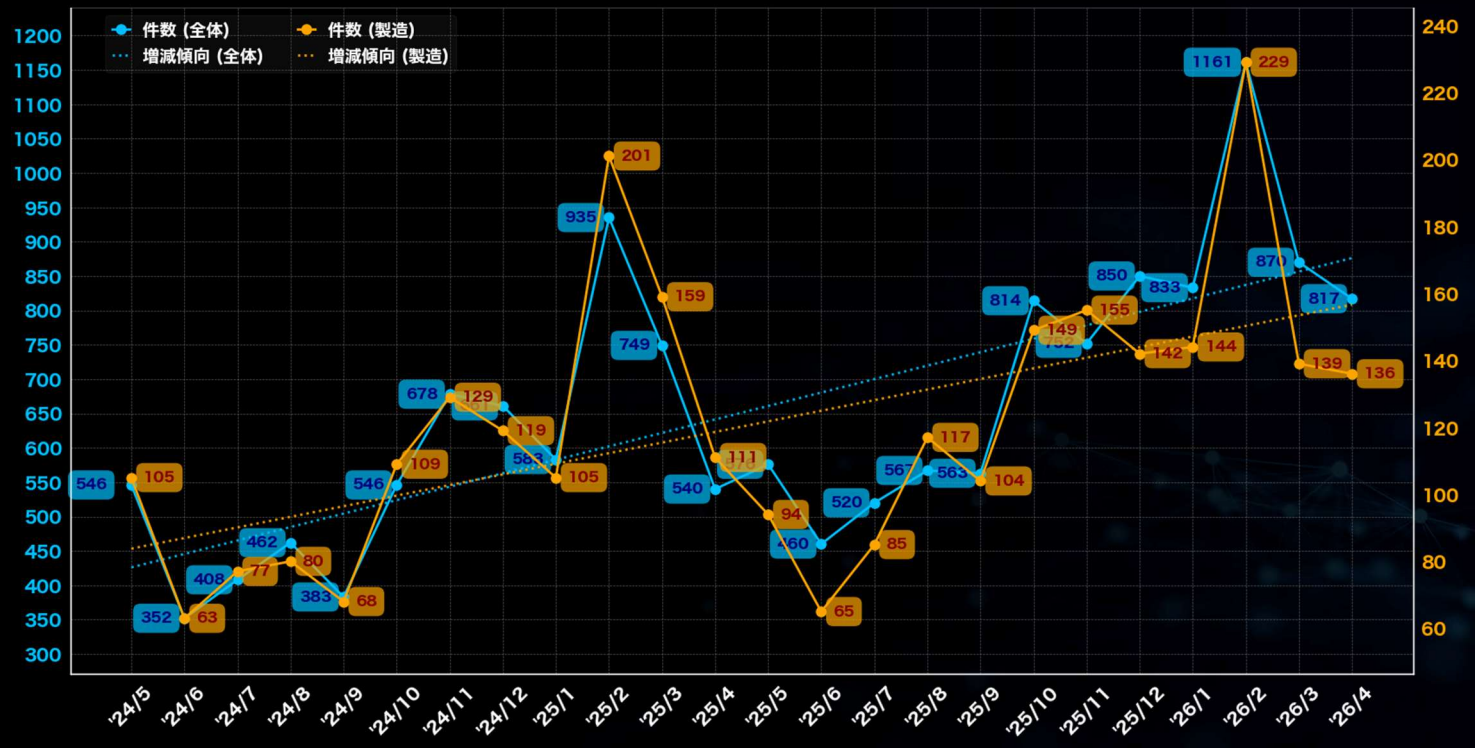
業種に関する分析

（過去2年間のリークサイト掲載上位10業種）

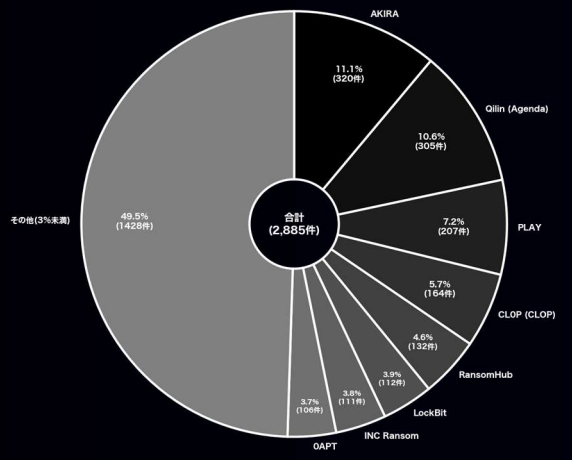
業種に関する分析（全世界）
（過去2年間／2024年5月～2026年4月）

製造

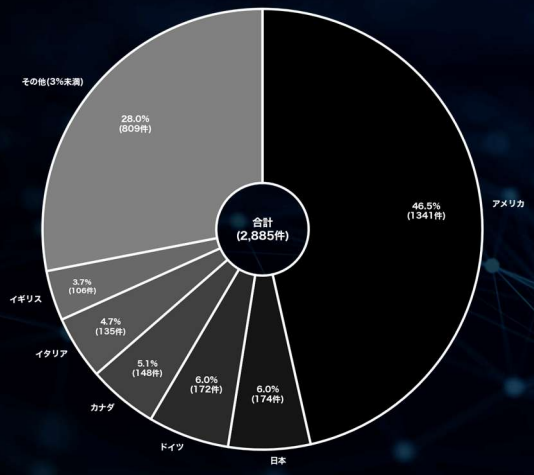
「製造」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年2月で、229件の掲載があった。一方、最も少なかった月は2024年6月で、63件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いで日本とドイツがそれぞれ約6%である。攻撃グループについては、少なくとも141のグループが関与しており、特に「AKIRA」が320件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「PLAY」がそれぞれ305件と207件の掲載を行っている。製造関連の件数は全体件数に対して高い割合で推移しており、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



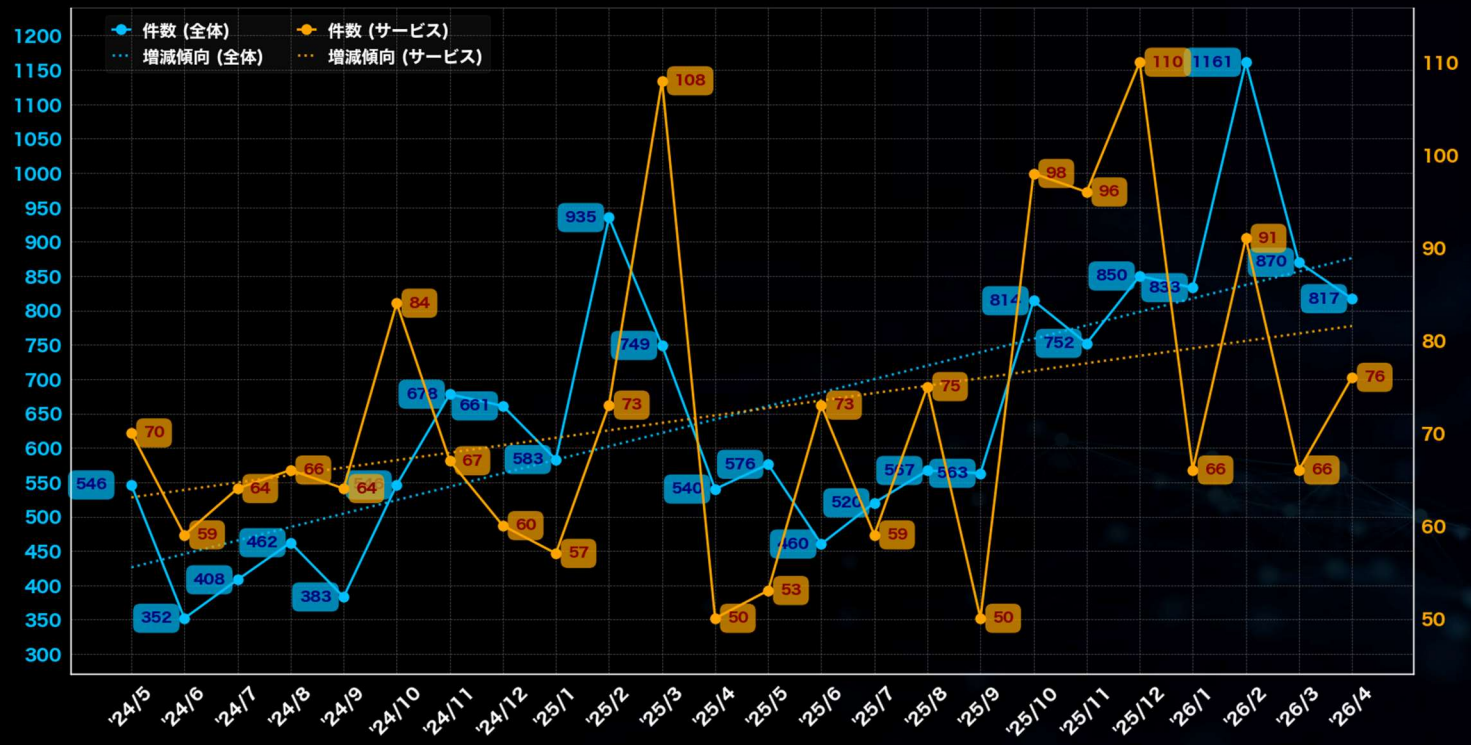
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

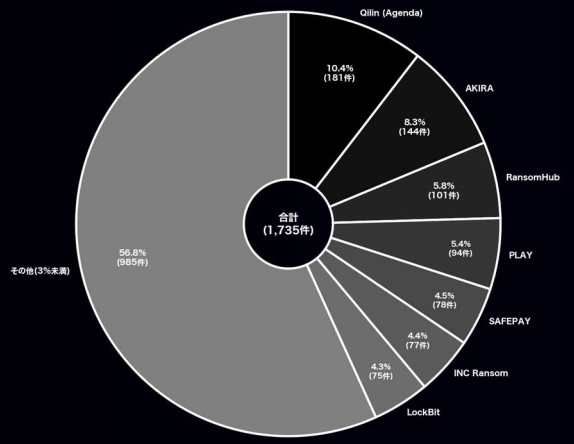
業種に関する分析（全世界）
（過去2年間／2024年5月～2026年4月）

サービス

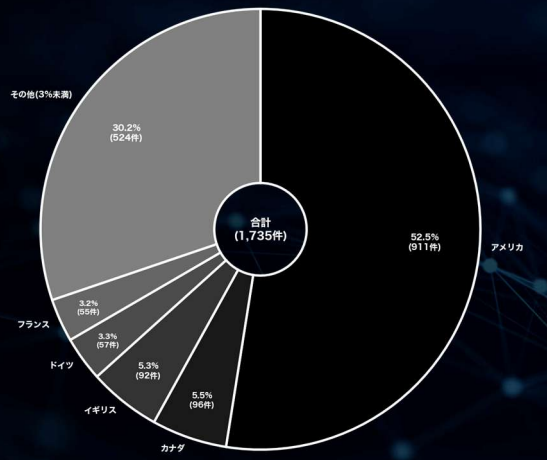
「サービス」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年12月で、110件の掲載があった。一方、最も少なかった月は2025年4月および2025年9月で、50件であった。被害組織の所在国の割合では、アメリカが約53%と最も多く、次いでカナダとイギリスがそれぞれ約6%と約5%である。攻撃グループについては、少なくとも134のグループが関与しており、特に「Qilin (Agenda)」が181件のリークサイト掲載を実施している。次いで「AKIRA」と「RansomHub」がそれぞれ144件と101件の掲載を行っている。サー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



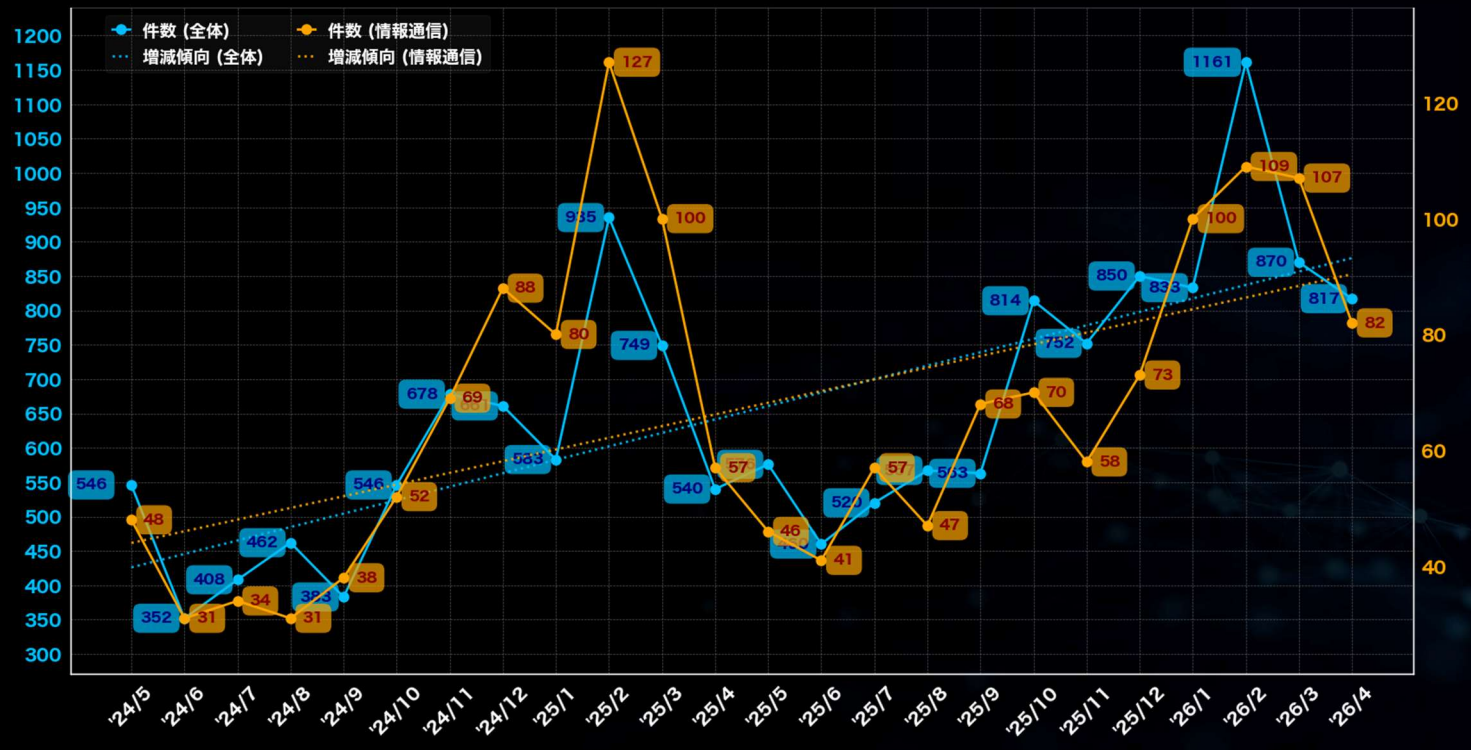
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

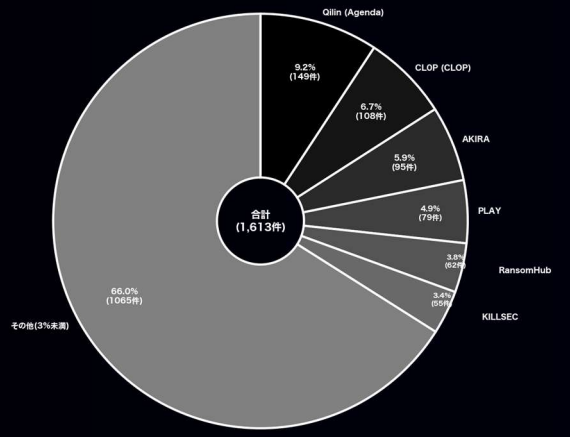
業種に関する分析（全世界）
（過去2年間／2024年5月～2026年4月）

情報通信

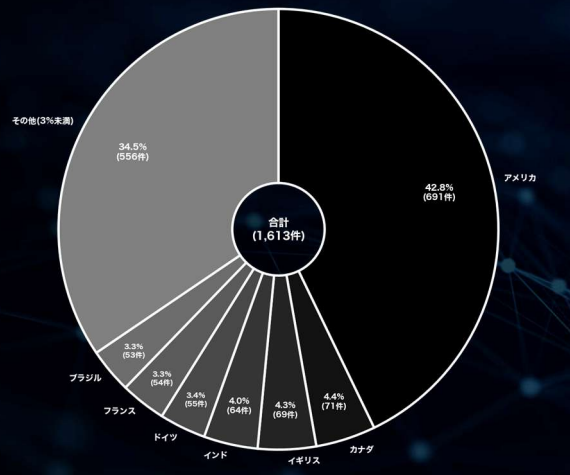
「情報通信」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、127件の掲載があった。一方、最も少なかった月は2024年6月および2024年8月で、31件であった。被害組織の所在国の割合では、アメリカが約43%と最も多く、次いでカナダとイギリスがそれぞれ約4%である。攻撃グループについては、少なくとも141のグループが関与しており、特に「Qilin (Agenda)」が149件のリークサイト掲載を実施している。次いで「CL0P (CLOP)」と「AKIRA」がそれぞれ108件と95件の掲載を行っている。情報通信業界は技術情報や顧客データを多く保有することから、引き続きランサムウェア攻撃の主要な標的となっており、関与グループ数も製造業と並ぶ規模となっている。



▼攻撃グループ別



▼国別



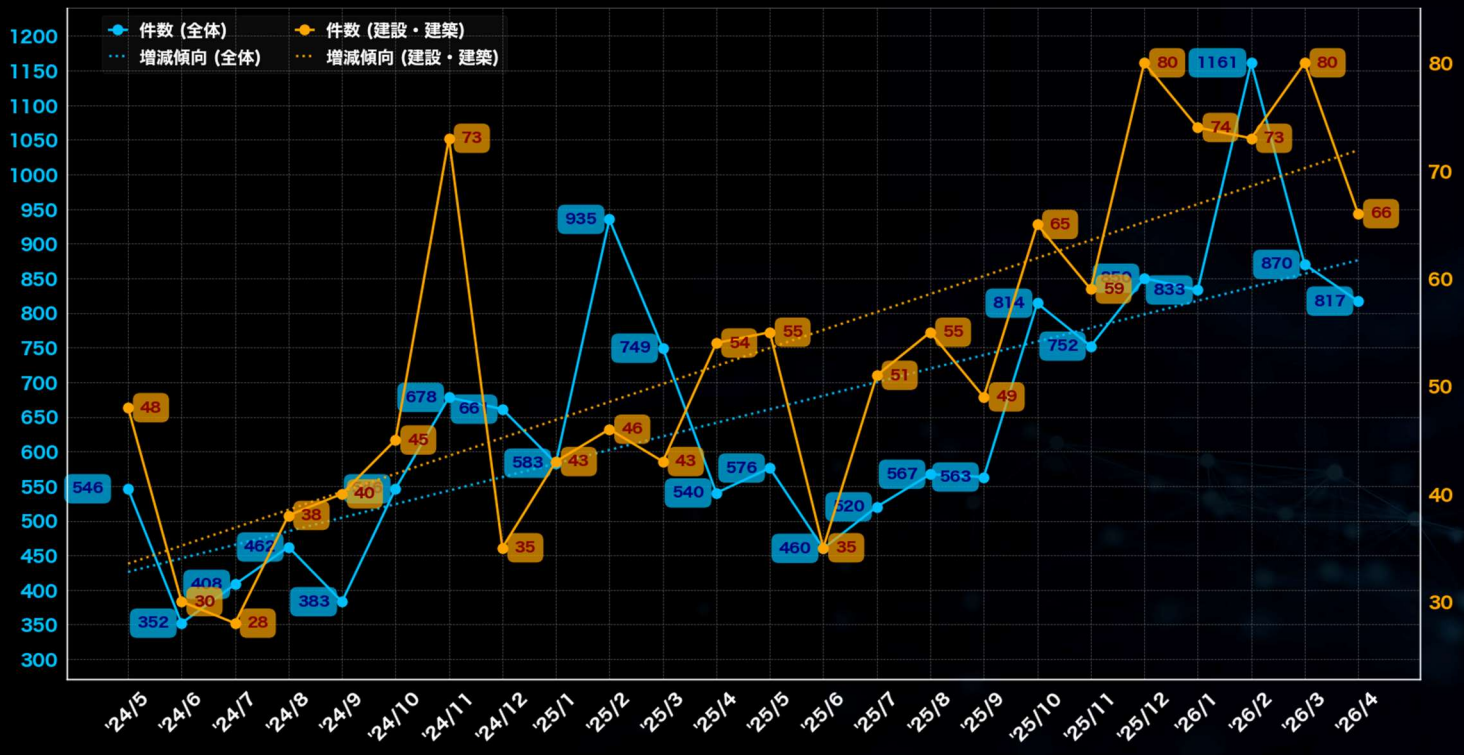
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

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

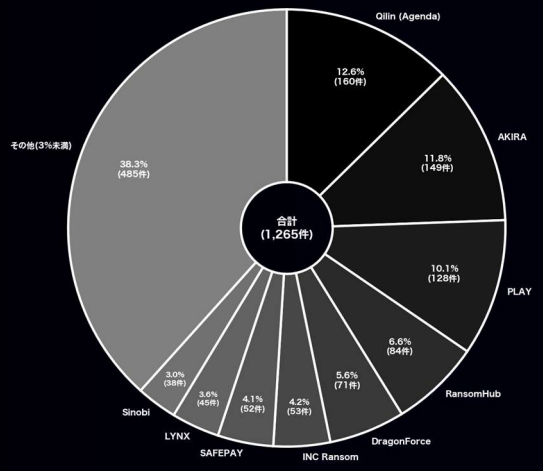
業種に関する分析（全世界）
（過去2年間／2024年5月～2026年4月）

建設・建築

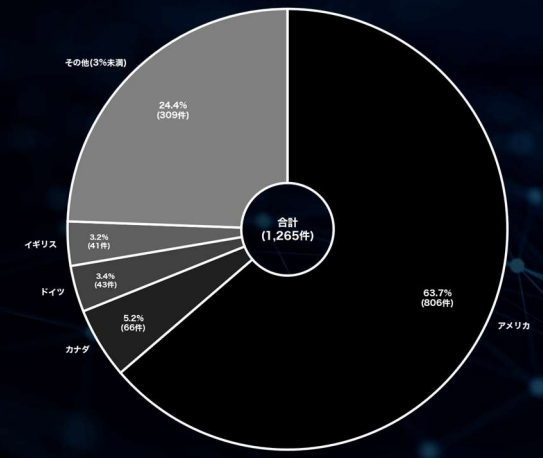
「建設・建築」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年12月および2026年3月で、それぞれ80件の掲載があった。一方、最も少なかった月は2024年7月で、28件であった。被害組織の所在国の割合では、アメリカが約64%と最も多く、次いでカナダとドイツがそれぞれ約5%と約3%である。攻撃グループについては、少なくとも106のグループが関与しており、特に「Qilin (Agenda)」が160件のリークサイト掲載を実施している。次いで「AKIRA」と「PLAY」がそれぞれ149件と128件の掲載を行っている。建設・建築業界はアメリカに被害が集中しており、攻撃対象としての偏りが顕著に表れている。



▼攻撃グループ別



▼国別



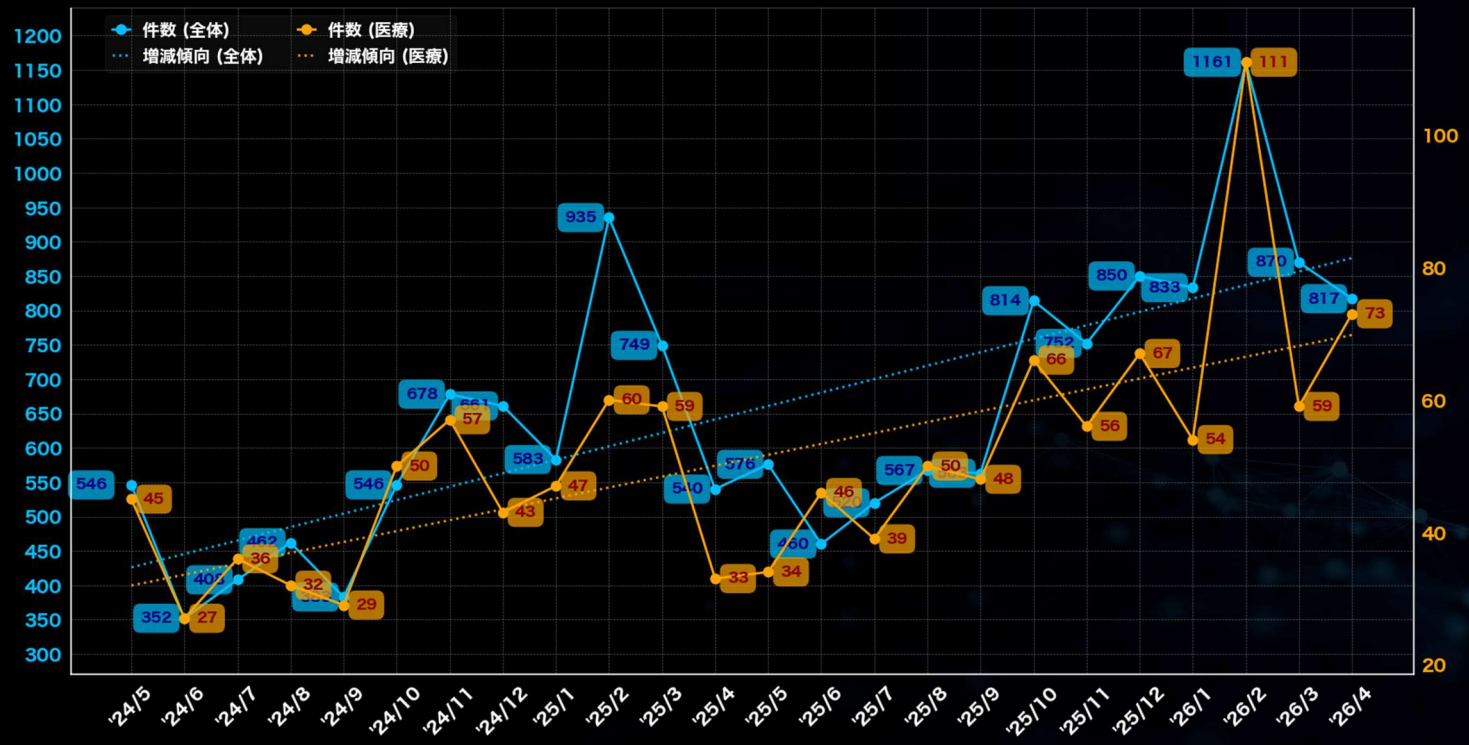
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

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

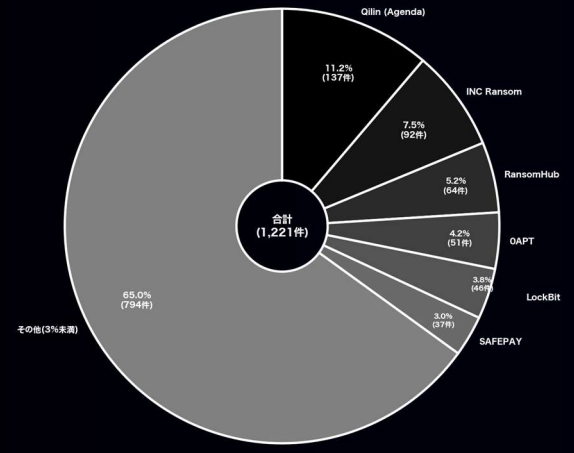
業種に関する分析（全世界）
（過去2年間／2024年5月～2026年4月）

医療

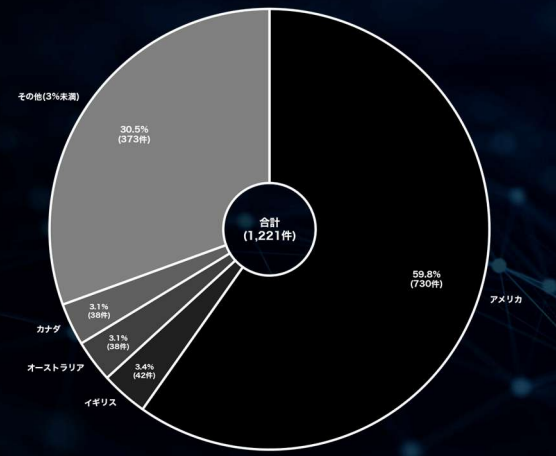
「医療」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年2月で、111件の掲載があった。一方、最も少なかった月は2024年6月で、27件であった。被害組織の所在国の割合では、アメリカが約60%と最も多く、次いでイギリスとオーストラリアがそれぞれ約3%である。攻撃グループについては、少なくとも123のグループが関与しており、特に「Qilin (Agenda)」が137件のリークサイト掲載を実施している。次いで「INC Ransom」と「RansomHub」がそれぞれ92件と64件の掲載を行っている。医療業界は患者情報など機微なデータを保有することから、依然として攻撃者の標的となっている。



▼攻撃グループ別



▼国別



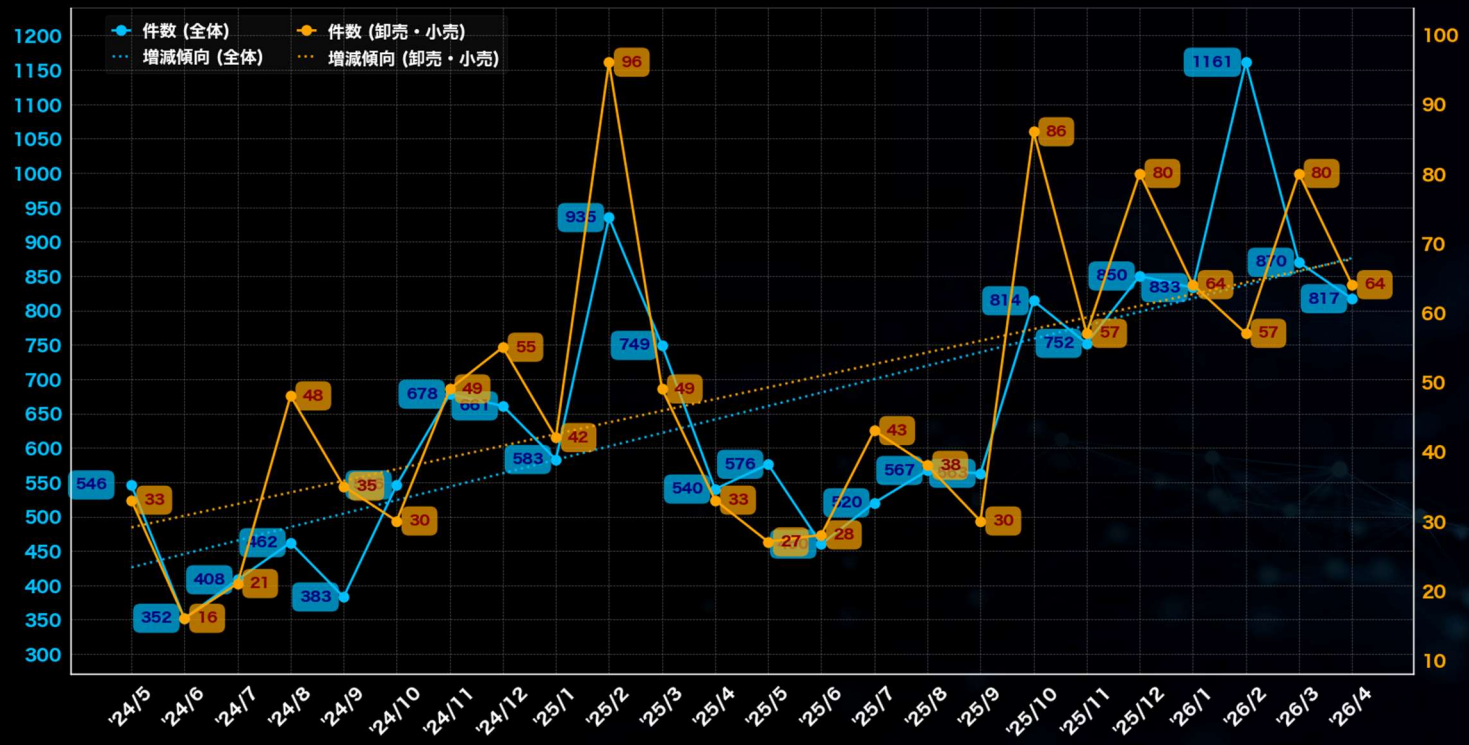
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

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

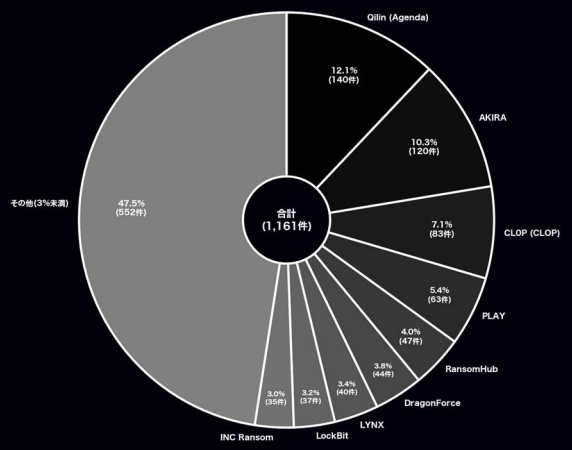
業種に関する分析（全世界）
（過去2年間／2024年5月～2026年4月）

卸売・小売

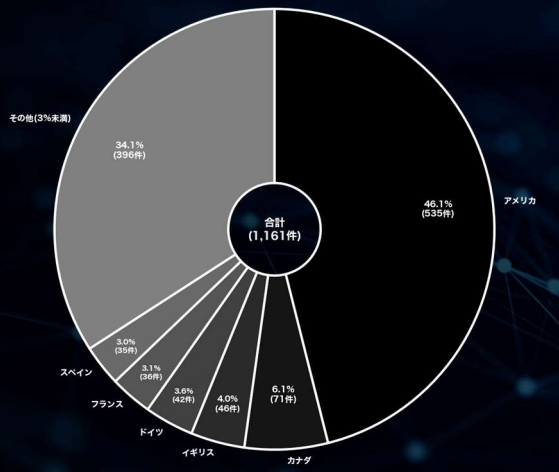
「卸売・小売」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、96件の掲載があった。一方、最も少なかった月は2024年6月で、16件であった。被害組織の所在国の割合では、アメリカが約46%と最も多く、次いでカナダとイギリスがそれぞれ約6%と約4%である。攻撃グループについては、少なくとも106のグループが関与しており、特に「Qilin (Agenda)」が140件のリークサイト掲載を実施している。次いで「AKIRA」と「CL0P (CLOP)」がそれぞれ120件と83件の掲載を行っている。卸売・小売業界は最大月と最小月の差が大きく月次変動の激しい業種でありながら、全体としては増加傾向が続いている。



▼攻撃グループ別



▼国別



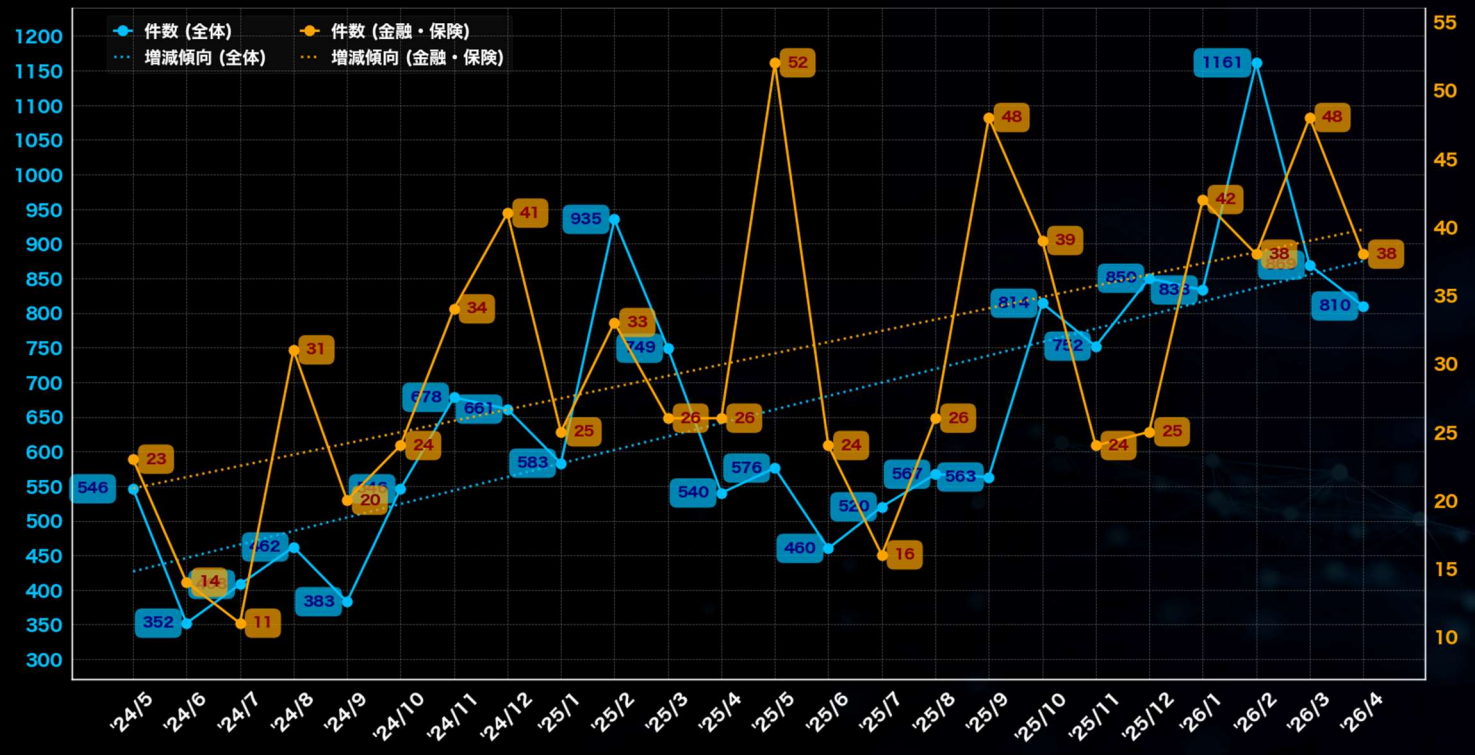
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

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

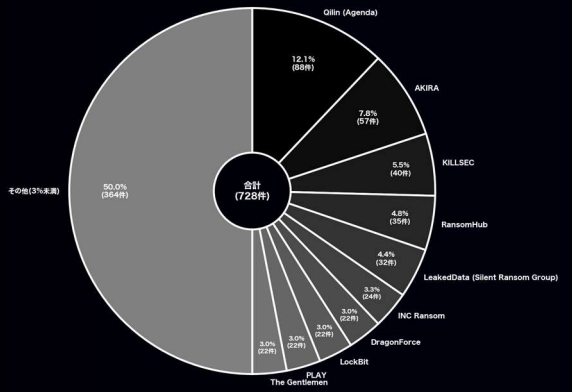
業種に関する分析（全世界）
（過去2年間／2024年5月～2026年4月）

金融・保険

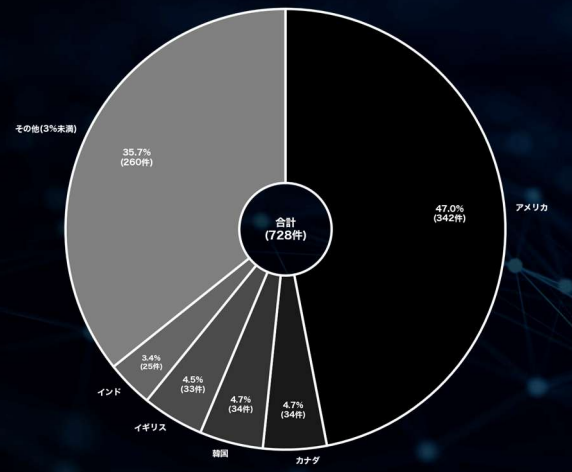
「金融・保険」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年5月で、52件の掲載があった。一方、最も少なかった月は2024年7月で、11件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いでカナダと韓国がそれぞれ約5%である。攻撃グループについては、少なくとも115のグループが関与しており、特に「Qilin (Agenda)」が88件のリークサイト掲載を実施している。次いで「AKIRA」と「KILLSEC」がそれぞれ57件と40件の掲載を行っている。金融・保険業界は被害件数こそ他業界に比べ少ないものの、関与する攻撃グループは115と多岐にわたっており、引き続き警戒が必要である。



▼攻撃グループ別



▼国別



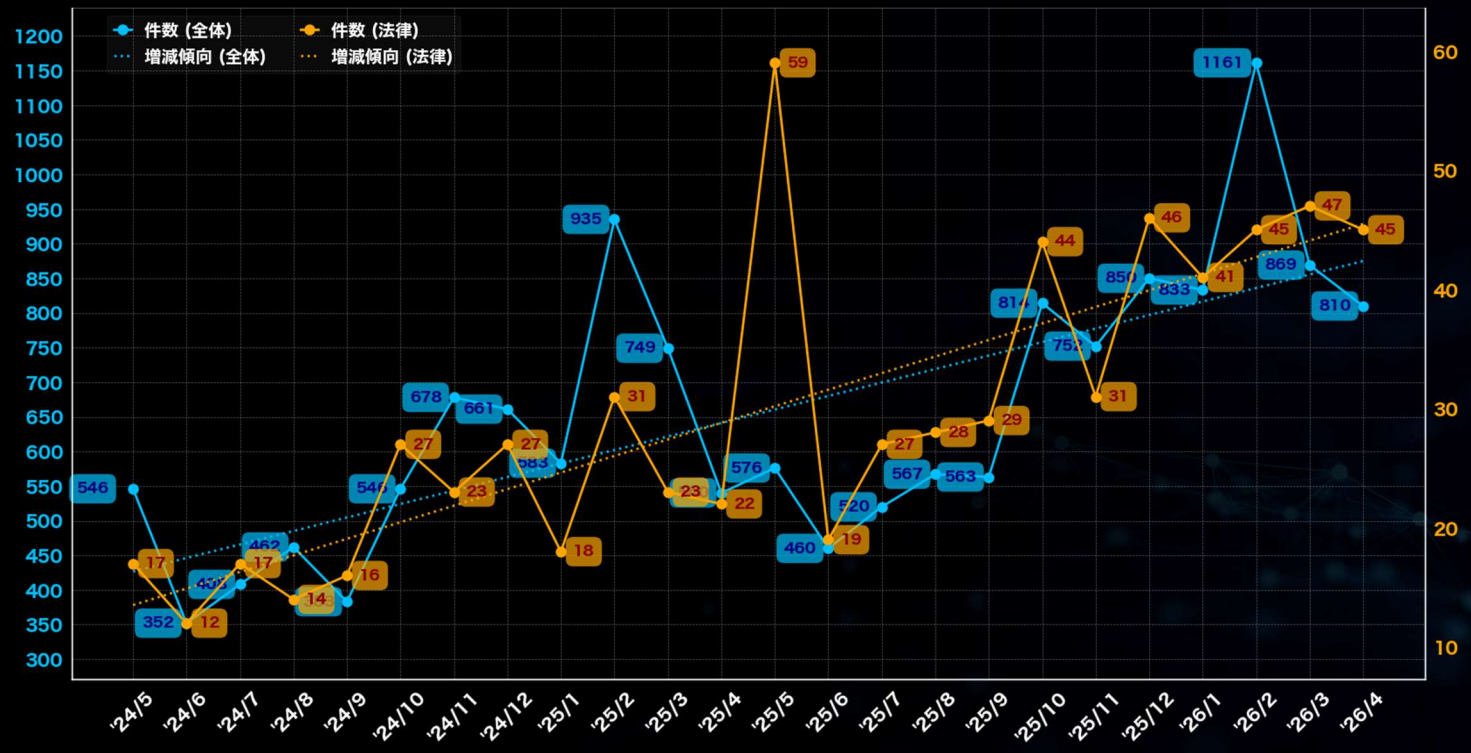
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

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

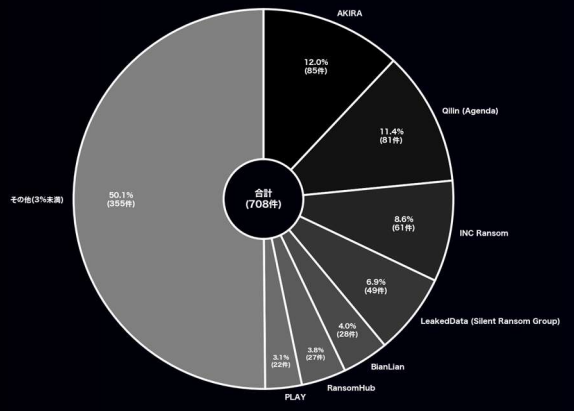
業種に関する分析（全世界）
（過去2年間／2024年5月～2026年4月）

法律

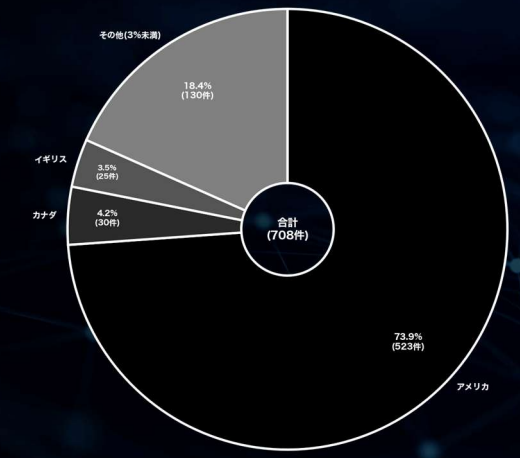
「法律」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年5月で、59件の掲載があった。一方、最も少なかった月は2024年6月で、12件であった。被害組織の所在国の割合では、アメリカが約74%と最も多く、次いでカナダとイギリスがそれぞれ約4%である。攻撃グループについては、少なくとも91のグループが関与しており、特に「AKIRA」が85件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「INC Ransom」がそれぞれ81件と61件の掲載を行っている。法律業界はアメリカの被害が極端に集中している点も特徴である。



▼攻撃グループ別



▼国別



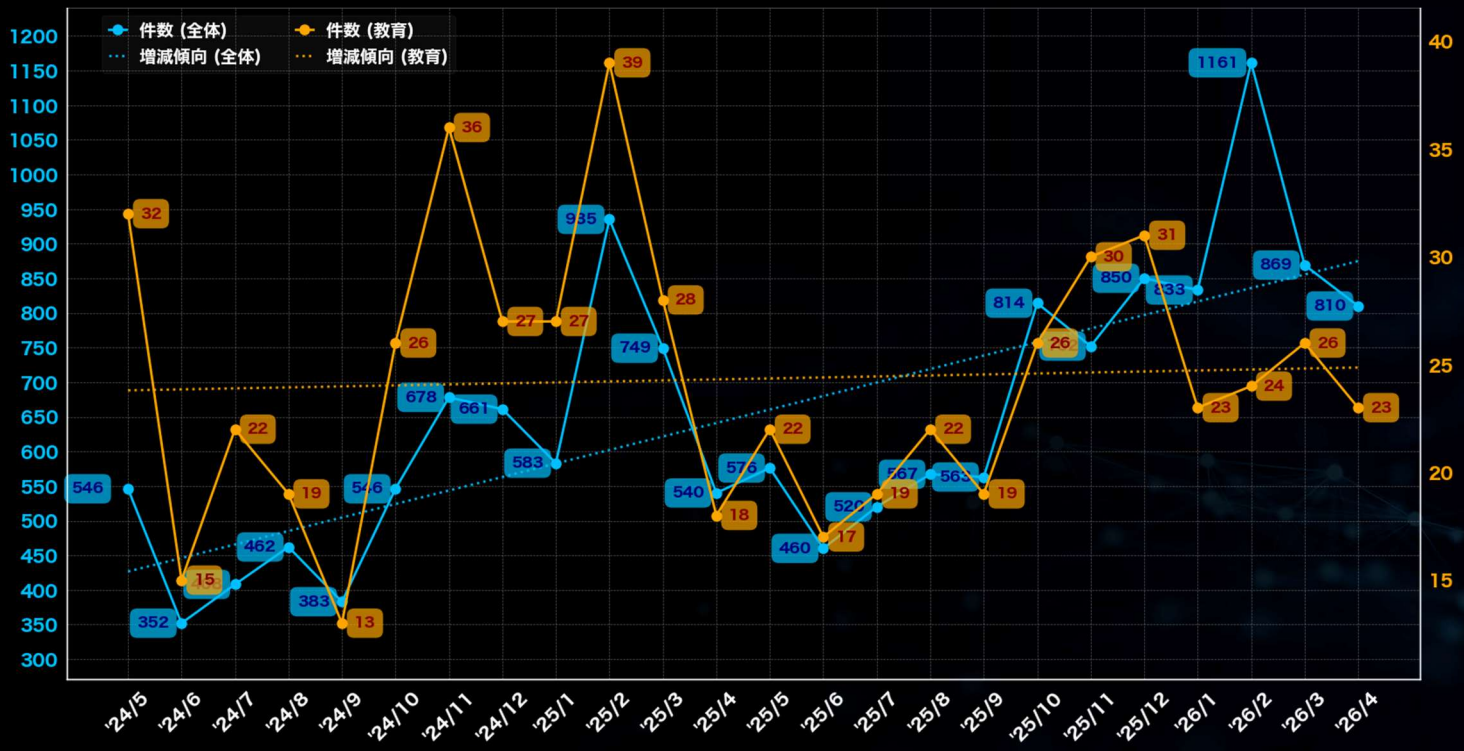
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

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

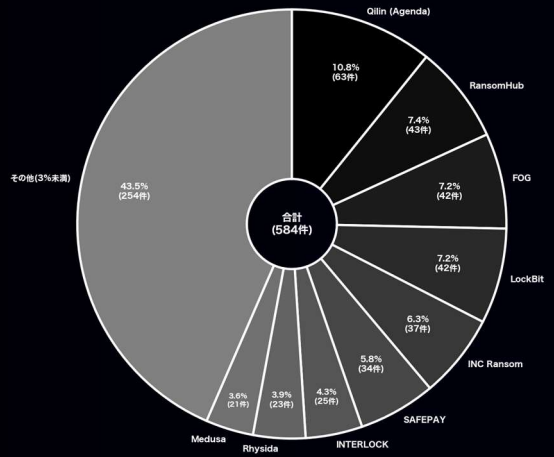
業種に関する分析（全世界）
（過去2年間／2024年5月～2026年4月）

教育

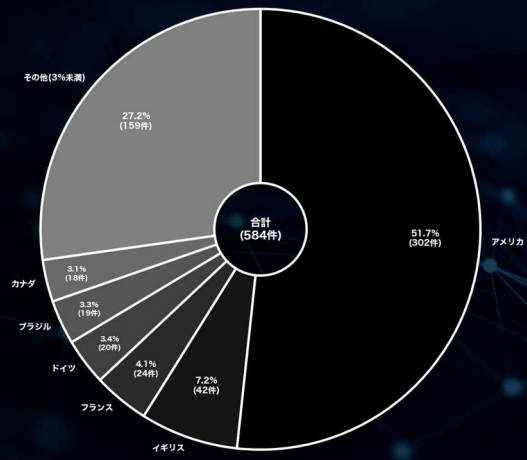
「教育」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、39件の掲載があった。一方、最も少なかった月は2024年9月で、13件であった。被害組織の所在国の割合では、アメリカが約52%と最も多く、次いでイギリスとフランスがそれぞれ約7%と約4%である。攻撃グループについては、少なくとも92のグループが関与しており、特に「Qilin (Agenda)」が63件のリークサイト掲載を実施している。次いで「RansomHub」と「FOG」がそれぞれ43件と42件の掲載を行っている。教育業界は他業界に比べ被害件数は限定的であるものの、関与する攻撃グループは92と多く、依然として注意が必要である。



▼攻撃グループ別



▼国別



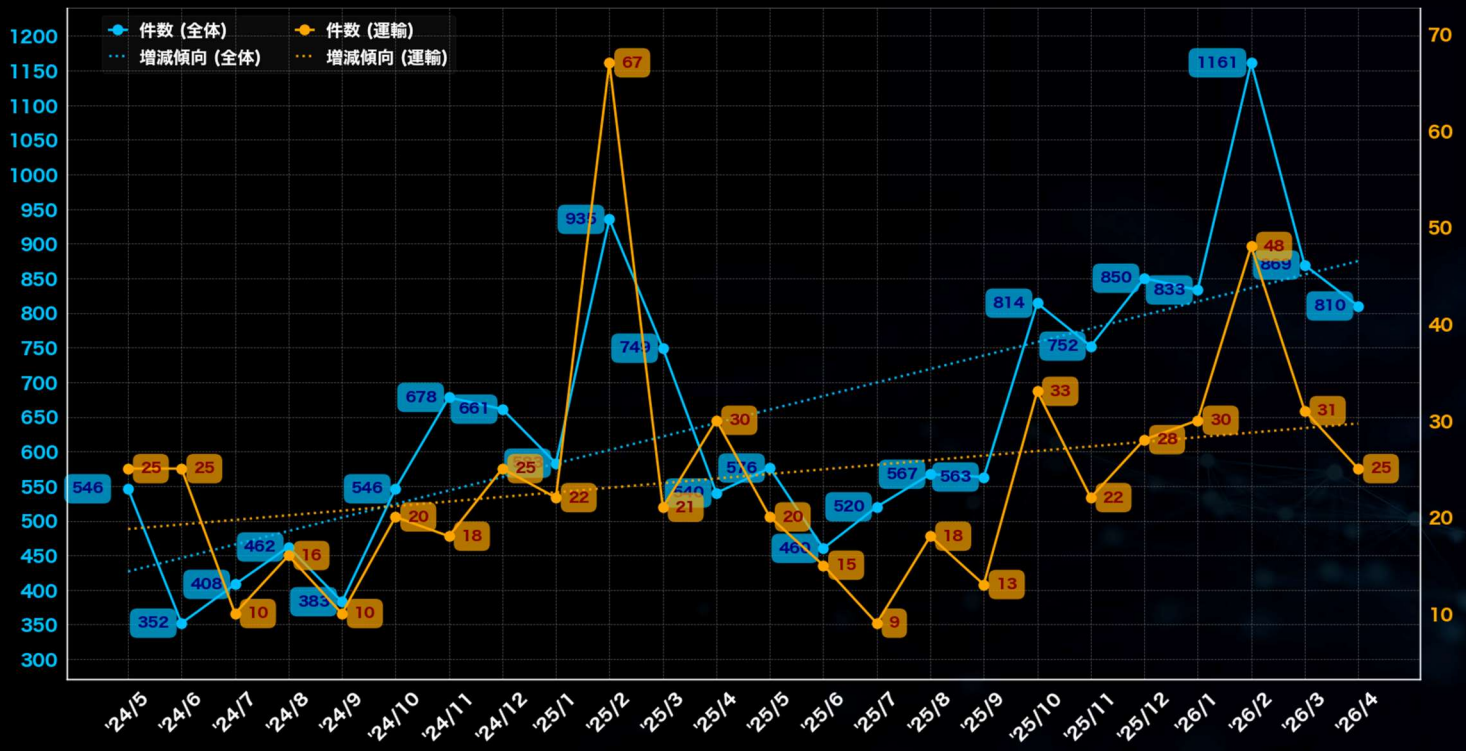
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

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

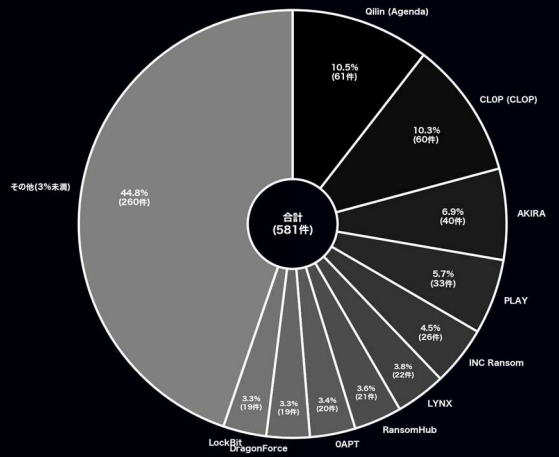
業種に関する分析（全世界）
（過去2年間／2024年5月～2026年4月）

運輸

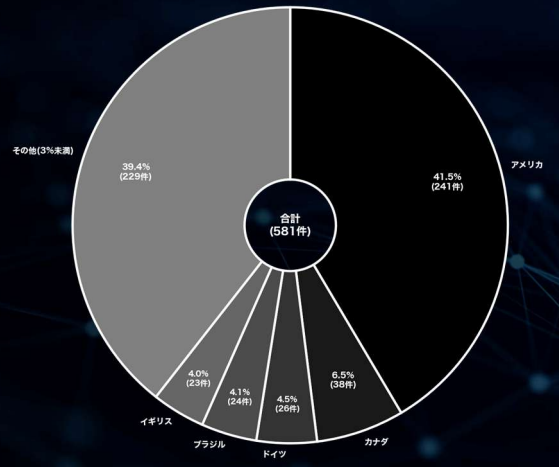
「運輸」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、67件の掲載があった。一方、最も少なかった月は2025年7月で、9件であった。被害組織の所在国の割合では、アメリカが約42%と最も多く、次いでカナダとドイツがそれぞれ約7%と約5%である。攻撃グループについては、少なくとも94のグループが関与しており、特に「Qilin (Agenda)」が61件のリークサイト掲載を実施している。次いで「CL0P (CLOP)」と「AKIRA」がそれぞれ60件と40件の掲載を行っている。運輸関係は全体件数に対する割合こそ低いものの、サプライチェーンへの影響を考慮すると引き続き注視が必要である。



▼攻撃グループ別



▼国別



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

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

CIGのコンテンツ紹介

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

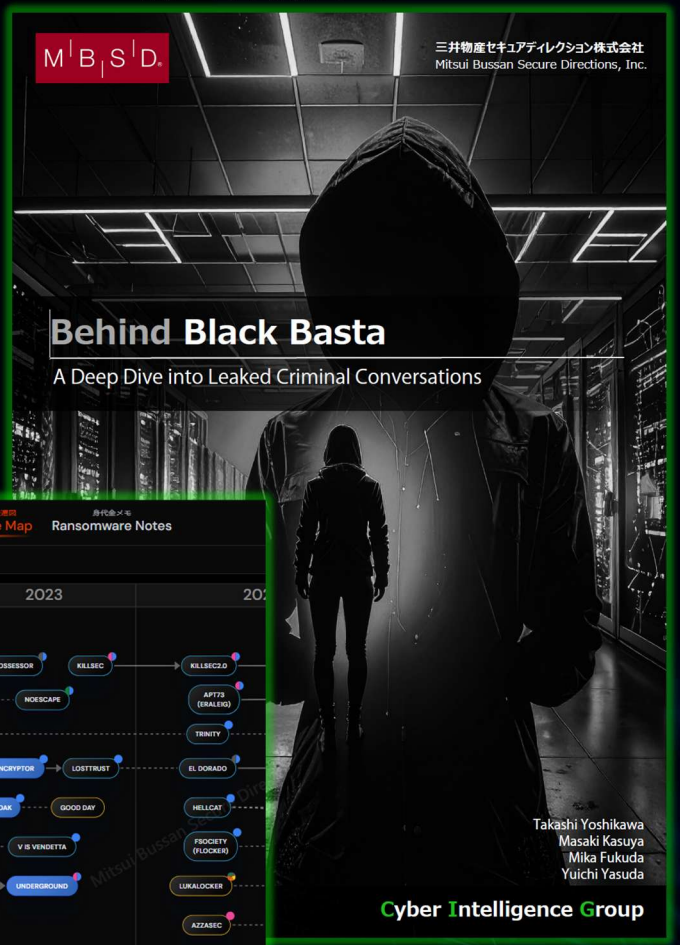
● CIG Ransomware Information Portal (WEBアプリケーション)：
https://www.mbsd.jp/cig-ransomware-portal/

● CIGランサム統計だより：
https://www.mbsd.jp/research/20231023/blog/

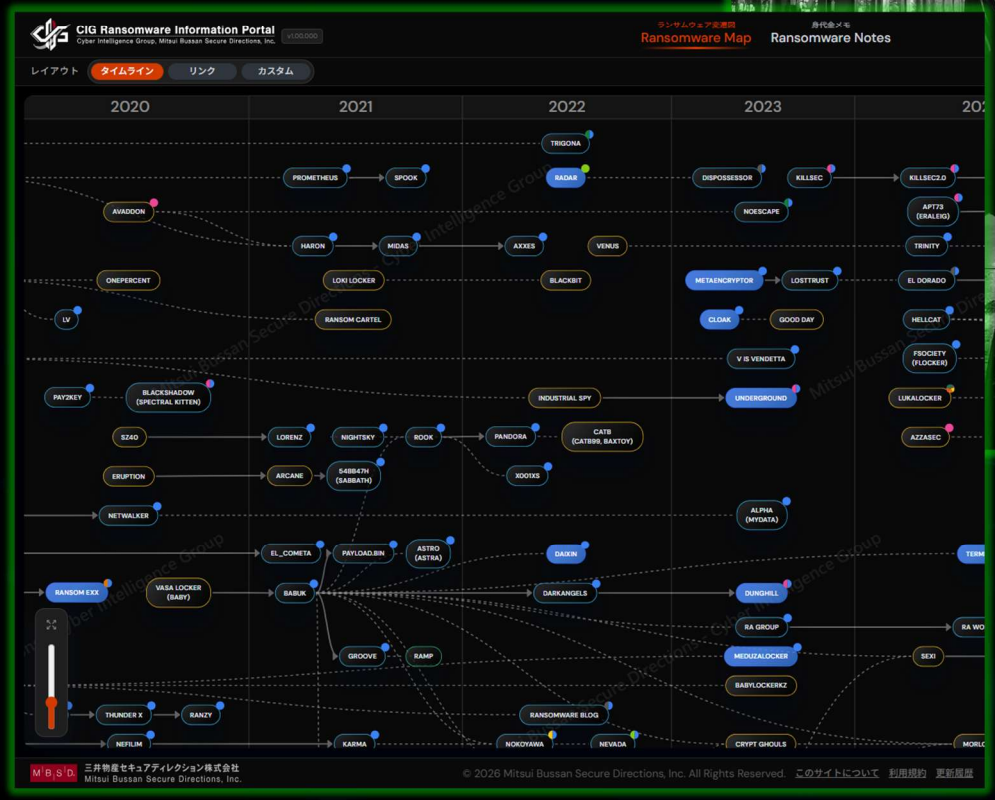
● 技術ブログ：
https://www.mbsd.jp/research/cig/
https://www.mbsd.jp/research/t.yoshikawa/

● 分析レポート：
https://www.mbsd.jp/report

Black Basta 内部チャット分析レポート



CIG Ransomware Information Portal



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

本資料に関する留意事項及び二次利用について

留意事項

・ 攻撃グループや被害組織などについて、正確な情報が公開されていない項目は「(Unknown)」として集計しています。

・各分析における掲載数は、特に注釈がない限り、公表や報道を含めず、リークサイトに掲載された数のみを基にしています。
（日本にフォーカスした一部の表／グラフのみ、公表や報道から判明した数を加味し集計）

・本レポートにおける「国」データは、被害組織の本社所在地情報を元に集計しています。
ただし、本社所在地情報が確認できない場合は、”攻撃された拠点の所在国”もしくは”(Unknown)”として集計しています。

・ 国内被害組織に関する各種データについては、海外拠点（支社／関連会社）を含みます。

・ 業種分類や集計方法を含む本レポートの各データ（値）はMBSD Cyber Intelligence Group (CIG) 独自の観測および集計結果となります。

・ 件数については、攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を基に集計しています。

・ごく一部の、ランサムウェアの使用が明確に確認されていない暴露＆恐喝グループの値も含まれています。

・ これらは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-list/

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