

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8月号 Rev 1.00 (2026年7月分)

2026

7

目次

総括と監視対象（レポート①～④）

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

グローバル統計（レポート⑤～⑬）

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

日本関連組織を対象とした統計（レポート⑬～⑲）

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

中小企業における被害分析（レポート⑲～⑲）

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

多重被害に関する分析（レポート⑲～⑲）

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

業種に関する分析（レポート⑲）

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

その他

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

2026

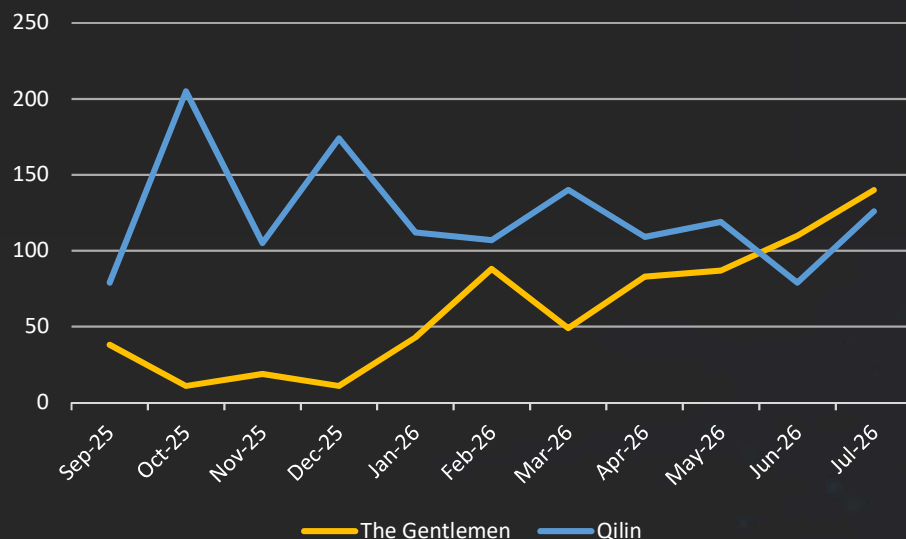
7

総括と監視対象

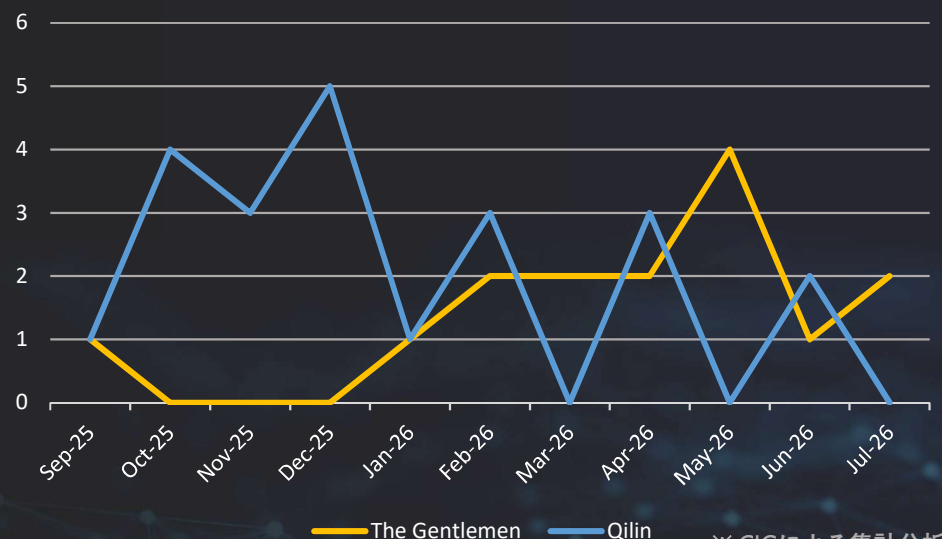
● The Gentlemen の勢力拡大

The Gentlemenは、2025年半ばに活動が表面化したランサムウェア攻撃グループであり、2026年に入ってから、攻撃グループ別の掲載件数で継続して10位以内に入っている。先月には、この一年間にわたり実質的に1位を維持してきたQilinランサムウェアを追い抜き首位に立ち、今月に入っても両者の順位は変わっていない。加えて、2026年には毎月、日本の関連企業をリークサイトに掲載している。日本企業にとっては、Qilin以上に警戒すべき攻撃グループであると言える。2026年5月初旬には、The Gentlemenの内部チャットログとみられるデータがダークフォーラム上に出回った^{※1}。同グループが利用していたホスティング事業者が侵害され、バックエンドやストレージへのアクセスを許したことが原因として指摘されている。しかし、今月時点までの掲載件数の推移を見る限り、活動が衰えた様子は確認できない。

The GentlemenとQilinによる被害組織の掲載数の推移（グローバル版）



The GentlemenとQilinによる被害組織の掲載数の推移（日本企業版）



※ CIGによる集計分析

The Gentlemenは、運営側が脆弱なカーネルドライバを悪用してEDRを無効化する手段を開発し、アフィリエイトへ提供していることが知られている^{※2}。こうした手法はBring Your Own Vulnerable Driver (BYOVD)と呼ばれる。同グループは、関連するエクスプロイトが公開されると、これを速やかに攻撃へ取り込む点に特徴がある。また、初期侵入では脆弱なVPN機器を経由する手口も確認されている。これらの手口を踏まえると、エンドポイントセキュリティ製品のみ依存する防御では、EDRが無効化された時点で有効な検知手段を失いかねない。対策の一つは、BYOVDで悪用される脆弱なカーネルドライバを検知する仕組みの整備である。例えば、既知の脆弱なドライバのハッシュ値をブラックリストに登録し、悪用されないようにする措置が考えられる。加えて、最新のセキュリティパッチを適用し、VPN機器などの脆弱性を解消することも初期侵入を防ぐ上で欠かせない。攻撃者が悪用しにくい環境を整え、維持していくことが、ランサムウェア被害を防ぐうえで引き続き重要である。

※1: (参考情報) <https://www.mbsd.jp/research/20260526/the-gentlemen/>

※2: (参考情報) <https://www.eset.com/us/about/newsroom/research/eset-research-gentlemen-ransomware-gang-edr-killers/>

【VECTとTeamPCPが提携、サプライチェーンで盗んだ認証情報をランサムウェア展開に利用】(出典: Sophos 2026/07/02)

Sophos社は、恐喝グループTeamPCPがサプライチェーン攻撃で窃取した認証情報を、提携先のVECTがランサムウェア展開に利用していたと報告。開発基盤の侵害が後続のランサムウェア攻撃を支える連携を確認。
<https://www.sophos.com/en-us/blog/vect-and-teampcp-partner-for-ransomware-campaigns>

【「GodDamn」ランサムウェア、BYOVDを利用して米国企業を攻撃】(出典: Dark Reading 2026/07/09)

Symantec社は、RaaSグループHyadinaが新ロッカー「GodDamn」の展開時に、Microsoft署名済みの悪意あるドライバーを利用してEDRやウイルス対策製品を無効化していたと報告した。
<https://www.darkreading.com/cyberattacks-data-breaches/goddamn-ransomware-byovd-smite-companies>

【米国各地で複数の被害者から身代金を脅し取り、攻撃を加えたフロリダ州出身のランサムウェア交渉担当者が実刑判決を受ける】(出典: 米司法省 2026/07/09)

米司法省は、被害組織の交渉方針をランサムウェア攻撃グループALPHV/BlackCat側へ漏らし、身代金の最大化を支援したとして、元ランサムウェア交渉担当者に禁錮70カ月が言い渡されたと発表した。
<https://www.justice.gov/opa/pr/florida-ransomware-negotiator-who-extorted-and-attacked-multiple-us-victims-sentenced-prison>

【米国へ引き渡されたアルメニア国籍の人物、Ryukランサムウェア恐喝共謀で有罪答弁】(出典: 米司法省 2026/07/09)

米司法省は、ウクライナから米国へ引き渡されたアルメニア国籍のKaren Serobovich Vardanyanが、2019～2020年にかけて複数の米企業に対しRyukランサムウェアを展開した恐喝共謀事件で有罪を認めたと発表。
<https://www.justice.gov/usao-or/pr/armenian-national-extradited-united-states-pleads-guilty-ransomware-extortion-conspiracy>

【米国・EU・英国、ランサムウェア運営者と支援インフラへの制裁を強化】(出典: Chainalysis 2026/07/14)

米国・EU・英国がランサムウェア関係者への制裁を強化。米国は1VPNとクリプター提供者、EUはTrickbot幹部「Stern」を指定し、運営者と支援インフラの双方へ圧力をかけた。
<https://www.chainalysis.com/blog/cyber-sanctions-trickbot-administrator-july-2026>

【Sophos「State of Ransomware 2026」ーランサムウェアの79%がIDの侵害から開始、脆弱性悪用は首位から降下】(出典: Sophos 2026/07/15)

Sophos社の2026年調査で、ランサムウェア攻撃の79%にID侵害が関与していることが判明。初期侵入経路の首位は4年ぶりに脆弱性悪用から悪意のあるメールへ交代し、ID管理の徹底が急務となる。
<https://www.sophos.com/en-us/blog/sophos-state-of-ransomware-2026>

【JadePufferがAI資産を狙う新ランサムウェア「EncForge」を展開】(出典: Sysdig 2026/07/20)

Sysdig社は、AIエージェント型脅威アクターJADEPUFFERが、AIモデルや学習データを暗号化する新ランサムウェア「ENCFORGE」を展開したと報告。AI開発資産も新たな恐喝対象となりつつある。
<https://www.sysdig.com/blog/jadepuffer-evolves-the-agentic-threat-actor-deploys-ransomware-built-to-destroy-ai-models>

【ランサムウェア集団が主要4ベンダのVPN・ファイアウォールを狙い、初期侵入の主流に】(出典: CyberSecurityNews 2026/07/27)

Cybersecurity Newsは、ランサムウェア集団がPalo Alto Networks、Fortinet、Citrix、Check Pointの境界機器を狙う攻撃を総括。脆弱性公表後の悪用が早期化しており、修正適用と認証情報の見直しが急務だと指摘。
<https://cybersecuritynews.com/ransomware-gangs-attack-vpn>

【北朝鮮Lazarusがランサムウェア集団Gunraとツール・インフラを共有、韓国4機関が合同警告】(出典: The Record 2026/07/30)

韓国4機関は、諜報目的のLazarusグループと恐喝目的のGunraランサムウェア集団が共通の攻撃ツールやC2基盤、SSHキーを用いたと警告。AhnLab社は技術的関連を指摘したが、協力関係や同一主体とは断定していない。
<https://therecord.media/north-korea-hackers-ransomware>

【Microsoft TeamsでITサポートを騙る音声フィッシングからChaosランサムウェアへ】(出典: BleepingComputer 2026/07/30)

Sophos社は、Microsoft Teamsの通話でITサポートを騙る音声フィッシングからChaosランサムウェア展開に至る攻撃を報告。遠隔サポートツールの利用統制と、正規の社内IT問い合わせ経路の周知が重要となる。
<https://www.bleepingcomputer.com/news/security/microsoft-teams-vishing-attacks-lead-to-chaos-ransomware-attacks>

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：350 ^(※1) ^(※2)

→ 当月リークサイト掲載の活動を確認した攻撃グループ数：64

● 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)

ODAPT
ODAY
Omega (Omega)
8BASE
Abyss
AilLock
AKIRA
AKO
ALP-001
Alpha (MYDATA)
AlphV (BlackCat)
Anubis
Apos Security
APT73 (Eraleig)
ARACHNA
ARCUS MEDIA
Argonauts
Arkana
ARVINCLUB
Astro (Astra)
AtomSilo
AUDIT
AURORA
Avaddon
AvosLocker
AWARE
Axxes
AzzaSec
Babuk
Babuk (2025)
BASHE
BAVACAI
BEAST
Benzona
BERT
BianLian
BL00DY (BLOODY)
BL4CKTOR (BLACKTOR)
Black Basta
BlackByte
BLACKDOLPHIN
BlackField
BlackLock
BlackMatter

Black Nevas
Blackout
BLACKSHRANTAC
BlackSuit
BLACKWATER
Black X
BLUEBOX
BLUESKY
BOOBA
BOTLOCK
Brain Cipher
BRAVOX
Brotherhood
Bully
BUSINESS DATA LEAKS
CACTUS
Cephalus
CHAOS (2025)
CHEERS
CHILLELOCKER (ARCRYPTER)
CHORT
Cicada3301
CiphBit
CipherForce
CipherLocker
CLOP (CLOP)
Cloak
CMD ORGANIZATION
COINBASE CARTEL
Conti
Cooming Project
Crazy Hunter Team
CROSSLOCK
● CRPX0
CRYO
CryptBB
CRYPTNET
CRYPTO24
CryptOn
Cuba
CYCLOPS
● DIR
D4RK4RMY
DAGON

DAIXIN
dAn0n (danon)
Dark Angels
Darkbit
● DARKMATTER
DARKPOWER
DarkRace
DarkRypt
DARK SHINIGAMIS
DarkSide
Dark Vault
DataCarry
DATAKEEPER
DEADLOCK
Desolator
DEVMAN
DEVMAN 2.0
Dire Wolf
DISPOSSESSOR[DATABROKER]
Donex
Donut Leaks
● DOOMMAGEDDON
DoppelPaymer
dotAdmin
DragonForce
DragonRansomware
DREAMFYRE
DUNGHILL
eCh0raix (eChoraix)
EL_COMETA
EL DORADO
EMBARGO
Endurance
ENTROPY
Everest
● EXFILSQUAD
EXITIUM
FOG
Frag
FSOCIETY / FLOCKER
FSTEAM
FulcrumSec
Funksec
● GAMMAX

GD LockerSec
Genesis
GLOBAL
● GLOBAL SECRET GROUP
Grief
Groove
Gunra / Fresh Gunra
HANDARA [HACKTIVIST]
Haron
HELLCAT
Helldown
HelloGookie
HITLER (AGLOBGVYCG)
Hive
HolyGhost
Hotarus
Hunters International
HYFLOCK
ICARUS
ICEFIRE
IMN Crew
INC Ransom
Insane
INSOMNIA
INTERLOCK
J GROUP
KAIROS
Karakurt
Karma
Kawa4096
Kazu
KILLSEC
Kittykatkrew
Knight
Kraken (HelloKitty)
KRYBIT
Kryptos
Kyber
LAMASHTU
LAMBDA
La Piovra
LAPSUS\$
LAPSUS\$ Group
LEAK BAZAAR

LeakedData (Silent Ransom Group)
LEAKNET
LILITH
Linkc
LockBit
LOKI
Lorenz
LostTrust
LunaLock
LV
Lynx
M3RX
MADCAT
MAD LIBERATOR
MALAS
MALEKTEAM
Mallox
MAMONA RIP
MBC
Medusa
MEDUZA LOCKER
MEOW
Metaencryptor
MIDAS
MIGA
Mindware
Minteye
MNT6
MOGILEVICH [FRAUD]
MOISHA
Money Message
Monti
Morpheus
MORTAR
MOUNT LOCKER
MS13-089
N3TWORK (NETWORM)
N4UGHTYSEC (NAUGHTYSEC)
NASIR SECUTRIY
Nefilim
NetRunner
NEVADA
NightSky
NightSpire

NITROGEN
NoEscape
Nokoyawa
NONAME (VFOXX)
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
RANSOMCORTX
Ransomed.vc
Ransom EXX
RansomHouse

RansomHub
Ransomware Blog
RANZY
RA WORLD
Raznatovic
REDACT
RedAlert (N13V)
Red Ransomware Group (Red CryptoApp)
Relic
REVIL (SODINOKIBI)
Reynolds
Rhysida
RISEN
ROOK
root
Royal
Rransom
RunSomeWares
RUSTY LOCKER
SABBATH (54BB47H)
SABBA
SAFEPAY
SARCOMA
SATAN LOCK
SATANLOCK V2
Scattered LAPSUS\$ Hunters
Secp0
● SECTION9
Securotrop
SenSayQ
SETTRA
SEVYWARE
SHADOWBYT3\$
Shaoleaks
● SHIBA
SHINYHUNTERS
Sicarii
SIEGEDSEC
Silent
Sinobi
SKIRA TEAM
SLUG
Snatch
SOLIDBIT

Space Bears
Sparta
Spook
SPY CORPORATE
STORMOUS
SUGAR
Suncrypt
SYNACK
TeamXXX
TENGU
Termite
The Gentlemen
THE GREEN BLOOD GROUP
ThreeAM (3AM)
TIMC
TITAN
TridentLocker
TRIGONA
TRINITY
Triple X
TRISEC
Underground
UnSafe
Valencia
VanHelsing
VanirGroup
Vect
Vice Society
V IS VENDETTA
VSOP
Wallstreet
WALocker
Warlock
WEREWOLVES
Weyhro
WORLD LEAKS
x001xs
XING TEAM
XP95
Yanluowang
Yurei
Zeon
Zero Tolerance

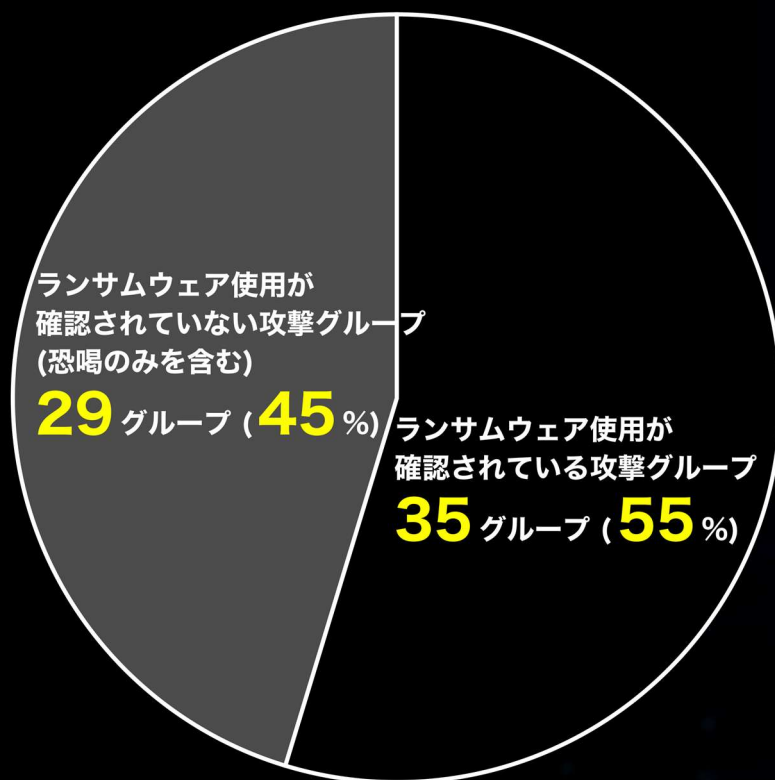
※1) レポート公開月に出現した攻撃グループは次月号に反映

※2) 活動停止した攻撃グループを含む

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 **7**月)

(※当月にリークサイト掲載を確認した攻撃グループ全 **64**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7月に活動中である事が確認された全64グループにおけるランサムウェア使用の割合の内訳を示した図である。

年間統計

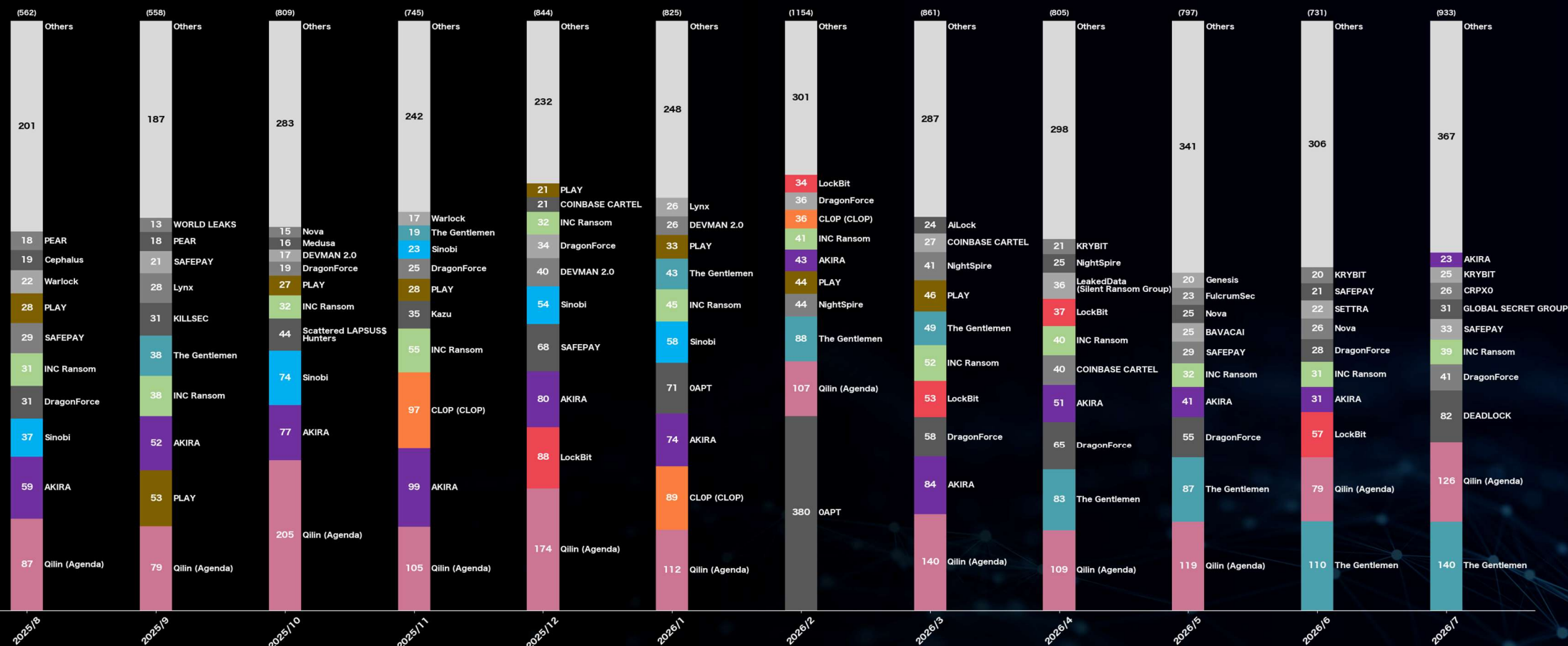
(全世界)

2026

7

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8月～2026年7月)



攻撃グループ 月別統計

(全世界) (過去3ヶ月分)

2026

7

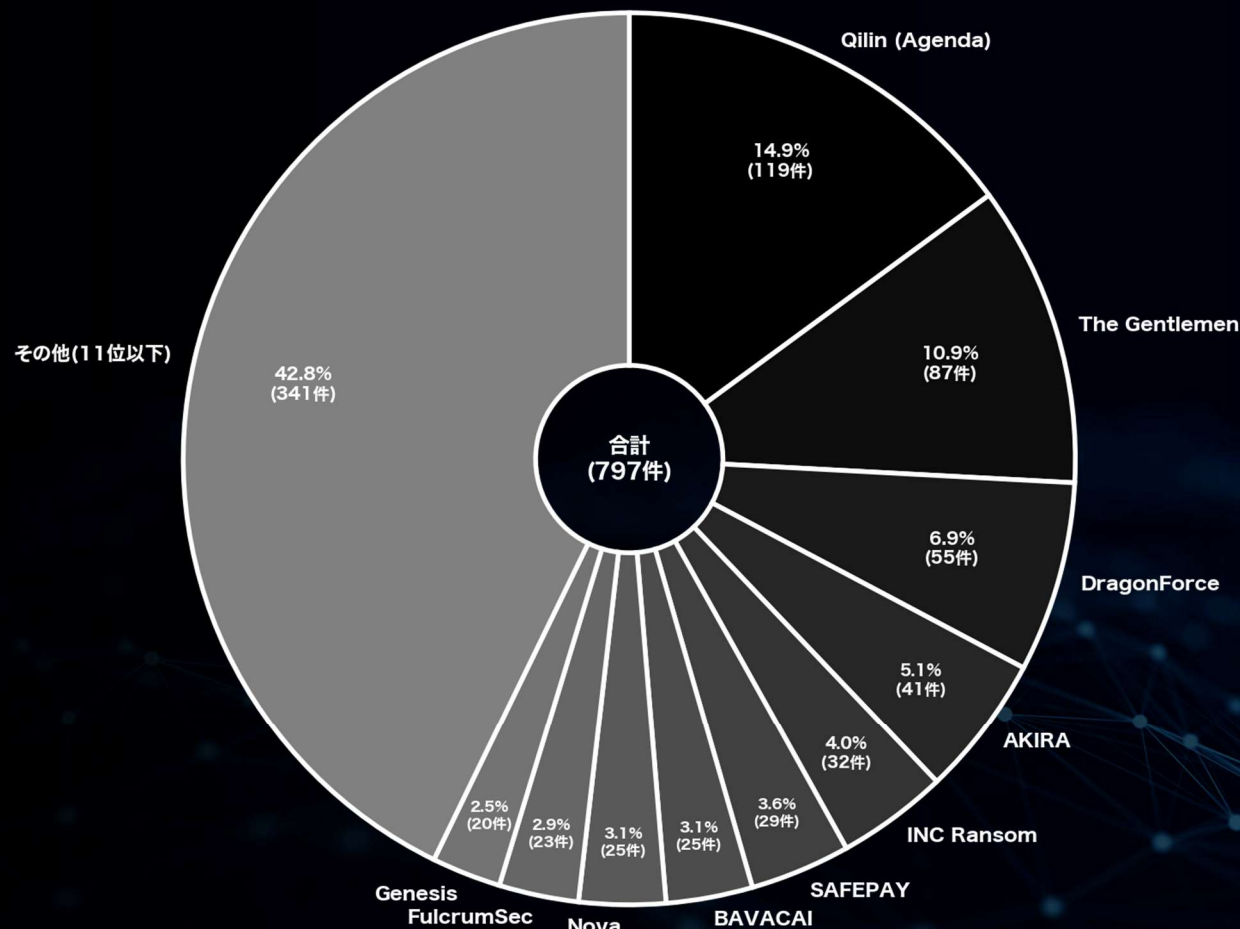
月別内訳 攻撃グループ TOP10 (全世界)

(2026年 5 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)	119	14.9	+ 10
The Gentlemen	87	10.9	+ 4
DragonForce	55	6.9	- 10
AKIRA	41	5.1	- 10
INC Ransom	32	4.0	- 8
SAFEPAY	29	3.6	+ 19
BAVACAI	25	3.1	+ 25
Nova	25	3.1	+ 18
FulcrumSec	23	2.9	+ 23
Genesis	20	2.5	+ 18

▼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)



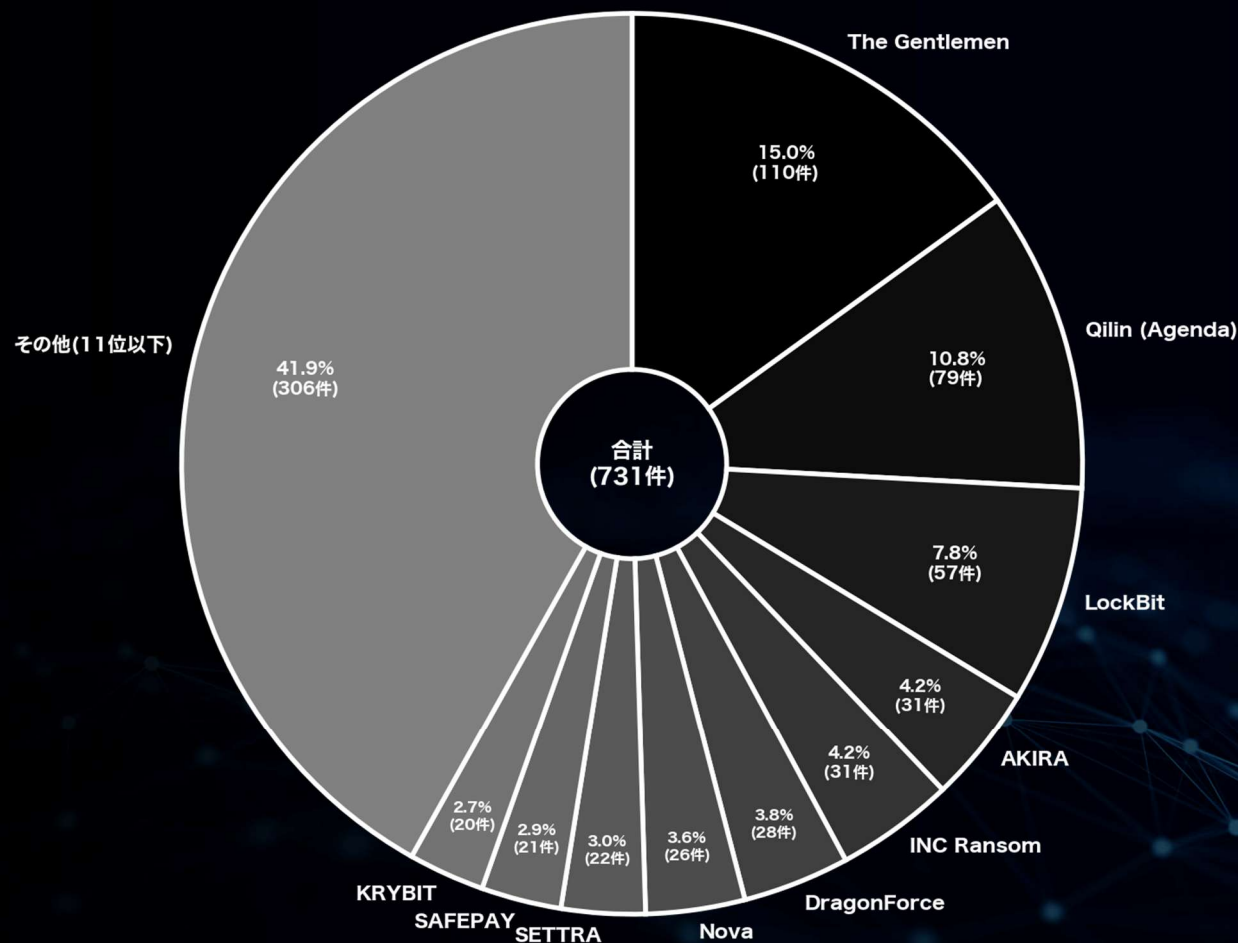
月別内訳 攻撃グループ TOP10 (全世界)

(2026年 6 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)
The Gentlemen	110	15.0	+ 23
Qilin (Agenda)	79	10.8	- 40
LockBit	57	7.8	+ 42
AKIRA	31	4.2	- 10
INC Ransom	31	4.2	- 1
DragonForce	28	3.8	- 27
Nova	26	3.6	+ 1
SETTRA	22	3.0	+ 22
SAFEPAY	21	2.9	- 8
KRYBIT	20	2.7	+ 5

▼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)



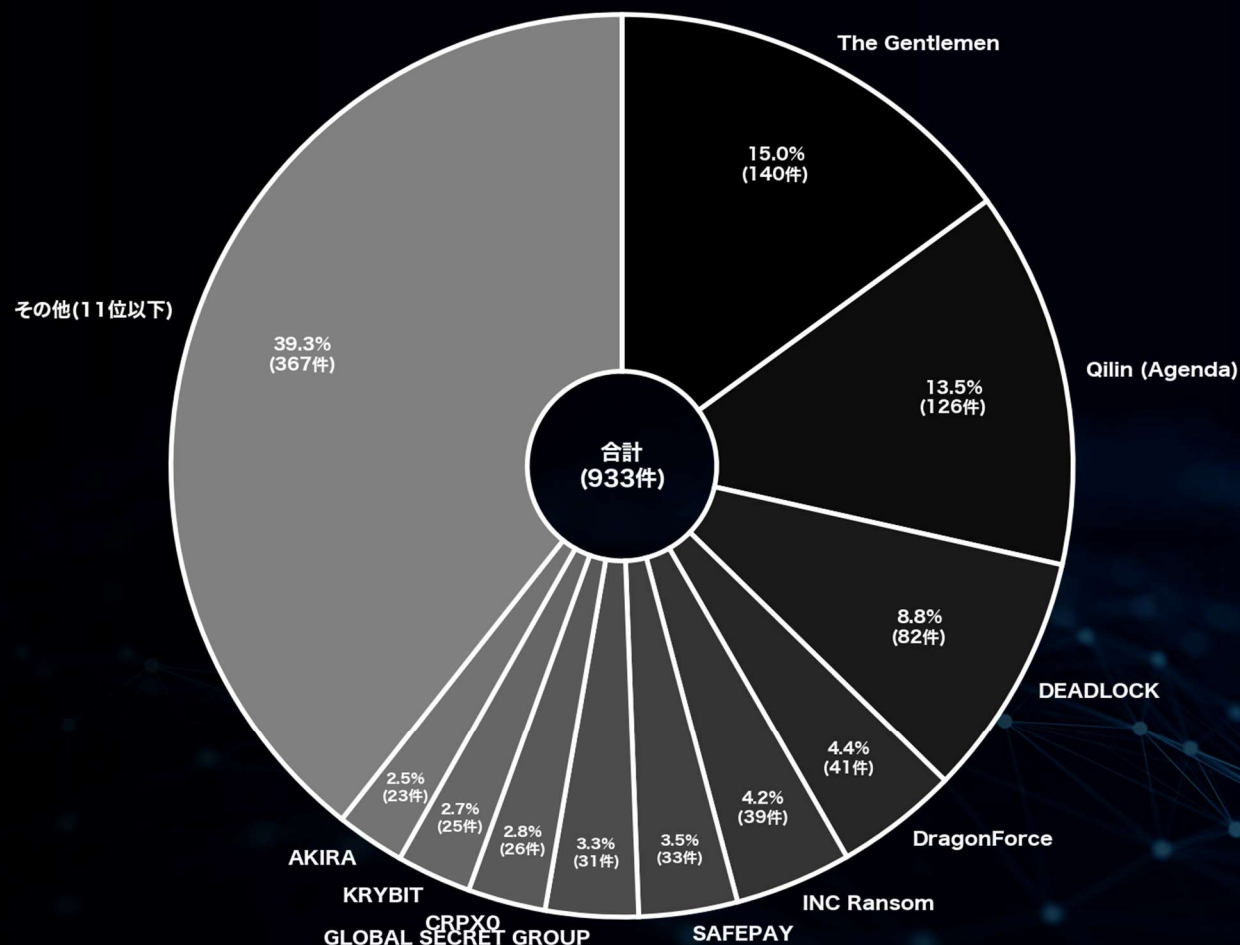
月別内訳 攻撃グループ TOP10 (全世界)

(2026年 7 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)
The Gentlemen	140	15.0	+ 30
Qilin (Agenda)	126	13.5	+ 47
DEADLOCK	82	8.8	+ 65
DragonForce	41	4.4	+ 13
INC Ransom	39	4.2	+ 8
SAFEPAY	33	3.5	+ 12
GLOBAL SECRET GROUP	31	3.3	+ 31
CRPX0	26	2.8	+ 26
KRYBIT	25	2.7	+ 5
AKIRA	23	2.5	- 8

▼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)



被害国 月別統計

(全世界) (過去3ヶ月分)

2026

7

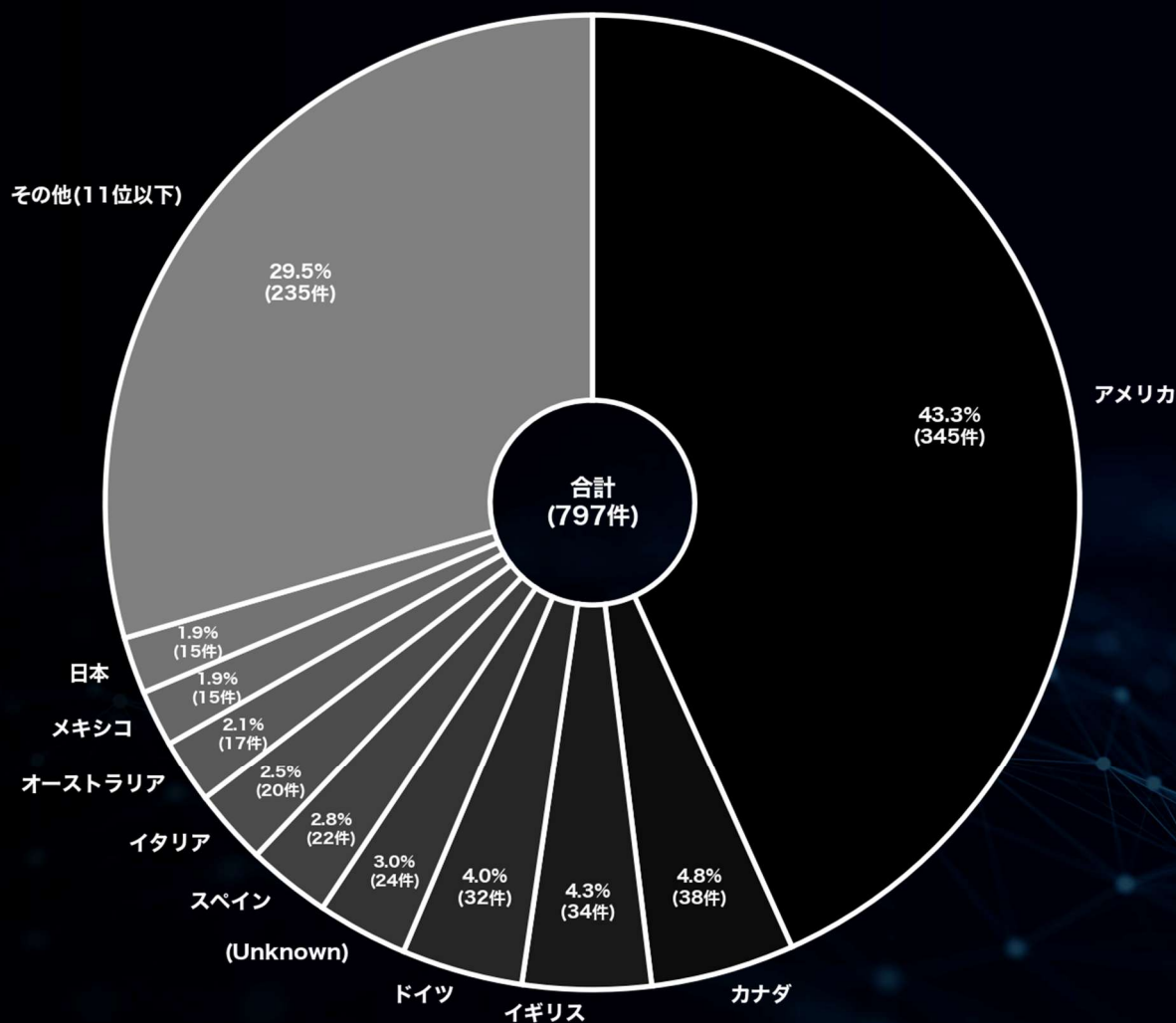
月別内訳 被害国TOP10 (全世界)

(2026年 5 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	345	43.3	+ 29
カナダ	38	4.8	+ 8
イギリス	34	4.3	± 0
ドイツ	32	4.0	- 6
(Unknown)	24	3.0	- 15
スペイン	22	2.8	- 1
イタリア	20	2.5	- 7
オーストラリア	17	2.1	- 5
メキシコ	15	1.9	+ 9
日本	15	1.9	+ 3

▼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)



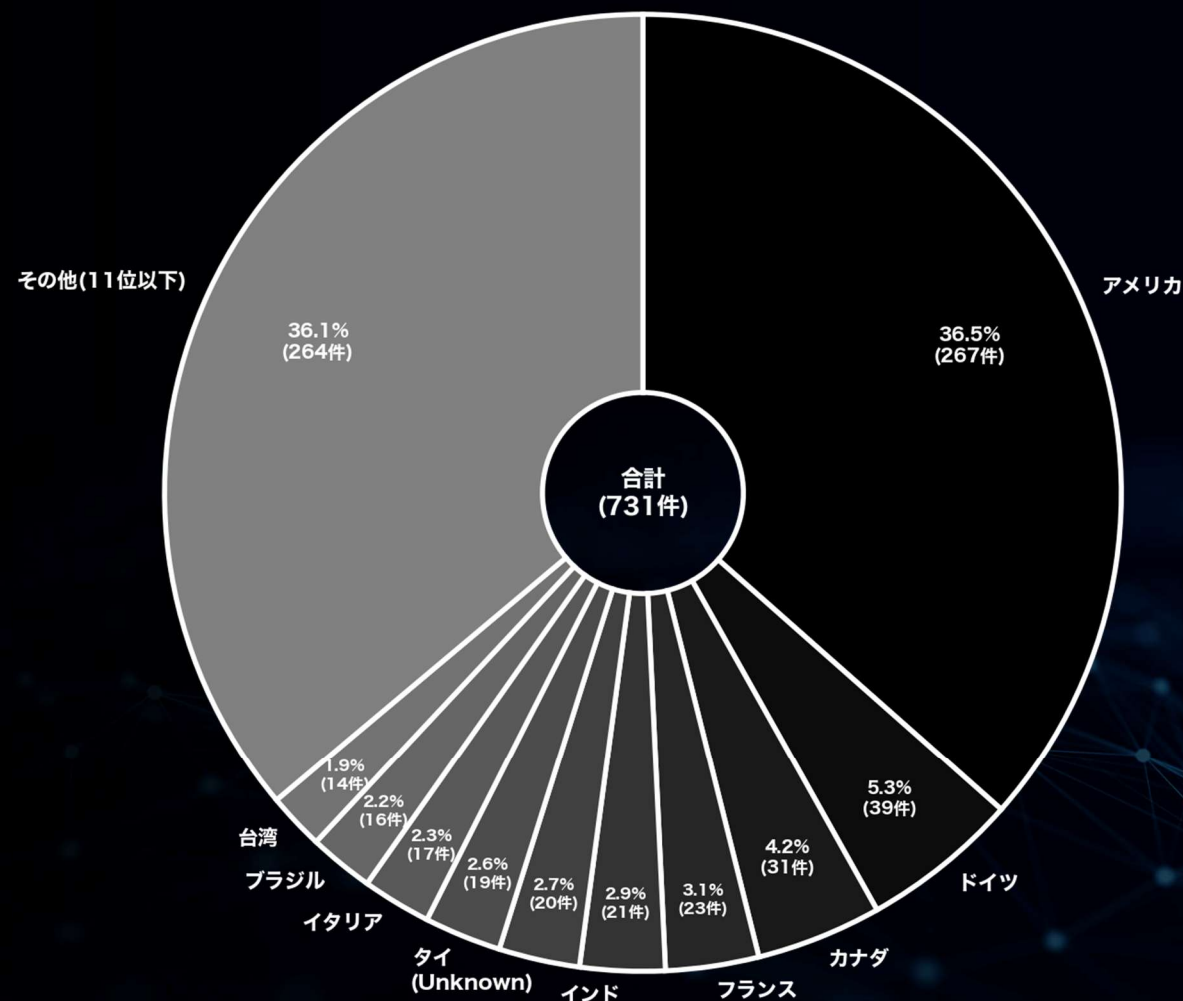
月別内訳 被害国TOP10 (全世界)

(2026年 6 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	267	36.5	- 78
ドイツ	39	5.3	+ 7
カナダ	31	4.2	- 7
フランス	23	3.1	+ 11
インド	21	2.9	+ 8
(Unknown)	20	2.7	- 4
タイ	19	2.6	+ 6
イタリア	17	2.3	- 3
ブラジル	16	2.2	+ 4
台湾	14	1.9	+ 6

▼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)



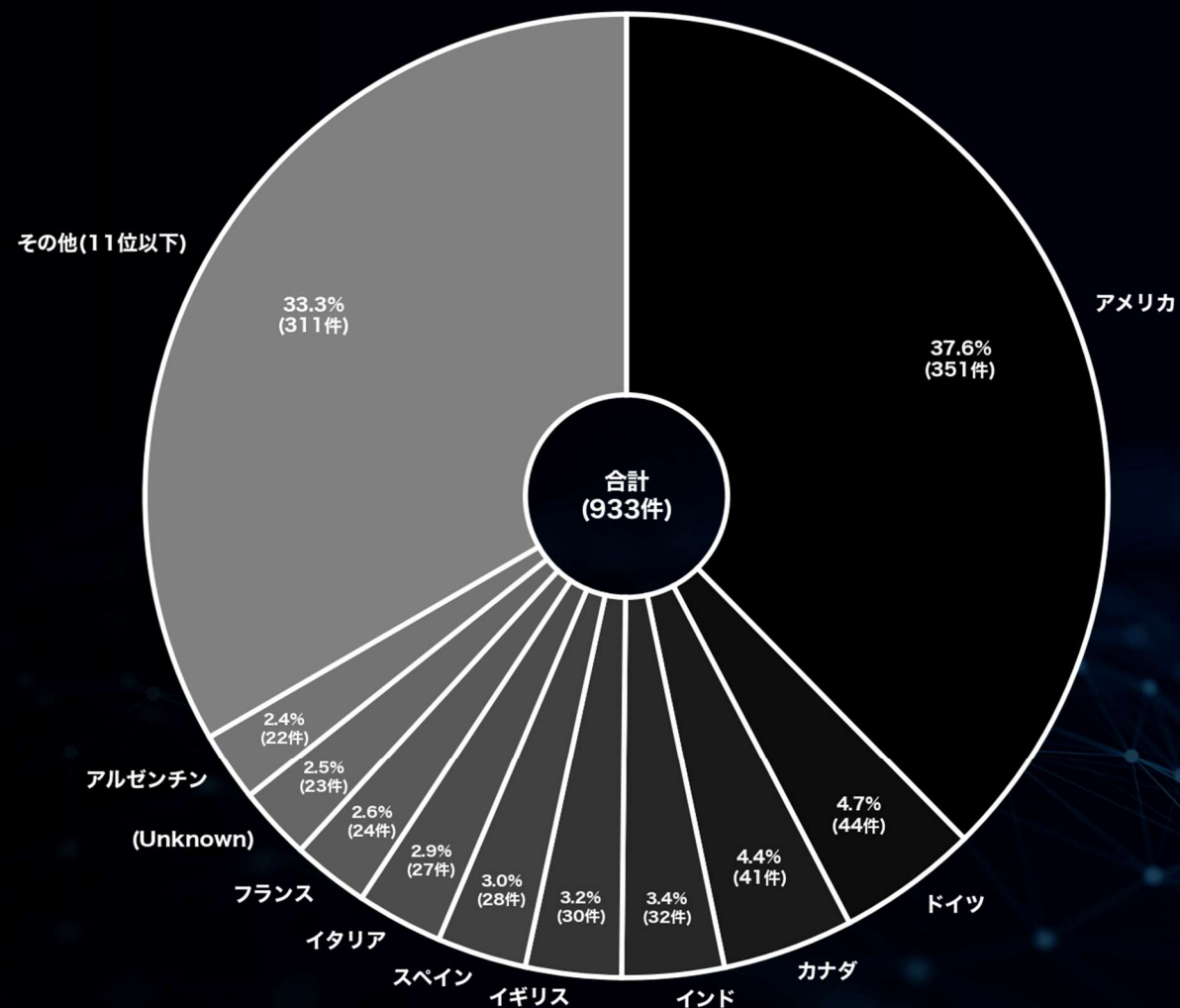
月別内訳 被害国TOP10 (全世界)

(2026年 7 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	351	37.6	+ 84
ドイツ	44	4.7	+ 5
カナダ	41	4.4	+ 10
インド	32	3.4	+ 11
イギリス	30	3.2	+ 17
スペイン	28	3.0	+ 17
イタリア	27	2.9	+ 10
フランス	24	2.6	+ 1
(Unknown)	23	2.5	+ 3
アルゼンチン	22	2.4	+ 14

▼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)



被害国 月別統計

(アジア) (過去3ヶ月分)

2026

7

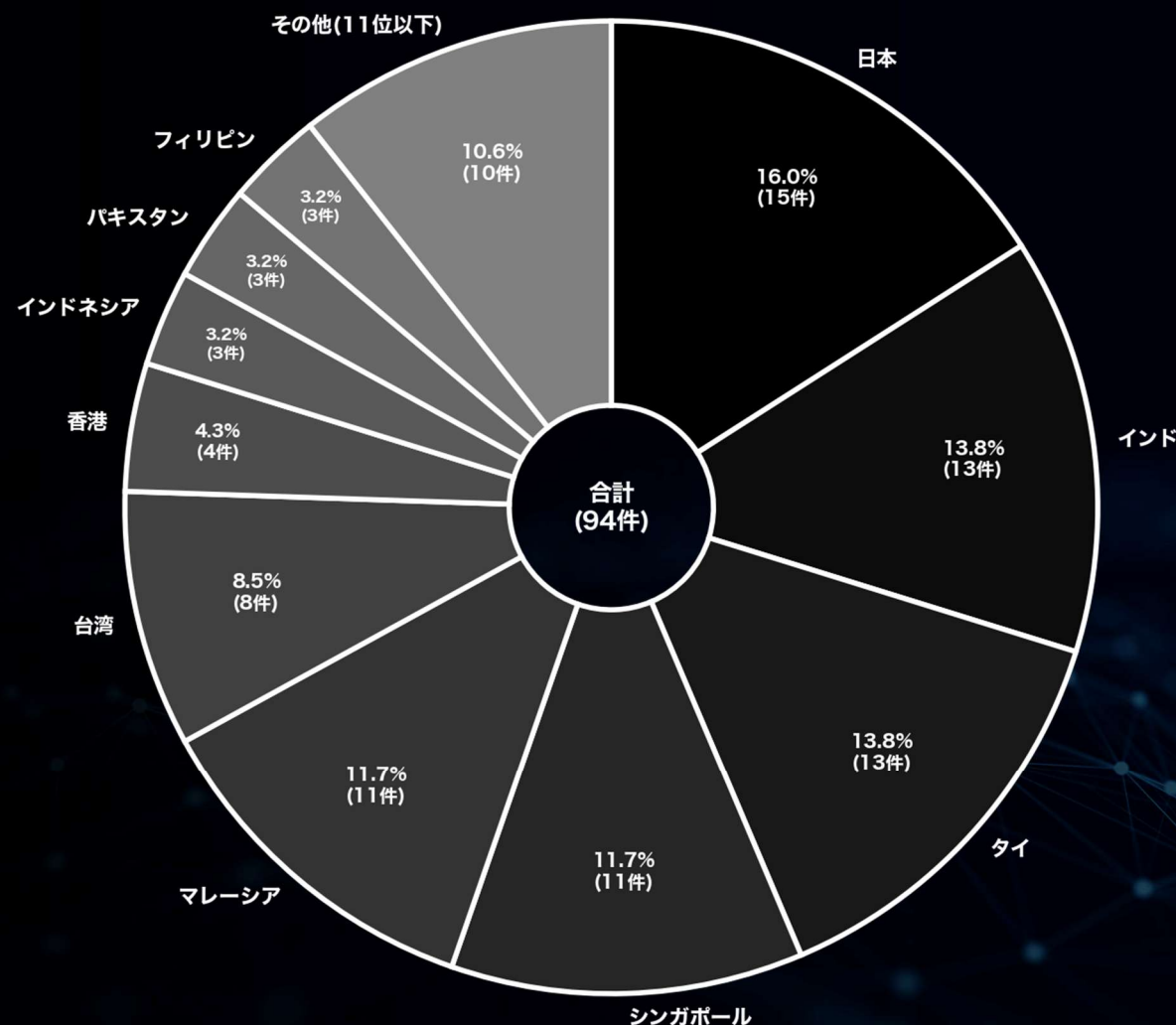
月別内訳 被害国TOP10 (アジア)

(2026年 5 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	15	16.0	+ 3
インド	13	13.8	+ 2
タイ	13	13.8	- 1
シンガポール	11	11.7	+ 8
マレーシア	11	11.7	+ 4
台湾	8	8.5	- 1
香港	4	4.3	- 3
インドネシア	3	3.2	- 7
パキスタン	3	3.2	+ 1
フィリピン	3	3.2	- 1

▼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)



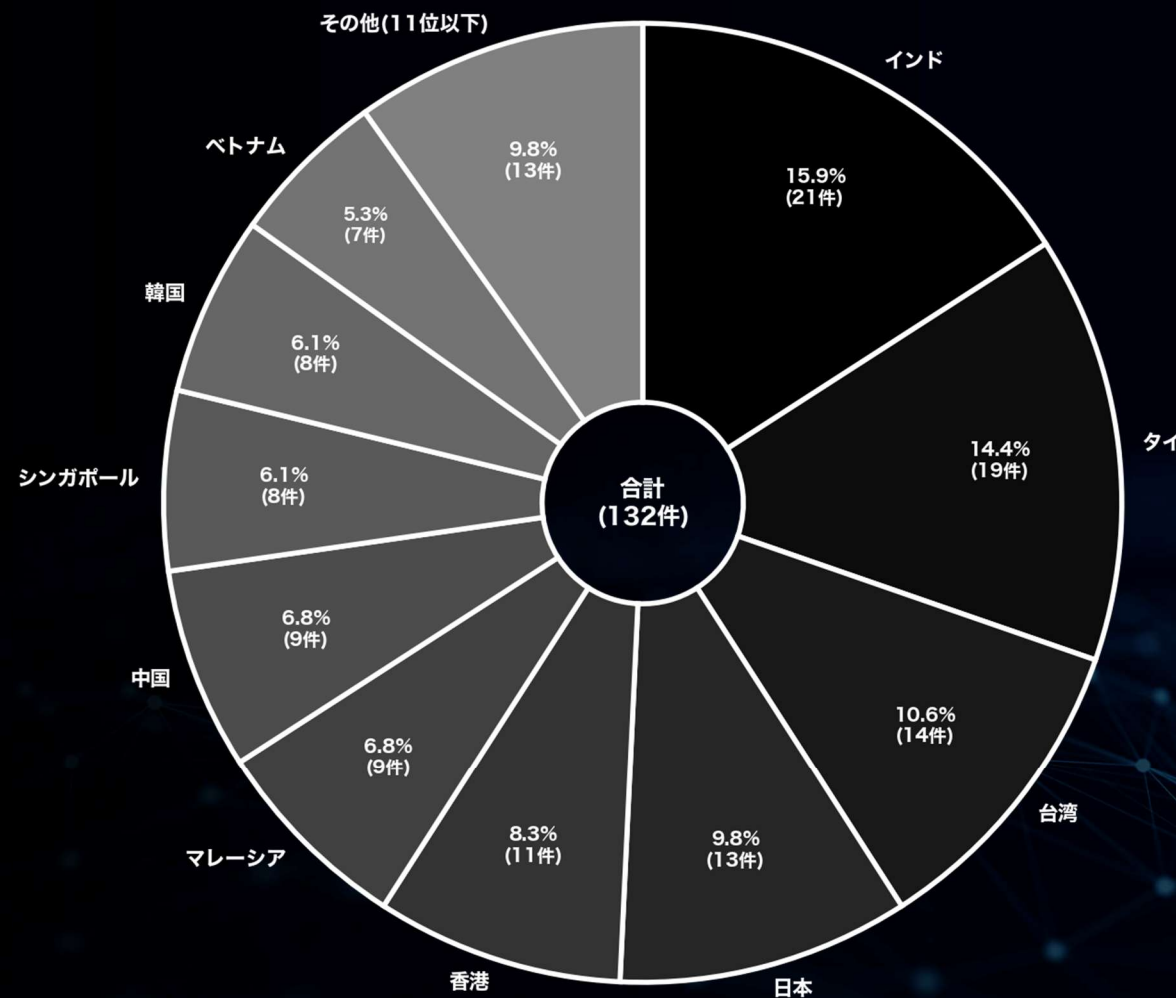
月別内訳 被害国TOP10 (アジア)

(2026年 6 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	21	15.9	+ 8
タイ	19	14.4	+ 6
台湾	14	10.6	+ 6
日本	13	9.8	- 2
香港	11	8.3	+ 7
マレーシア	9	6.8	- 2
中国	9	6.8	+ 6
シンガポール	8	6.1	- 3
韓国	8	6.1	+ 5
ベトナム	7	5.3	+ 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)



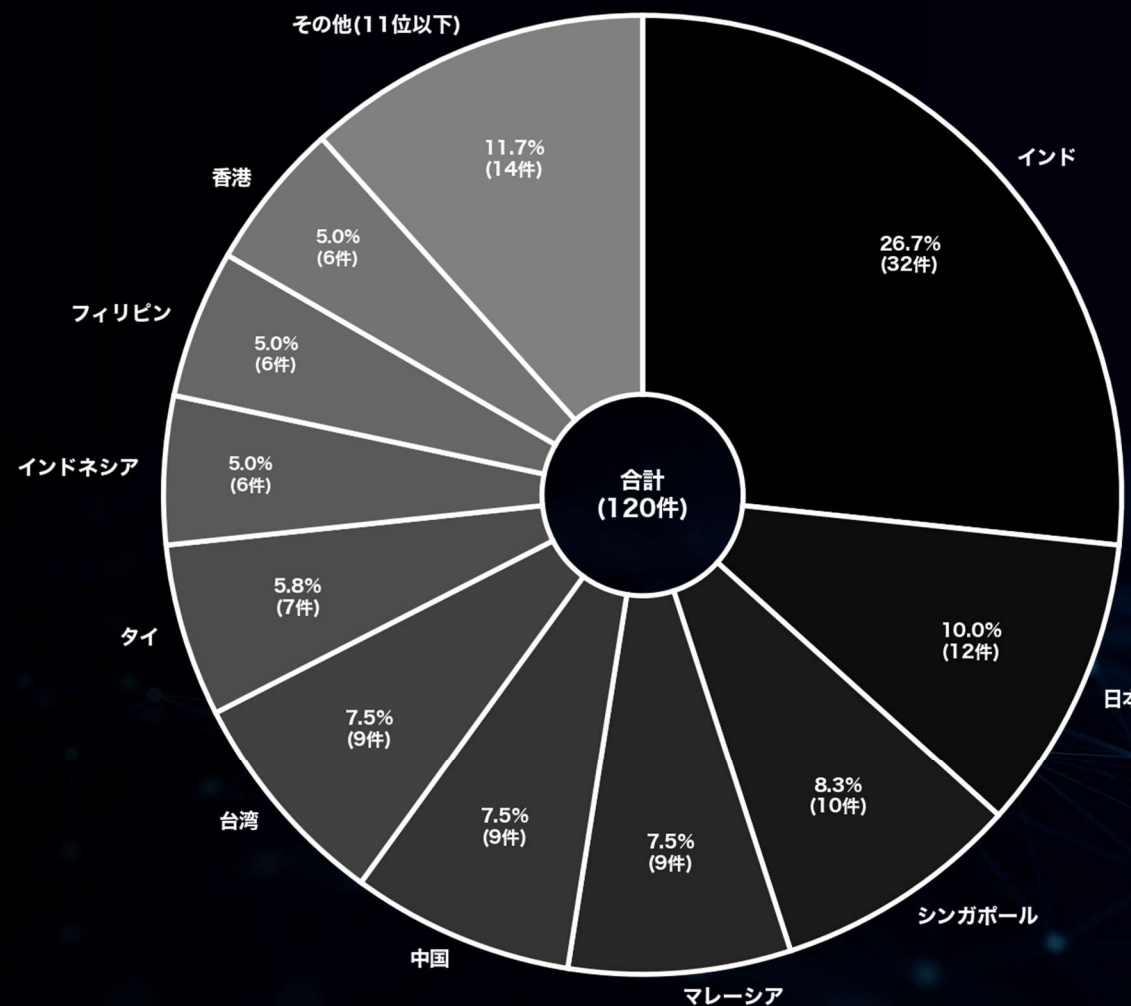
月別内訳 被害国TOP10 (アジア)

(2026年 7 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	32	26.7	+ 11
日本	12	10.0	- 1
シンガポール	10	8.3	+ 2
マレーシア	9	7.5	± 0
中国	9	7.5	± 0
台湾	9	7.5	- 5
タイ	7	5.8	- 12
インドネシア	6	5.0	+ 1
フィリピン	6	5.0	+ 4
香港	6	5.0	- 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)



業種 月別統計

(全世界) (過去3ヶ月分)

2026

7

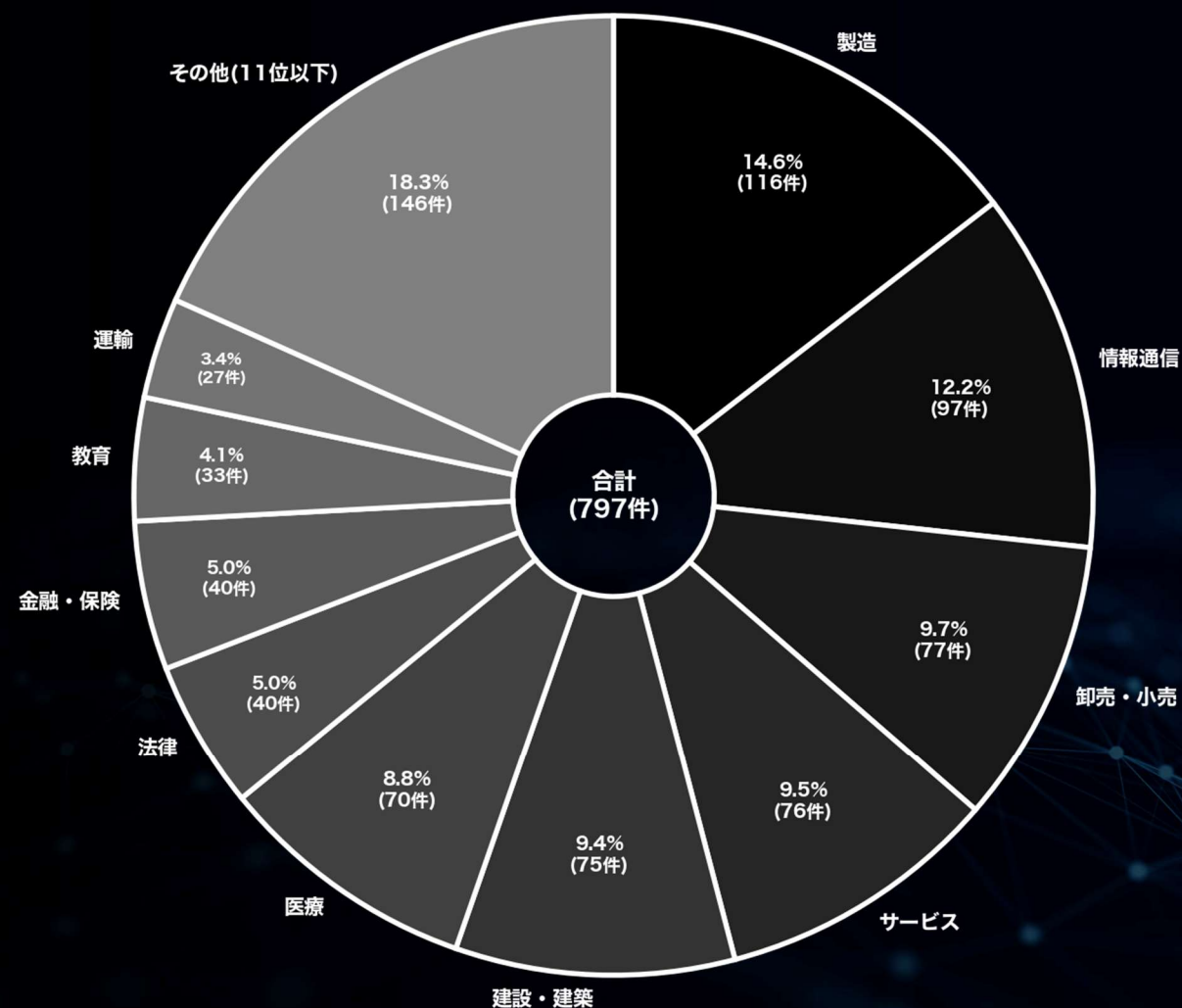
月別内訳 業種 TOP10 (全世界)

(2026年 5 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	116	14.6	- 16
情報通信	97	12.2	+ 20
卸売・小売	77	9.7	+ 12
サービス	76	9.5	+ 1
建設・建築	75	9.4	+ 6
医療	70	8.8	- 2
法律	40	5.0	- 6
金融・保険	40	5.0	+ 1
教育	33	4.1	+ 10
運輸	27	3.4	+ 2

▼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)



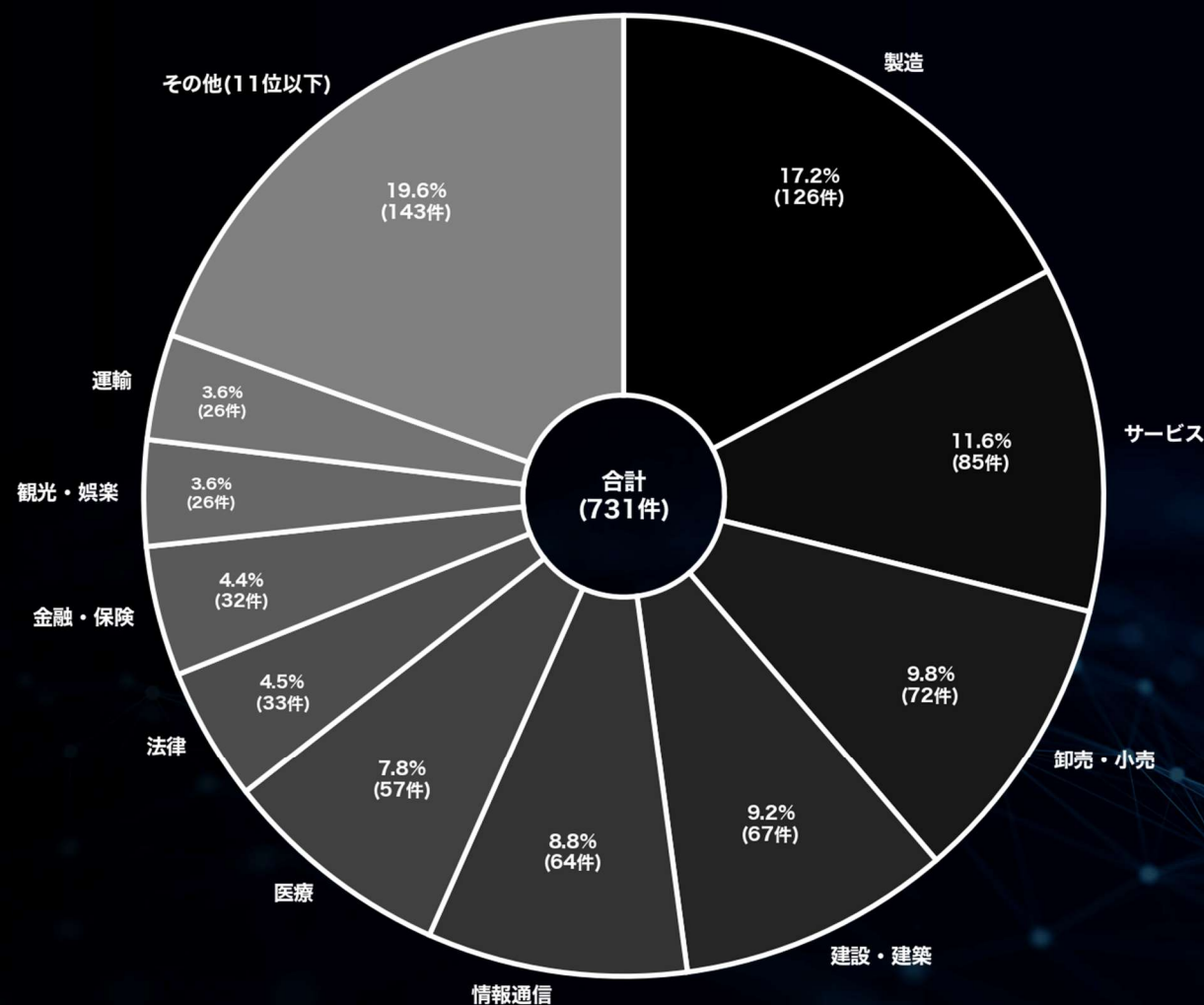
月別内訳 業種 TOP10 (全世界)

(2026年 6 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	126	17.2	+ 10
サービス	85	11.6	+ 9
卸売・小売	72	9.8	- 5
建設・建築	67	9.2	- 8
情報通信	64	8.8	- 33
医療	57	7.8	- 13
法律	33	4.5	- 7
金融・保険	32	4.4	- 8
観光・娯楽	26	3.6	+ 11
運輸	26	3.6	- 1

▼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)



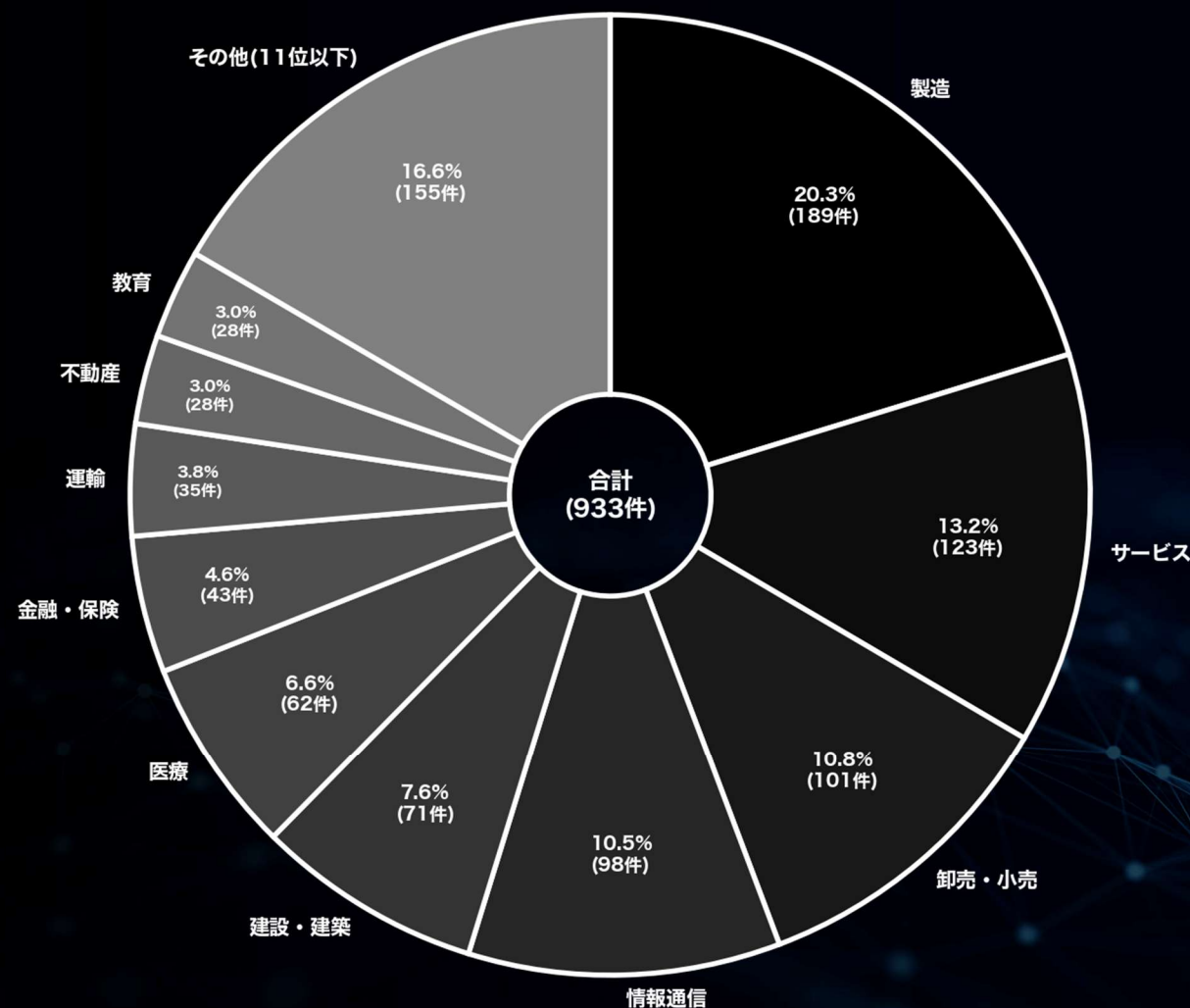
月別内訳 業種 TOP10 (全世界)

(2026年 7 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	189	20.3	+ 63
サービス	123	13.2	+ 38
卸売・小売	101	10.8	+ 29
情報通信	98	10.5	+ 34
建設・建築	71	7.6	+ 4
医療	62	6.6	+ 5
金融・保険	43	4.6	+ 11
運輸	35	3.8	+ 9
不動産	28	3.0	+ 7
教育	28	3.0	+ 3

▼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)



被害数の推移に関する統計

(全世界及び国内)

2026

7

被害数の推移 (全世界及び国内)

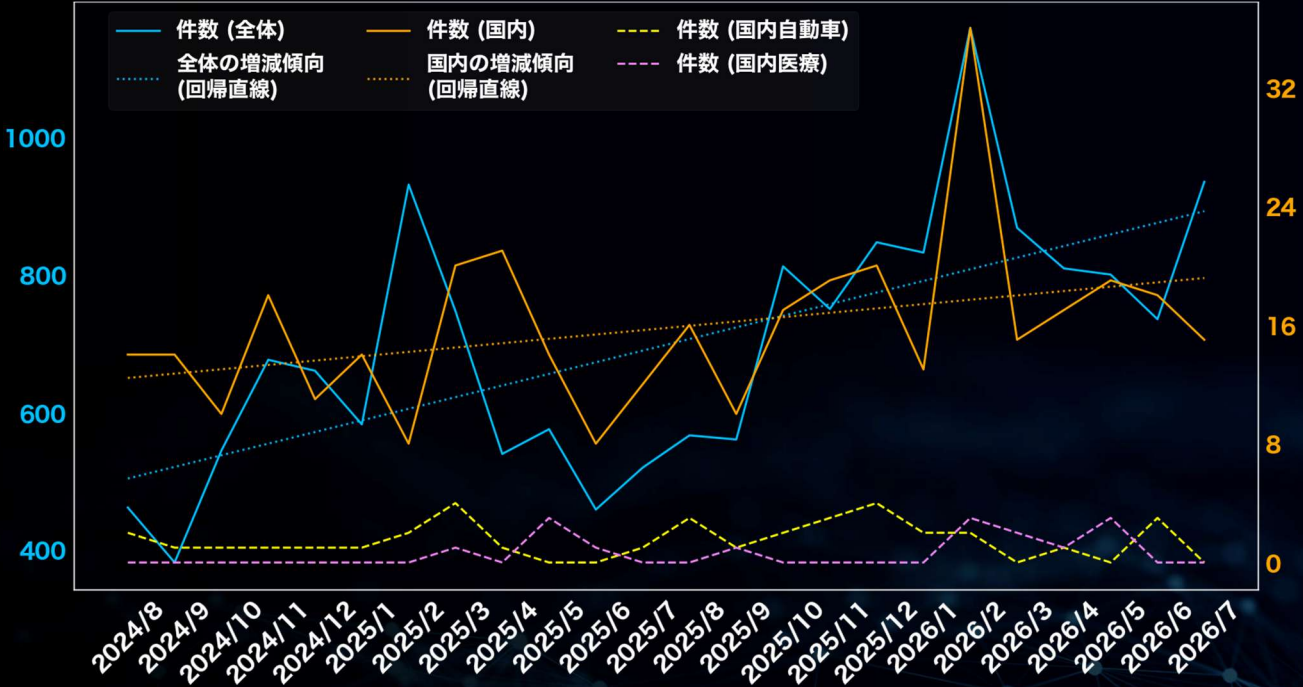
(過去2年間／2024年8月～2026年7月)

※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)
2024/8	462	14	2	0
2024/9	382	14	1	0
2024/10	545	10	1	0
2024/11	677	18	1	0
2024/12	661	11	1	0
2025/1	583	14	1	0
2025/2	932	8	2	0
2025/3	748	20	4	1
2025/4	540	21	1	0
2025/5	576	14	0	3
2025/6	459	8	0	1
2025/7	520	12	1	0
2025/8	567	16	3	0
2025/9	561	10	1	1
2025/10	813	17	2	0
2025/11	751	19	3	0
2025/12	848	20	4	0
2026/1	833	13	2	0
2026/2	1160	36	2	3
2026/3	869	15	0	2
2026/4	810	17	1	1
2026/5	801	19	0	3
2026/6	736	18	3	0
2026/7	936	15	0	0
合計	16770	379	36	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)

2026

7

資本金別の統計

(国内)

資本金別（国内）

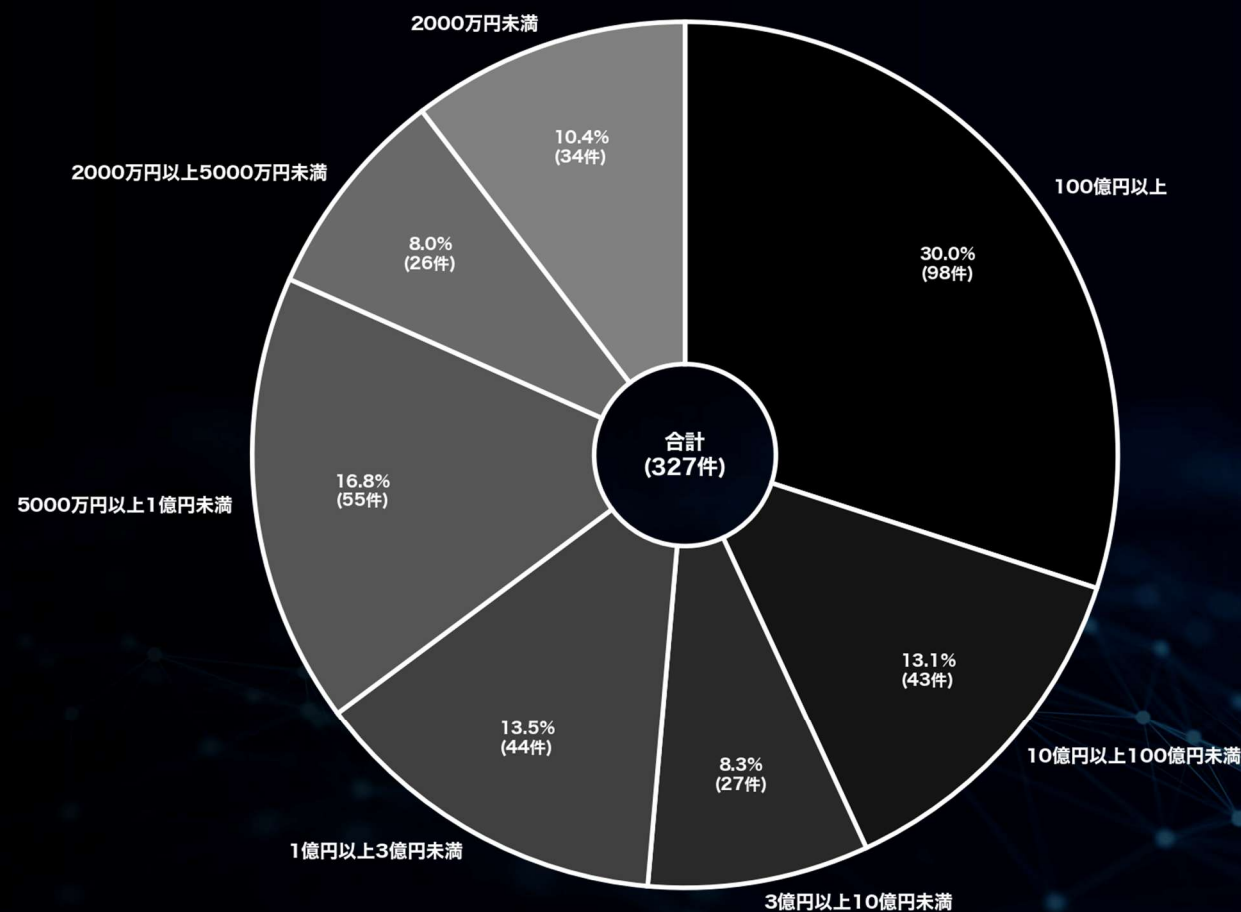
（過去2年間／2024年8月～2026年7月）

※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	98	30.0
10億円以上100億円未満	43	13.1
3億円以上10億円未満	27	8.3
1億円以上3億円未満	44	13.5
5000万円以上1億円未満	55	16.8
2000万円以上5000万円未満	26	8.0
2000万円未満	34	10.4

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）

2026

7

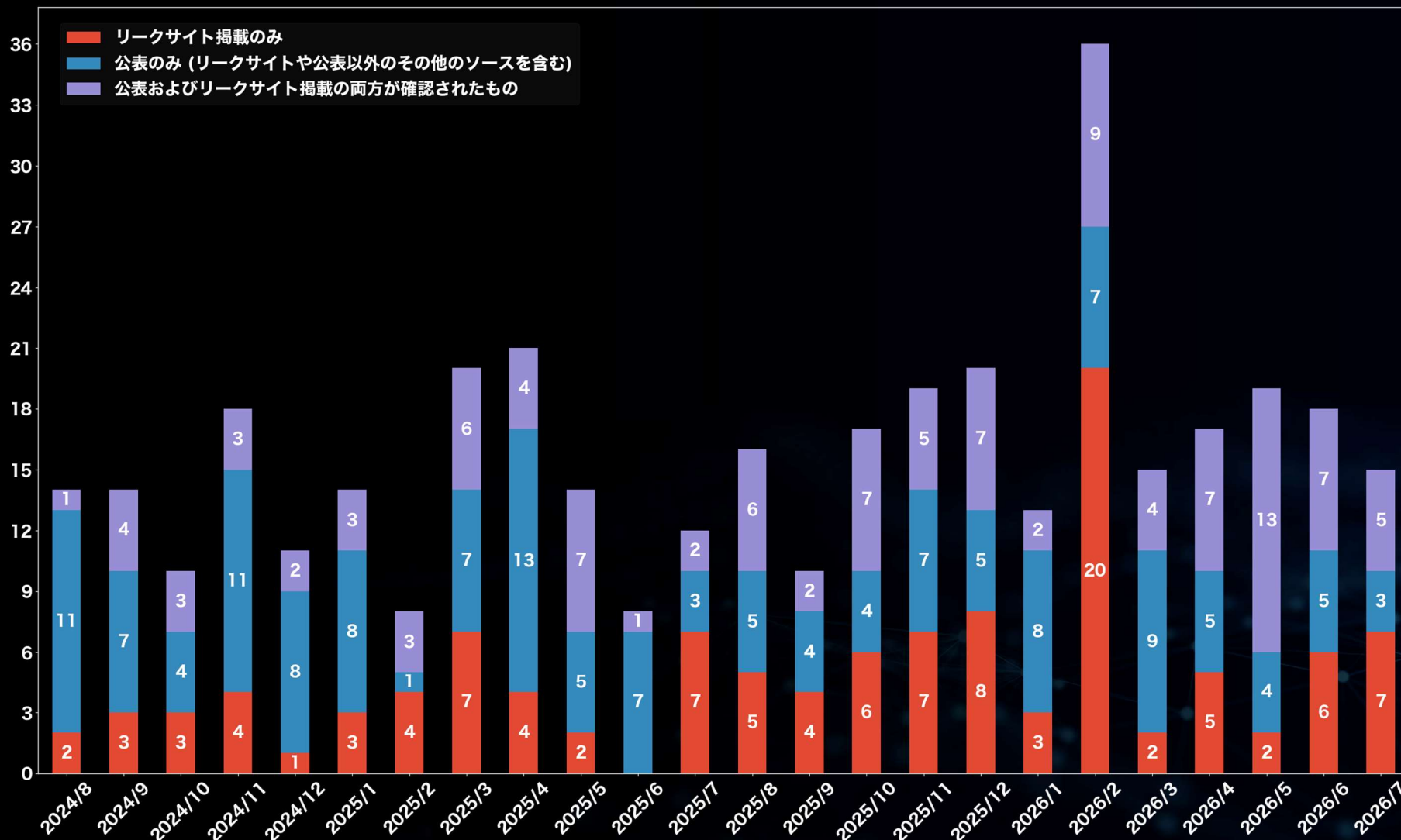
公表と暴露に関する統計

(国内)

公表割合 月別内訳 (国内)

(過去2年間／2024年8月～2026年7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)

公となった国内被害組織 概要一覧

2026

7

公となった国内被害組織概要一覧 (国内)

(過去1年間／2025年8月～2026年7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	(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\$ Hu...	大手自動車メーカー
2025/10	Scattered LAPSUS\$ Hu...	大手スポーツ用品メーカー
2025/10	Scattered LAPSUS\$ Hu...	大手総合化学メーカー
2025/10	Qilin (Agenda)	大手飲料・食品メーカー
2025/10	(Unknown)	大学法人
2025/10	Rhysida	産業機械メーカー
2025/10	WORLD LEAKS	化粧品メーカー
2025/10	(Unknown)	金融機器メーカー
2025/10	AKIRA	各種機械類・刃物メーカー(海外拠点)
2025/10	(Unknown)	私立学校

被害月	攻撃グループ	業種概要
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
2025/11	(Unknown)	国際総合検定機関
2025/12	(Unknown)	エレクトロニクス専門商社(海外拠点)
2025/12	(Unknown)	教育系ITサービス提供
2025/12	AKIRA	食用油脂メーカー(海外拠点)
2025/12	Payouts King	プラスチック精密工業部品メーカー(海外拠点)
2025/12	COINBASE CARTEL	大手半導体メーカー
2025/12	INC Ransom	ワイヤーハーネスメーカー
2025/12	Lynx	総合デベロッパー
2025/12	Qilin (Agenda)	空調・衛生設備工事(海外拠点)
2025/12	(Unknown)	総合色材・機能性化学メーカー(海外拠点)
2025/12	root	金融商品取引所

被害月	攻撃グループ	業種概要
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	タイマーメーカー(海外拠点)
2026/1	(Unknown)	飲料メーカー
2026/1	(Unknown)	スポーツ教室
2026/1	The Gentlemen	産業廃棄物処理
2026/1	Brain Cipher	システムインテグレーター
2026/2	Qilin (Agenda)	特殊金属材料・製造
2026/2	Everest	機械器具製造
2026/2	Everest	金属加工メーカー
2026/2	(Unknown)	大手化学素材メーカー(海外拠点)
2026/2	OAPT	大手電気機器メーカー
2026/2	OAPT	大手テクノロジー企業
2026/2	OAPT	自動制御機器製品メーカー
2026/2	(Unknown)	ペット関連用品製造
2026/2	OAPT	医療機器メーカー
2026/2	OAPT	医療機器メーカー
2026/2	(Unknown)	スキー場運営
2026/2	INC Ransom	国際貨物運送取扱業
2026/2	The Gentlemen	伝熱管メーカー

(※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8月～2026年7月)

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

被害月	攻撃グループ	業種概要
2026/2	OAPT	タイマーメーカー
2026/2	OAPT	総合電機メーカー
2026/2	OAPT	大手自動車メーカー
2026/2	OAPT	建設機械メーカー
2026/2	OAPT	総合電機メーカー
2026/2	(Unknown)	ソフトウェア開発
2026/2	Qilin (Agenda)	総合テレロッパー
2026/2	(Unknown)	ホテル業・飲食店業
2026/2	OAPT	鉄道会社
2026/2	OAPT	地方自治体
2026/2	OAPT	電力会社
2026/2	OAPT	地方自治体
2026/2	Qilin (Agenda)	種苗メーカー兼商社(海外拠点)
2026/2	NightSpire	繊維・衣料関連卸売業
2026/2	(Unknown)	半導体試験装置メーカー
2026/2	NetRunner	総合病院
2026/2	LockBit	機械・工具メーカー(海外拠点)
2026/2	BLACKSHRANTAC	紳士服・婦人服販売
2026/2	NightSpire	モータースポーツチーム運営
2026/2	(Unknown)	印刷会社
2026/2	INC Ransom	石油製品・LPガス販売
2026/2	The Gentlemen	材料加工装置メーカー
2026/2	Everest	商用車メーカー
2026/3	(Unknown)	市場調査・コンサルティング
2026/3	NetRunner	療養型病院
2026/3	(Unknown)	FAX通信・BPOサービス
2026/3	(Unknown)	工業用ゴム・樹脂・配管資材商社
2026/3	(Unknown)	住宅・商業施設向けリペア
2026/3	(Unknown)	美容クリニック
2026/3	(Unknown)	シティホテル運営
2026/3	The Gentlemen	医療・看護専門出版社
2026/3	Space Bears	介護・カラオケ・飲食事業
2026/3	(Unknown)	光半導体デバイスメーカー(海外拠点)
2026/3	WORLD LEAKS	広告・制作
2026/3	The Gentlemen	繊維加工・食品加工メーカー
2026/3	(Unknown)	設備工事

被害月	攻撃グループ	業種概要
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)	生活協同組合
2026/4	COINBASE CARTEL	大学研究会
2026/4	Ransom EXX	ソフトウェア開発
2026/4	LockBit	電子部品(コネクタ)製造(海外拠点)
2026/4	(Unknown)	二輪用品専門チェーン
2026/4	The Gentlemen	ソフトウェア開発
2026/4	Qilin (Agenda)	大手自動車部品メーカー(海外拠点)
2026/5	(Unknown)	百貨店業・不動産賃貸業
2026/5	(Unknown)	不動産コンサルティング・資産管理
2026/5	FulcrumSec	移植医療支援
2026/5	KILLSEC	オンライン地方選挙サービス
2026/5	(Unknown)	教育サービス・学習教材
2026/5	AiLock	半導体製造装置・精密機器メーカー(海外拠点)
2026/5	The Gentlemen	医薬品卸売業
2026/5	The Gentlemen	商業施設運営サービス
2026/5	SAFEPAY	産業資材商社
2026/5	AKIRA	家電メーカー(海外拠点)
2026/5	Lynx	水処理装置メーカー(海外拠点)
2026/5	Lynx	蓄電池・電源システム(海外拠点)
2026/5	The Gentlemen	ジュエリー輸入・企画販売
2026/5	Payload	空調設備施工
2026/5	The Gentlemen	ガラス容器メーカー
2026/5	NightSpire	医薬品・食品関連製造(海外拠点)
2026/5	(Unknown)	国立大学法人

被害月	攻撃グループ	業種概要
2026/5	SAFEPAY	紙幣製造
2026/5	SAFEPAY	建材リペア・再生工事
2026/6	SAFEPAY	楽器メーカー(海外拠点)
2026/6	(Unknown)	サポーター・健康用品製造販売
2026/6	(Unknown)	化粧品・健康食品製造販売、エステ運営
2026/6	STORMOUS	化学系専門商社(海外拠点)
2026/6	(Unknown)	米穀・飼料・食品卸売等
2026/6	(Unknown)	ローカルキャラクターの活動支援
2026/6	SAFEPAY	音楽系書籍販売
2026/6	(Unknown)	シェアモビリティ、駐車場運営
2026/6	Qilin (Agenda)	トラック・バス等の製造販売(海外拠点)
2026/6	CMD ORGANIZATION	ロボットシステムインテグレーター
2026/6	SHADOWBYT3\$	大手ゲーム機・ゲームソフトメーカー(海外拠点)
2026/6	AURORA	非鉄金属・自動車部品メーカー(海外拠点)
2026/6	SAFEPAY	建設コンサルタント
2026/6	LockBit	自動車部品・合成樹脂製品メーカー(海外拠点)
2026/6	BlackField	自動車部品メーカー(海外拠点)
2026/6	DragonForce	特殊弁メーカー
2026/6	Qilin (Agenda)	私立大学
2026/6	The Gentlemen	化粧品・健康食品製造販売
2026/7	(Unknown)	私立中学・高等学校
2026/7	(Unknown)	引越し・配送会社
2026/7	(Unknown)	穀物乾燥機メーカー
2026/7	AiLock	大手タクシー会社
2026/7	AiLock	業務用ソフトウェア開発会社
2026/7	COINBASE CARTEL	航空機向け電子機器メーカー(海外拠点)
2026/7	CHAOS (2025)	大手酒類・食品持株会社(海外拠点)
2026/7	The Gentlemen	排水処理設備メーカー
2026/7	The Gentlemen	ソフトウェア開発会社
2026/7	INC Ransom	特装車メーカー
2026/7	INC Ransom	大手酒類・食品持株会社(海外拠点)
2026/7	RansomHouse	大手冷凍食品メーカー
2026/7	Morpheus	めっき・樹脂成形メーカー(海外拠点)
2026/7	GLOBAL SECRET GROUP	オンラインゲーム会社
2026/7	Everest	ITサービス会社

(※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)

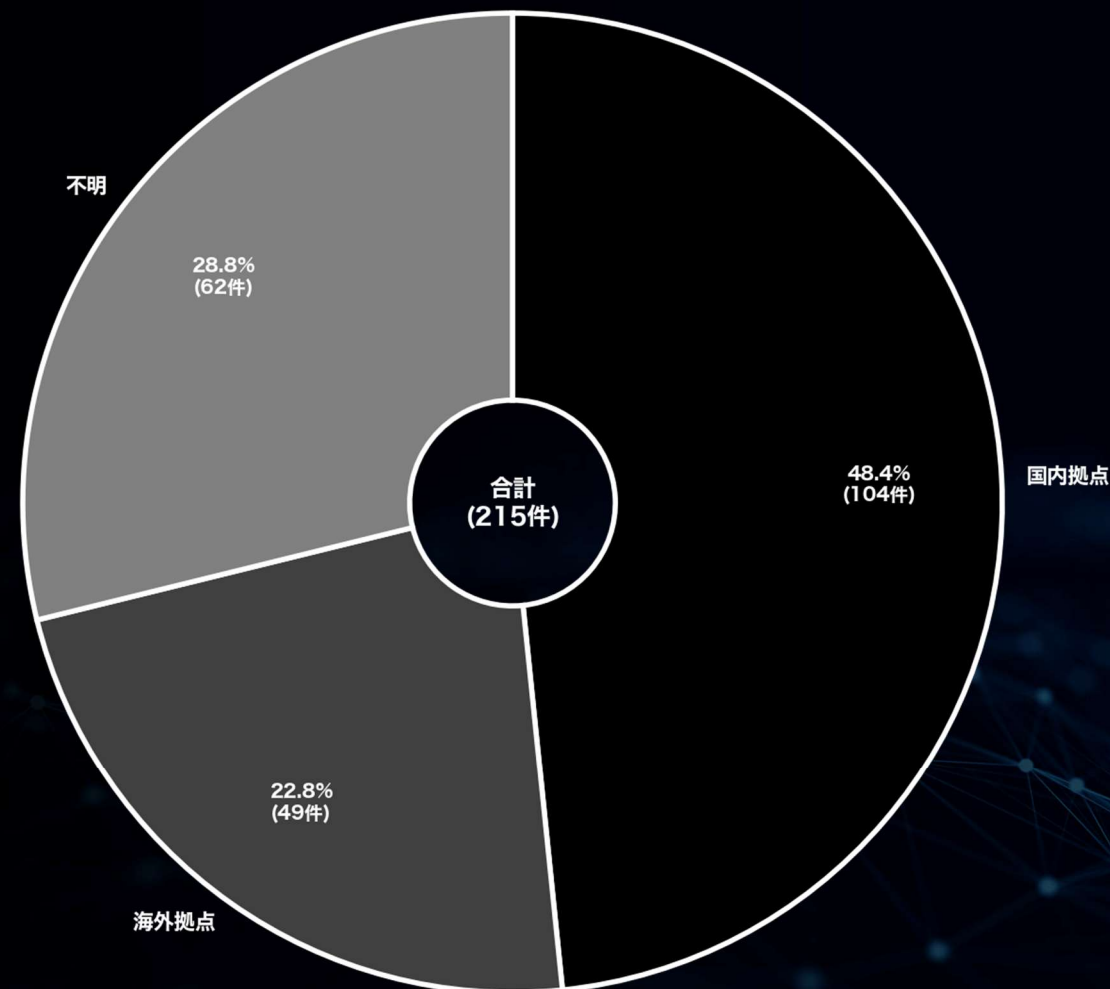
(過去1年間／2025年8月～2026年7月)

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

▼ランサムウェア攻撃を受けた日本関連組織の拠点別割合

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

拠点	件数	割合(%)
国内拠点	104	48.4
海外拠点	49	22.8
不明	62	28.8



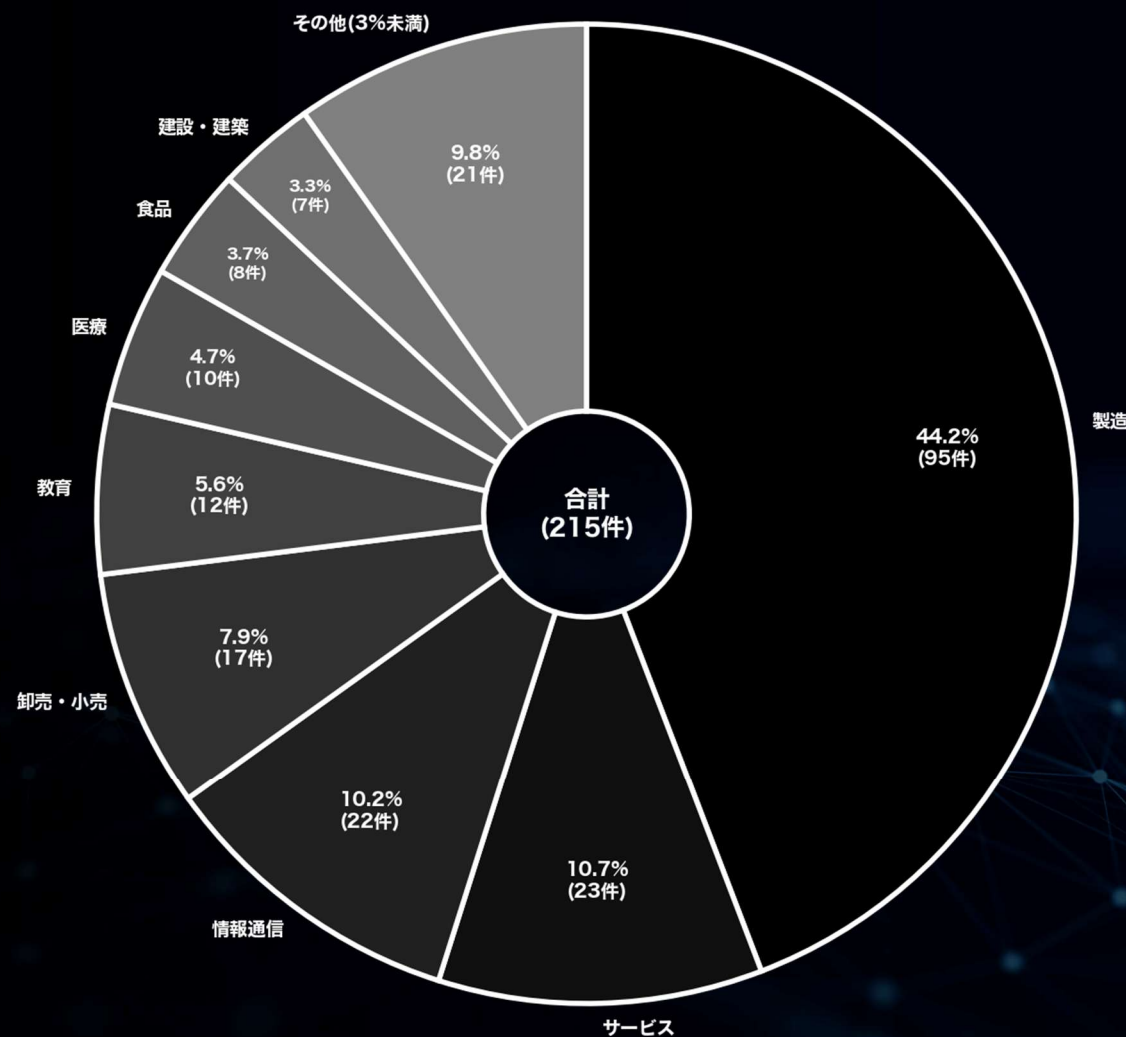
(※本ページの表／グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

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8月～2026年7月)

業種	件数	割合(%)
製造	95	44.2
サービス	23	10.7
情報通信	22	10.2
卸売・小売	17	7.9
教育	12	5.6
医療	10	4.7
食品	8	3.7
建設・建築	7	3.3
その他(3%未満)	21	9.8

▼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)

2026

7

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8月～2026年7月）

赤色は中小企業を示す

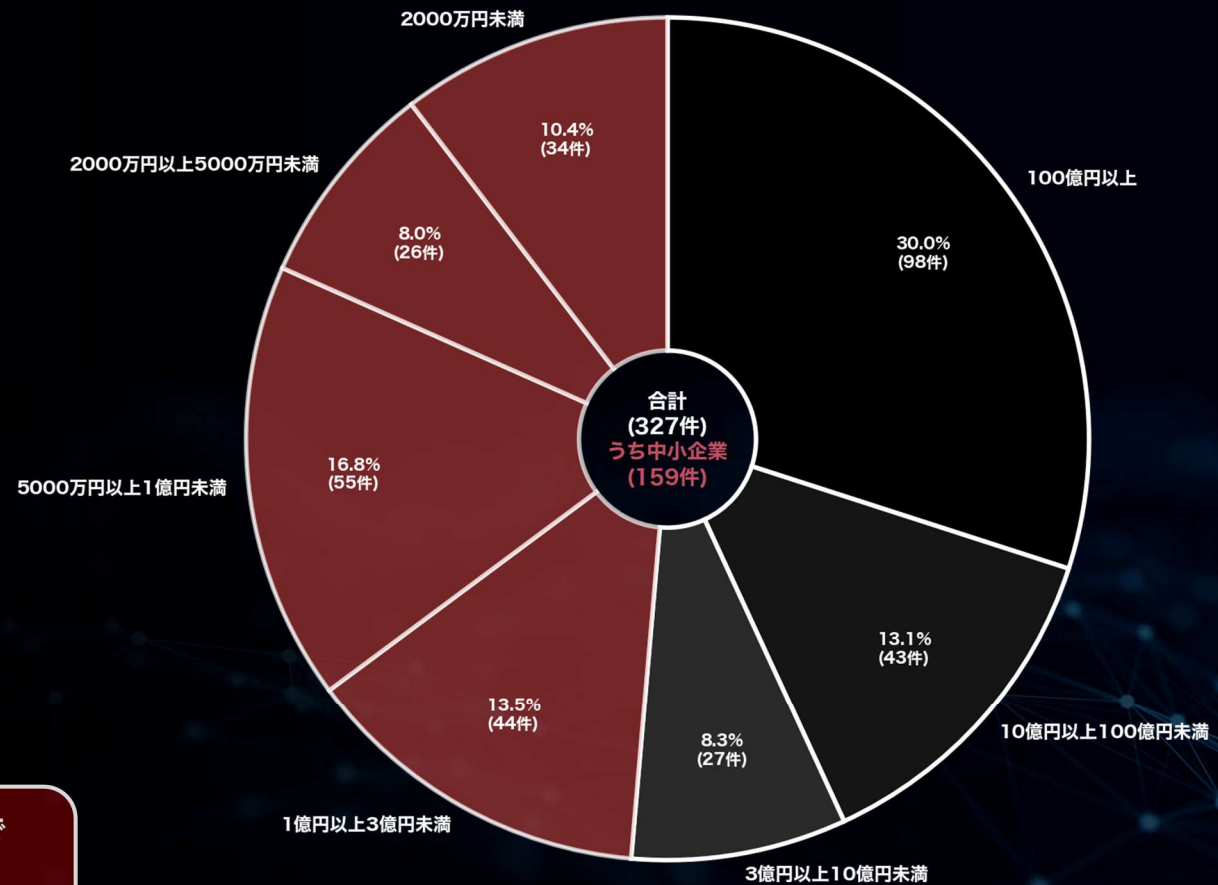
※資本金順に降順 / 資本金情報を公表していない一部の被害組織は除外

資本金	件数	割合(%)
100億円以上	98	30.0
10億円以上100億円未満	43	13.1
3億円以上10億円未満	27	8.3
1億円以上3億円未満	44	13.5
5000万円以上1億円未満	55	16.8
2000万円以上5000万円未満	26	8.0
2000万円未満	34	10.4

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159件にのぼり、全体の48.6%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。

▼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）



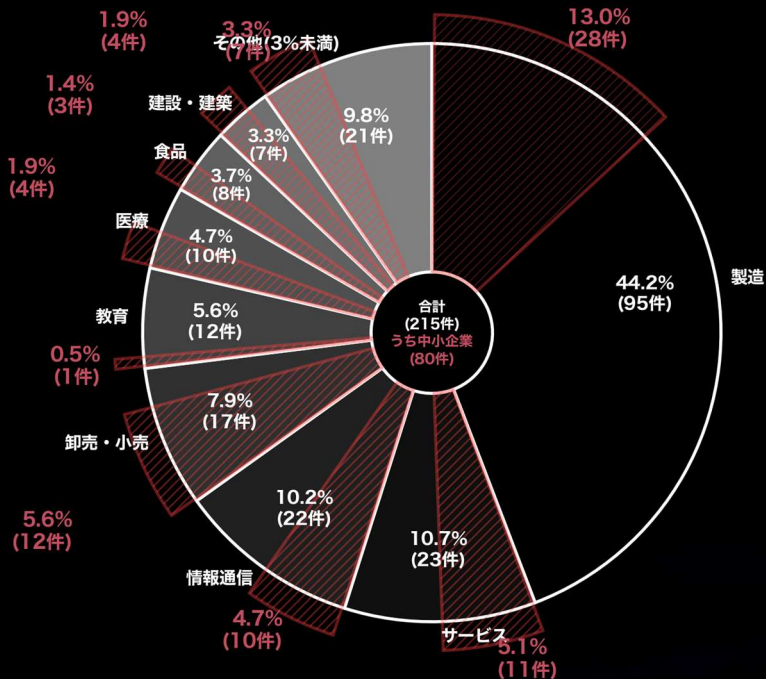
（※本ページの表／グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している）

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8月~2026年7月)

赤色は中小企業を示す

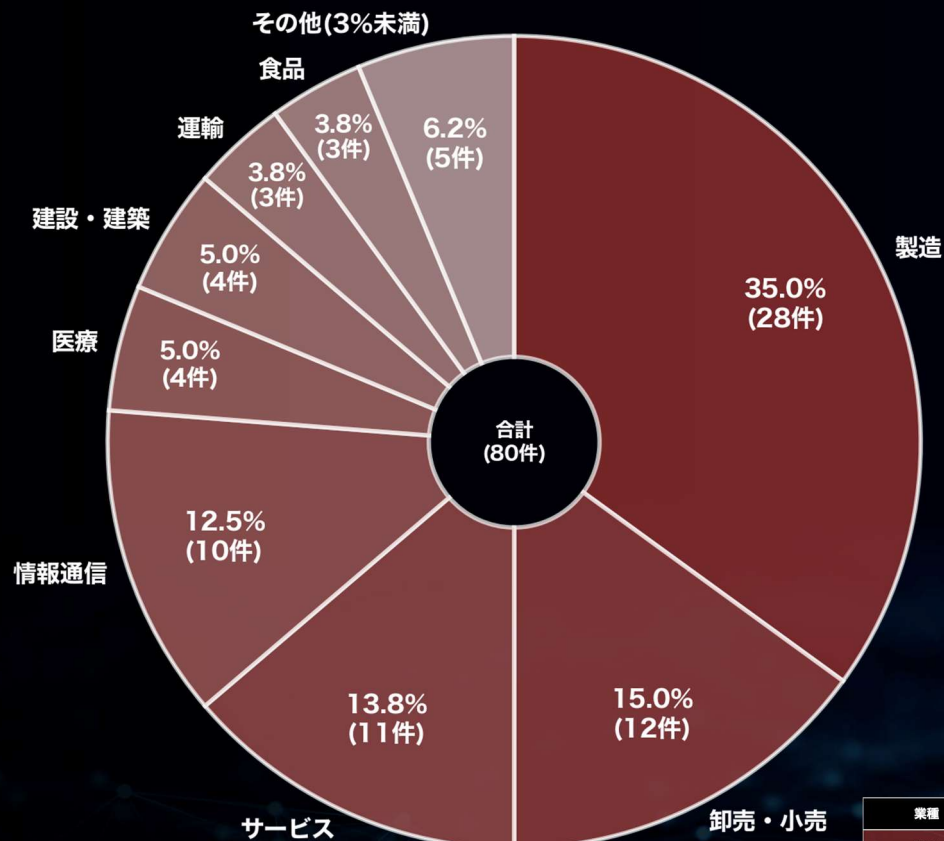
▼全体割合



※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	95 (28)	44.2 (13.0)
サービス	23 (11)	10.7 (5.1)
情報通信	22 (10)	10.2 (4.7)
卸売・小売	17 (12)	7.9 (5.6)
教育	12 (1)	5.6 (0.5)
医療	10 (4)	4.7 (1.9)
食品	8 (3)	3.7 (1.4)
建設・建築	7 (4)	3.3 (1.9)
その他(3%未満)	21 (7)	9.8 (3.3)

▼中小企業のための割合



業種	件数	割合(%)
製造	28	35.0
卸売・小売	12	15.0
サービス	11	13.8
情報通信	10	12.5
医療	4	5.0
建設・建築	4	5.0
運輸	3	3.8
食品	3	3.8
その他(3%未満)	5	6.2

過去1年間の業種別分析においては、中小企業のみ限定すると、被害件数の割合は業種を問わず、より全体に分散していることがわかる。

※医療や教育、行政機関など資本金が不明な一部の組織については集計から除外

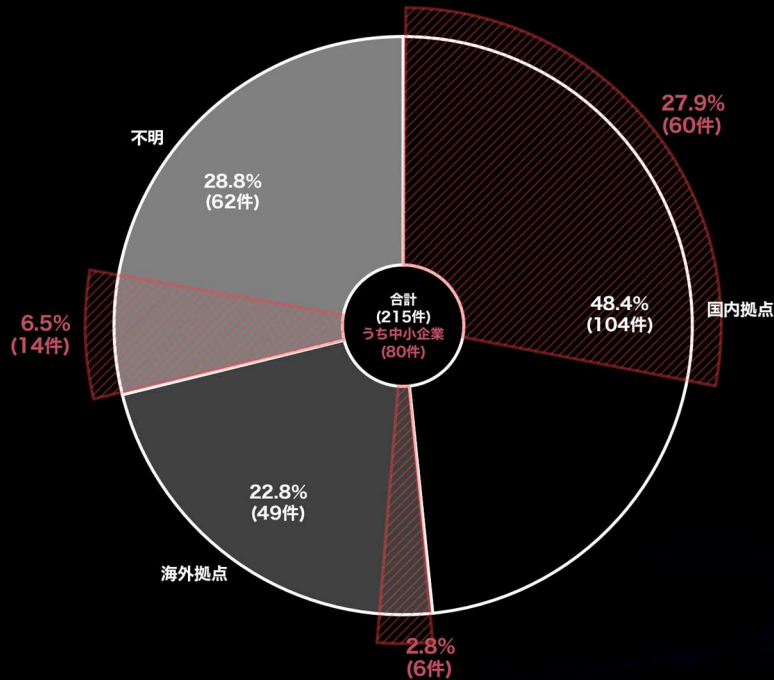
(※本ページの表/グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

公となった国内被害組織における拠点割合 (国内-中小企業)

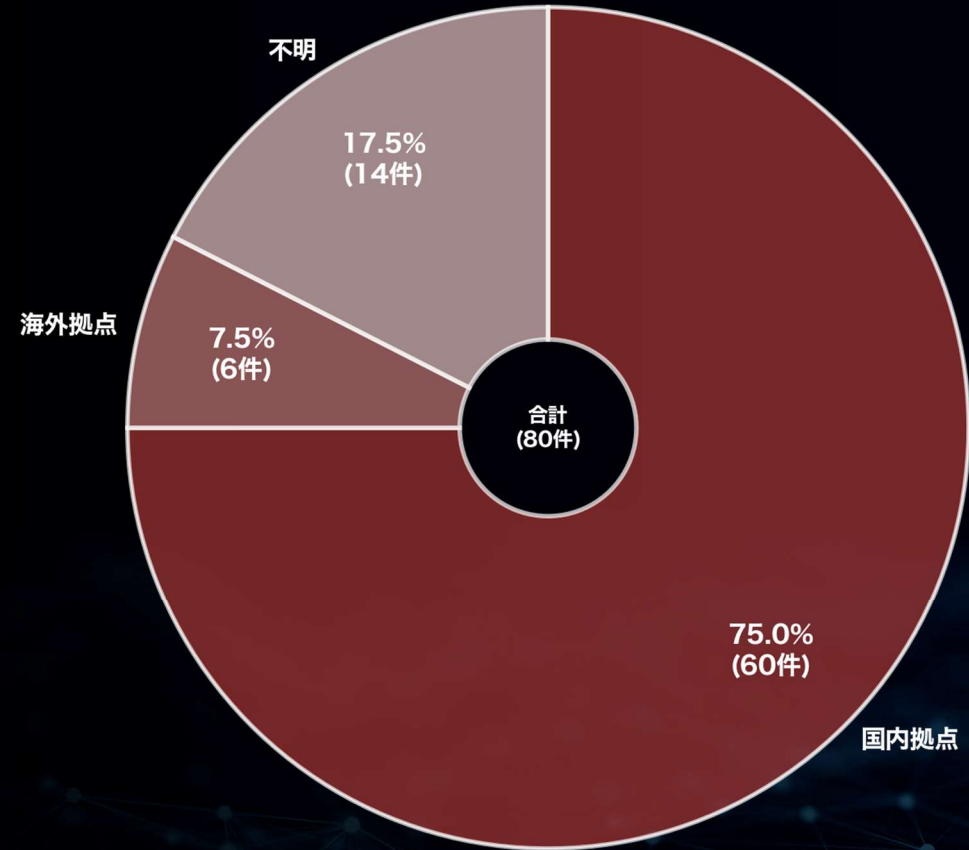
(過去1年間/2025年8月~2026年7月)

赤色は中小企業を示す

▼全体割合



▼中小企業のための割合



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

拠点	件数 (中小企業)	割合 (%)
国内拠点	104 (60)	48.4 (27.9)
海外拠点	49 (6)	22.8 (2.8)
不明	62 (14)	28.8 (6.5)
合計	215 (80)	100 (37.2)

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	60	75.0
海外拠点	6	7.5
不明	14	17.5

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

公となった国内被害組織概要一覧 (国内-中小企業)

(過去1年間／2025年8月～2026年7月)

赤色は中小企業を示す

被害月	攻撃グループ	業種概要
2025/8	(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\$ Hu...	大手自動車メーカー
2025/10	Scattered LAPSUS\$ Hu...	大手スポーツ用品メーカー
2025/10	Scattered LAPSUS\$ Hu...	大手総合化学メーカー
2025/10	Qilin (Agenda)	大手飲料・食品メーカー
2025/10	(Unknown)	大学法人
2025/10	Rhysida	産業機械メーカー
2025/10	WORLD LEAKS	化粧品メーカー
2025/10	(Unknown)	金融機器メーカー
2025/10	AKIRA	各種機械組・刃物メーカー(海外拠点)
2025/10	(Unknown)	私立学校

被害月	攻撃グループ	業種概要
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	情報装置メーカー
2025/11	Qilin (Agenda)	大手建設会社(海外拠点)
2025/11	(Unknown)	精密部品製造
2025/11	(Unknown)	国際総合検定機関
2025/12	(Unknown)	エレクトロニクス専門商社(海外拠点)
2025/12	(Unknown)	教育系ITサービス提供
2025/12	AKIRA	食用油脂メーカー(海外拠点)
2025/12	Payouts King	プラスチック精密工業部品メーカー(海外拠点)
2025/12	COINBASE CARTEL	大手半導体メーカー
2025/12	INC Ransom	ワイヤーハーネスメーカー
2025/12	Lynx	総合デベロッパー
2025/12	Qilin (Agenda)	空調・衛生設備工事(海外拠点)
2025/12	(Unknown)	総合色材・機能性化学メーカー(海外拠点)
2025/12	root	金融商品取引所

被害月	攻撃グループ	業種概要
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)
2026/2	OAPT	大手電気機器メーカー
2026/2	OAPT	大手テクノロジー企業
2026/2	OAPT	自動制御機器製品メーカー
2026/2	(Unknown)	ペット関連用品製造
2026/2	OAPT	医療機器メーカー
2026/2	OAPT	医療機器メーカー
2026/2	(Unknown)	スキー場運営
2026/2	INC Ransom	国際貨物運送取扱業
2026/2	The Gentlemen	伝熱管メーカー

※ (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

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

暴露型ランサムウェア攻撃統計CIGマンスリーレポート2026年8月号 Rev 1.00

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8月～2026年7月)

赤色は中小企業を示す

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

被害月	攻撃グループ	業種概要
2026/2	OAPT	タイヤメーカー
2026/2	OAPT	総合電機メーカー
2026/2	OAPT	大手自動車メーカー
2026/2	OAPT	建設機械メーカー
2026/2	OAPT	総合電機メーカー
2026/2	(Unknown)	ソフトウェア開発
2026/2	Qilin (Agenda)	総合デベロッパー
2026/2	(Unknown)	ホテル業・飲食店業
2026/2	OAPT	鉄道会社
2026/2	OAPT	地方自治体
2026/2	OAPT	電力会社
2026/2	OAPT	地方自治体
2026/2	Qilin (Agenda)	種苗メーカー兼商社(海外拠点)
2026/2	NightSpire	繊維・衣料関連卸売業
2026/2	(Unknown)	半導体試験装置メーカー
2026/2	NetRunner	総合病院
2026/2	LockBit	機械・工具メーカー(海外拠点)
2026/2	BLACKSHRANTAC	紳士服・婦人服販売
2026/2	NightSpire	モータースポーツチーム運営
2026/2	(Unknown)	印刷会社
2026/2	INC Ransom	石油製品・LPガス販売
2026/2	The Gentlemen	材料加工装置メーカー
2026/2	Everest	商用車メーカー
2026/3	(Unknown)	市場調査・コンサルティング
2026/3	NetRunner	療養型病院
2026/3	(Unknown)	FAX通信・BPOサービス
2026/3	(Unknown)	工業用ゴム・樹脂・配管資材商社
2026/3	(Unknown)	住宅・商業施設向けリペア
2026/3	(Unknown)	美容クリニック
2026/3	(Unknown)	シティホテル運営
2026/3	The Gentlemen	医療・看護専門出版社
2026/3	Space Bears	介護・カラオケ・飲食事業
2026/3	(Unknown)	光半導体デバイスメーカー(海外拠点)
2026/3	WORLD LEAKS	広告・制作
2026/3	The Gentlemen	繊維加工・食品加工メーカー
2026/3	(Unknown)	設備工事

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

被害月	攻撃グループ	業種概要
2026/5	SAFEPAY	紙器製造
2026/5	SAFEPAY	建材リペア・再生工事
2026/6	SAFEPAY	楽器メーカー(海外拠点)
2026/6	(Unknown)	サポーター・健康用品製造販売
2026/6	(Unknown)	化粧品・健康食品製造販売・エステ運営
2026/6	STORMOUS	化学系専門商社(海外拠点)
2026/6	(Unknown)	米穀・飼料・食品卸売等
2026/6	(Unknown)	ローカルキャラクターの活動支援
2026/6	SAFEPAY	音楽系書籍販売
2026/6	(Unknown)	シェアモビリティ、駐車場運営
2026/6	Qilin (Agenda)	トラック・バス等の製造販売(海外拠点)
2026/6	CMD ORGANIZATION	ロボットシステムインテグレーター
2026/6	SHADOWBYT3\$	大手ゲーム機・ゲームソフトメーカー(海外拠点)
2026/6	AURORA	非鉄金属・自動車部品メーカー(海外拠点)
2026/6	SAFEPAY	建設コンサルタント
2026/6	LockBit	自動車部品・合成樹脂製品メーカー(海外拠点)
2026/6	BlackField	自動車部品メーカー(海外拠点)
2026/6	DragonForce	特殊井メーカー
2026/6	Qilin (Agenda)	私立大学
2026/6	The Gentlemen	化粧品・健康食品製造販売
2026/7	(Unknown)	私立中学・高等学校
2026/7	(Unknown)	引越し・配送会社
2026/7	(Unknown)	穀物乾燥機メーカー
2026/7	AI Lock	大手タクシー会社
2026/7	AI Lock	業務用ソフトウェア開発会社
2026/7	COINBASE CARTEL	航空機向け電子機器メーカー(海外拠点)
2026/7	CHAOS (2025)	大手酒類・食品持株会社(海外拠点)
2026/7	The Gentlemen	排水処理設備メーカー
2026/7	The Gentlemen	ソフトウェア開発会社
2026/7	INC Ransom	特装車メーカー
2026/7	INC Ransom	大手酒類・食品持株会社(海外拠点)
2026/7	RansomHouse	大手冷凍食品メーカー
2026/7	Morpheus	めっき・樹脂成形メーカー(海外拠点)
2026/7	GLOBAL SECRET GROUP	オンラインゲーム会社
2026/7	Everest	ITサービス会社

※ (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

2026

7

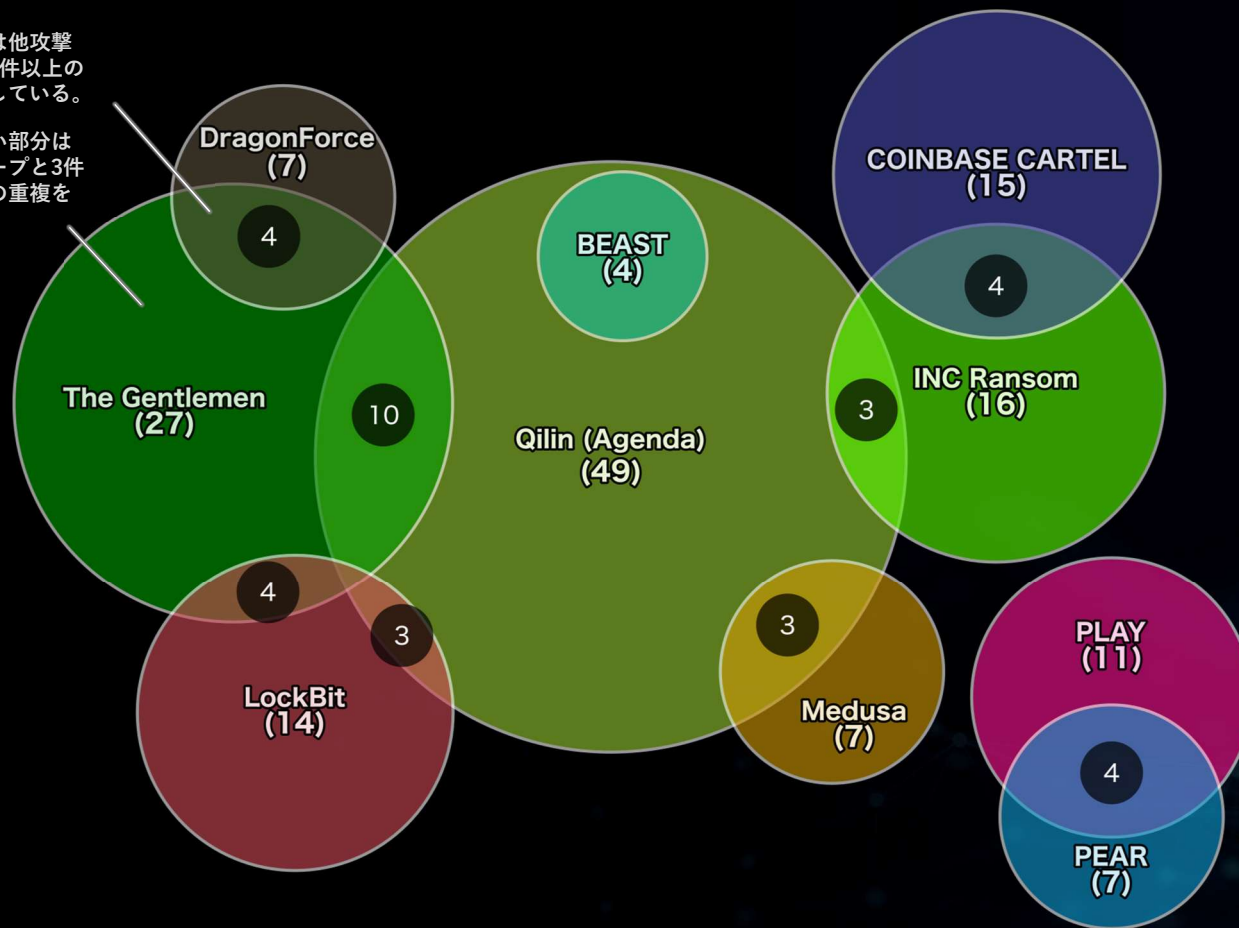
多重被害に関する分析

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8月～2026年7月) (累計148件) ※多重被害に遭った組織数の累計

※ 円の重なりは他攻撃グループと3件以上の重なりを表している。

※ 重なりのない部分は他攻撃グループと3件未満の事案の重複を表している。



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

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

例えば

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

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

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

※異なる攻撃グループによるリークサイトへの掲載件数を元に算出

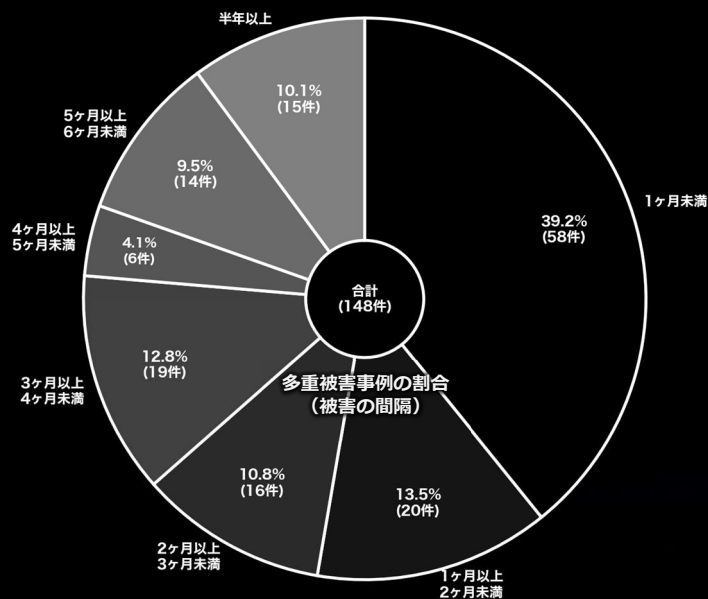
多重被害に遭った被害組織の傾向と分析 (全世界)

(過去1年間／2025年8月～2026年7月)

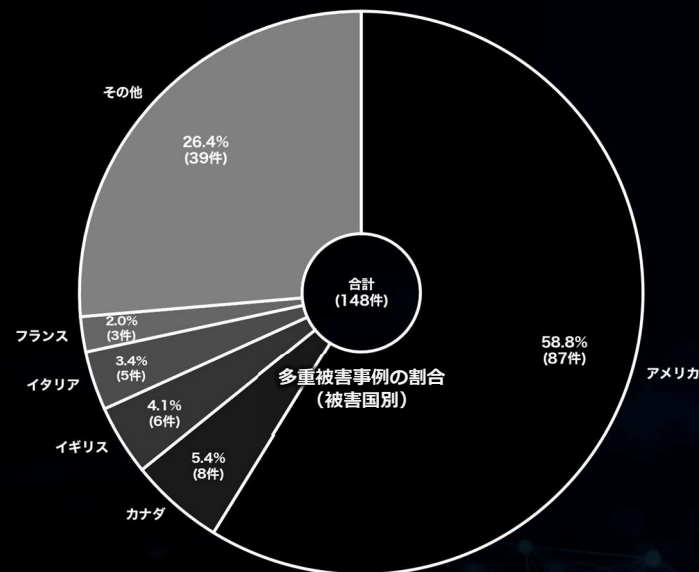
※多重被害：一度ランサムウェア攻撃の被害を受けた組織が異なる時期に異なる攻撃グループのリークサイトに再び掲載されるケース

▼被害の間隔

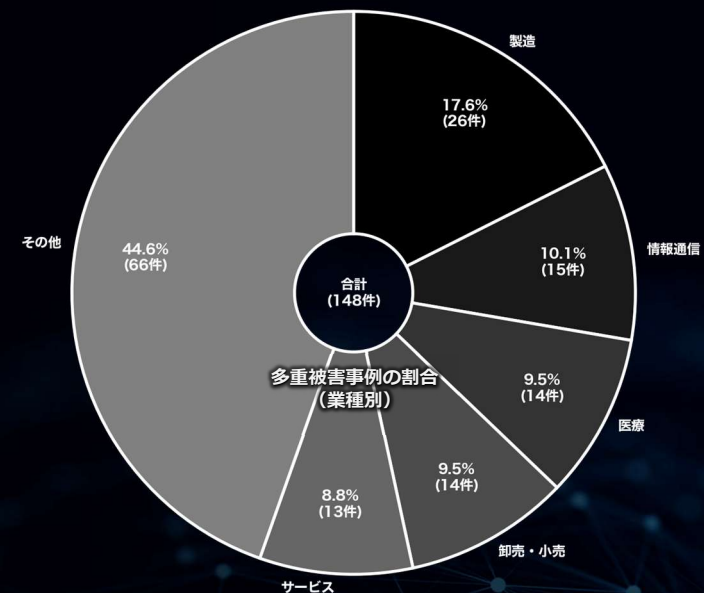
(一度目の被害から二度目の被害までの間隔)



▼被害国別



▼業種別



▶多重被害に遭った組織数の累計：148件 (全体9685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、実に半数以上が一度目の掲載から2ヶ月以内に再び発生していることが判明した。これら多重被害の事例には日本関連の組織も含まれており、一度侵入されデータ窃取されれば、いかなる組織でも多重被害に遭う可能性がある事を示す。

こうした被害を防ぐためには、日頃からの対策に加え万が一ランサムウェアの被害に遭っても身代金を支払わない（脅せば支払う組織であると認知されてしまう）ことや、繰り返しの侵入を防ぐために侵入経路の徹底的な洗い出し等の事後対応・再発防止策の実施が不可欠である。

業種に関する分析

(過去2年間のリークサイト掲載上位10業種)

2026

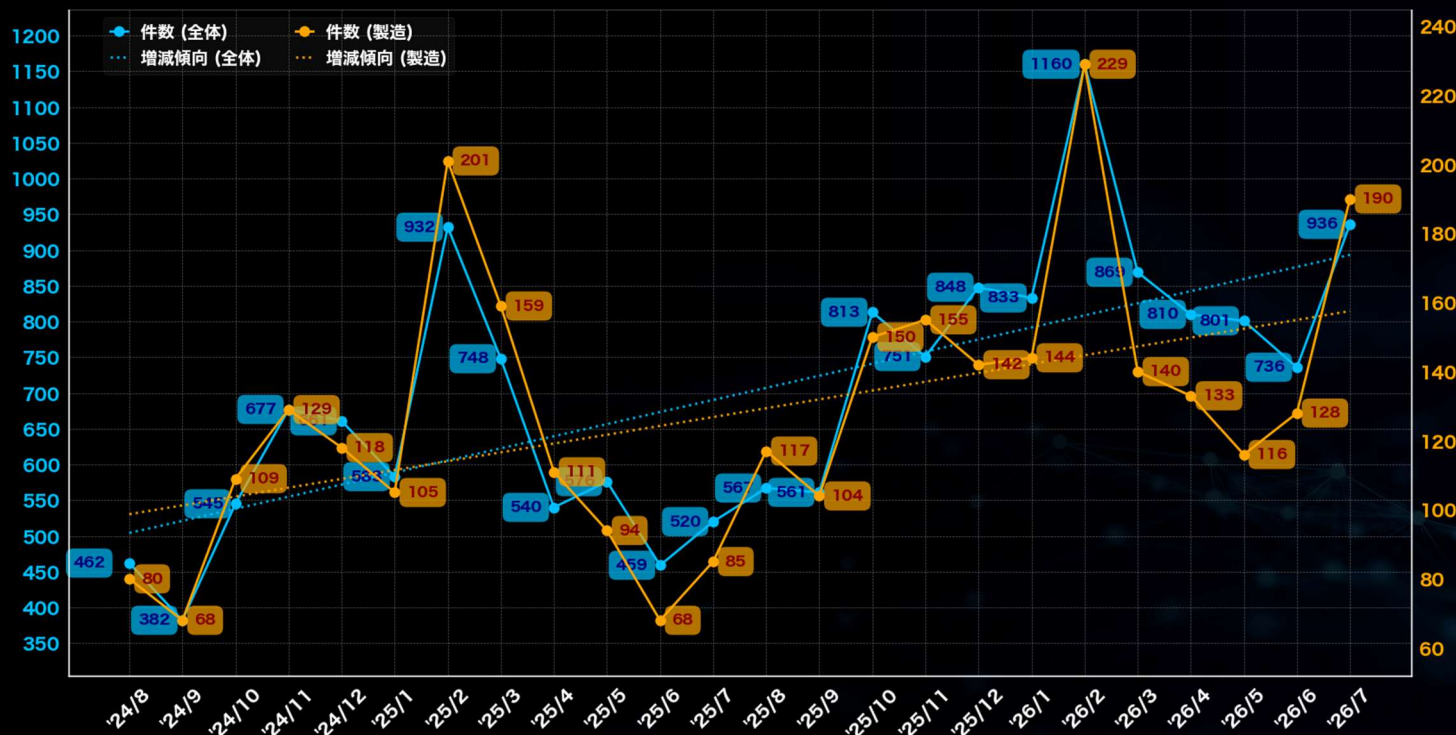
7

業種に関する分析 (全世界)

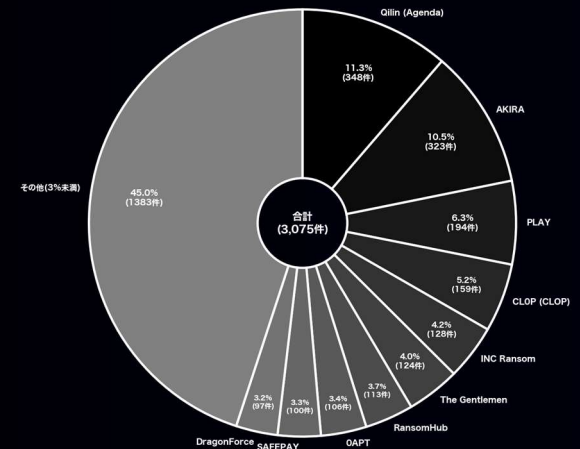
(過去2年間／2024年8月～2026年7月)

製造

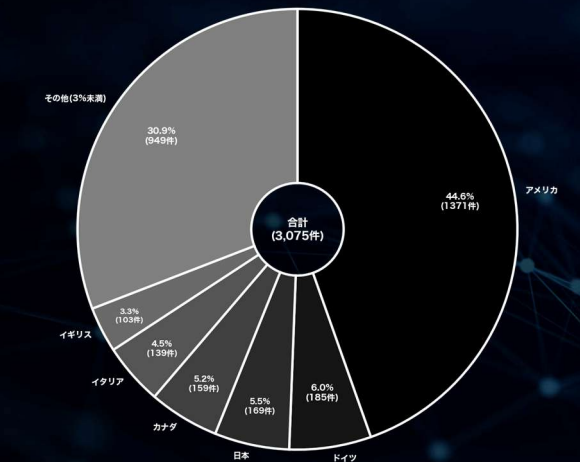
「製造」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年2月で、229件の掲載があった。一方、最も少なかった月は2024年9月と2025年6月で、いずれも68件であった。被害組織の所在国の割合では、アメリカが約45%と最も多く、次いでドイツと日本がそれぞれ約6%である。攻撃グループについては、少なくとも156のグループが関与しており、特に「Qilin (Agenda)」が348件のリークサイト掲載を実施している。次いで「AKIRA」と「PLAY」がそれぞれ323件と194件の掲載を行っている。製造関連の件数は全体件数に対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



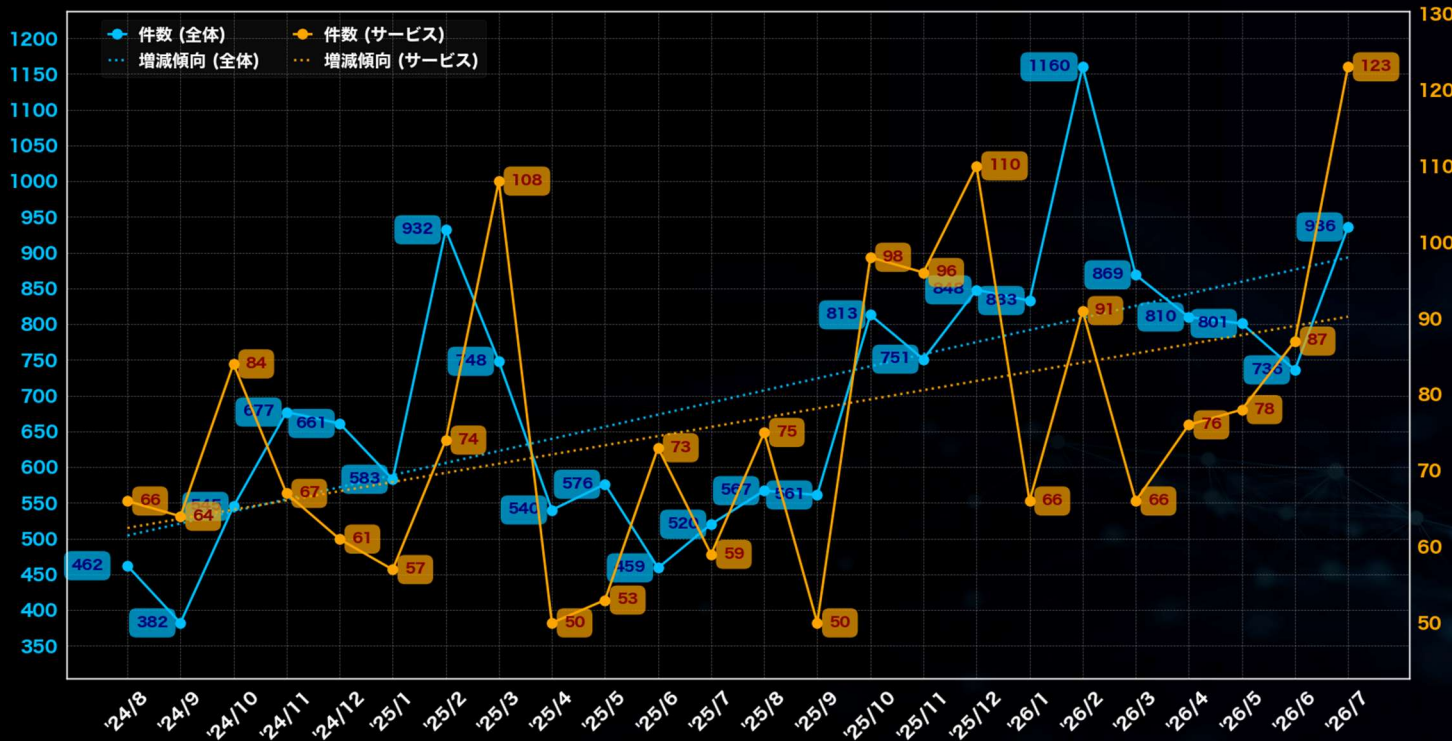
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

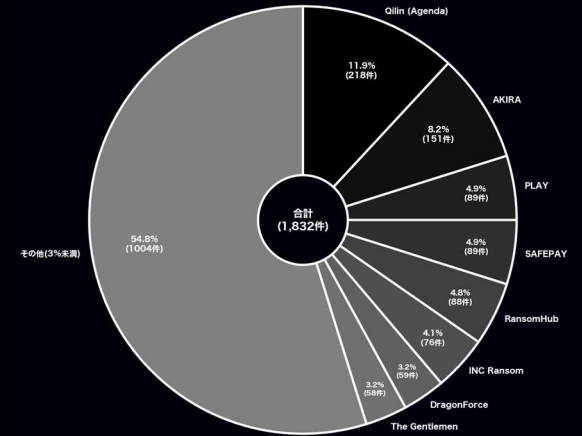
(過去2年間／2024年8月～2026年7月)

サービス

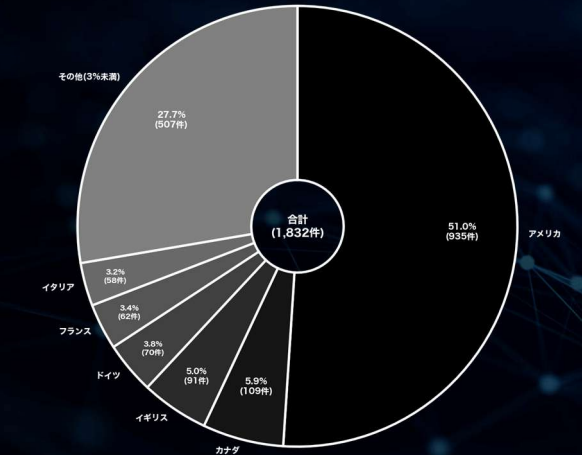
「サービス」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年7月で、123件の掲載があった。一方、最も少なかった月は2025年4月および2025年9月で、50件であった。被害組織の所在国の割合では、アメリカが約51%と最も多く、次いでカナダとイギリスがそれぞれ約6%と約5%である。攻撃グループについては、少なくとも145のグループが関与しており、特に「Qilin (Agenda)」が218件のリークサイト掲載を実施している。次いで「AKIRA」と「PLAY」がそれぞれ151件と89件の掲載を行っている。サービス関連の件数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



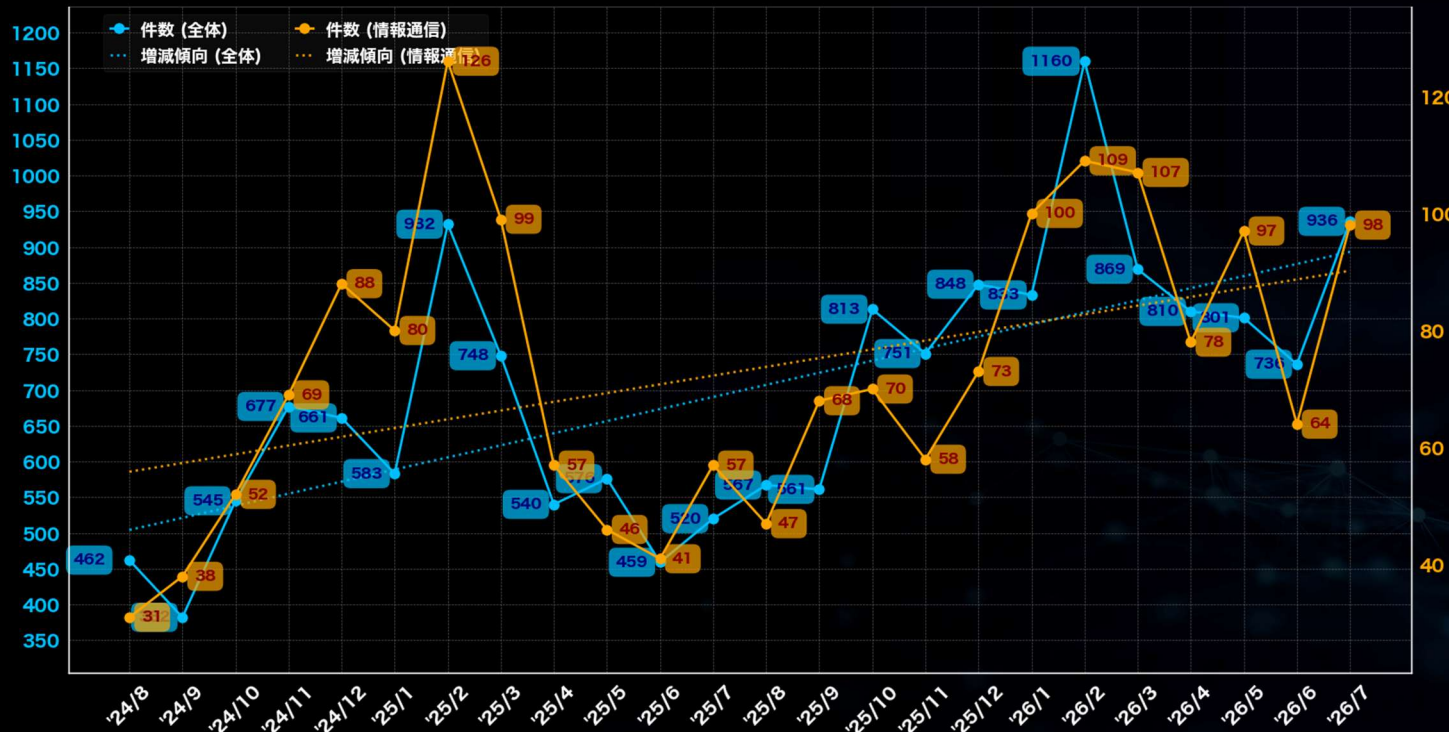
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

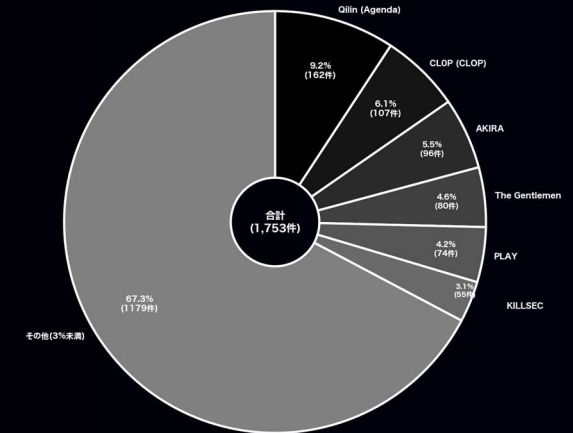
(過去2年間／2024年8月～2026年7月)

情報通信

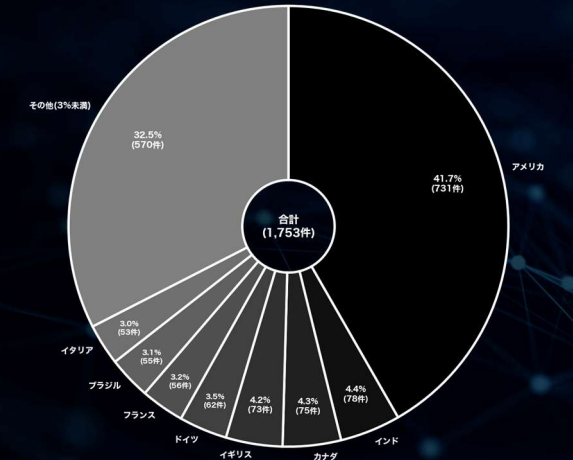
「情報通信」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、126件の掲載があった。一方、最も少なかった月は2024年8月で、31件であった。被害組織の所在国の割合では、アメリカが約42%と最も多く、次いでインドとカナダがそれぞれ約4%である。攻撃グループについては、少なくとも157のグループが関与しており、特に「Qilin (Agenda)」が162件のリークサイト掲載を実施している。次いで「CLOP (CLOP)」と「AKIRA」がそれぞれ107件と96件の掲載を行っている。情報通信業界は技術情報や顧客データ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



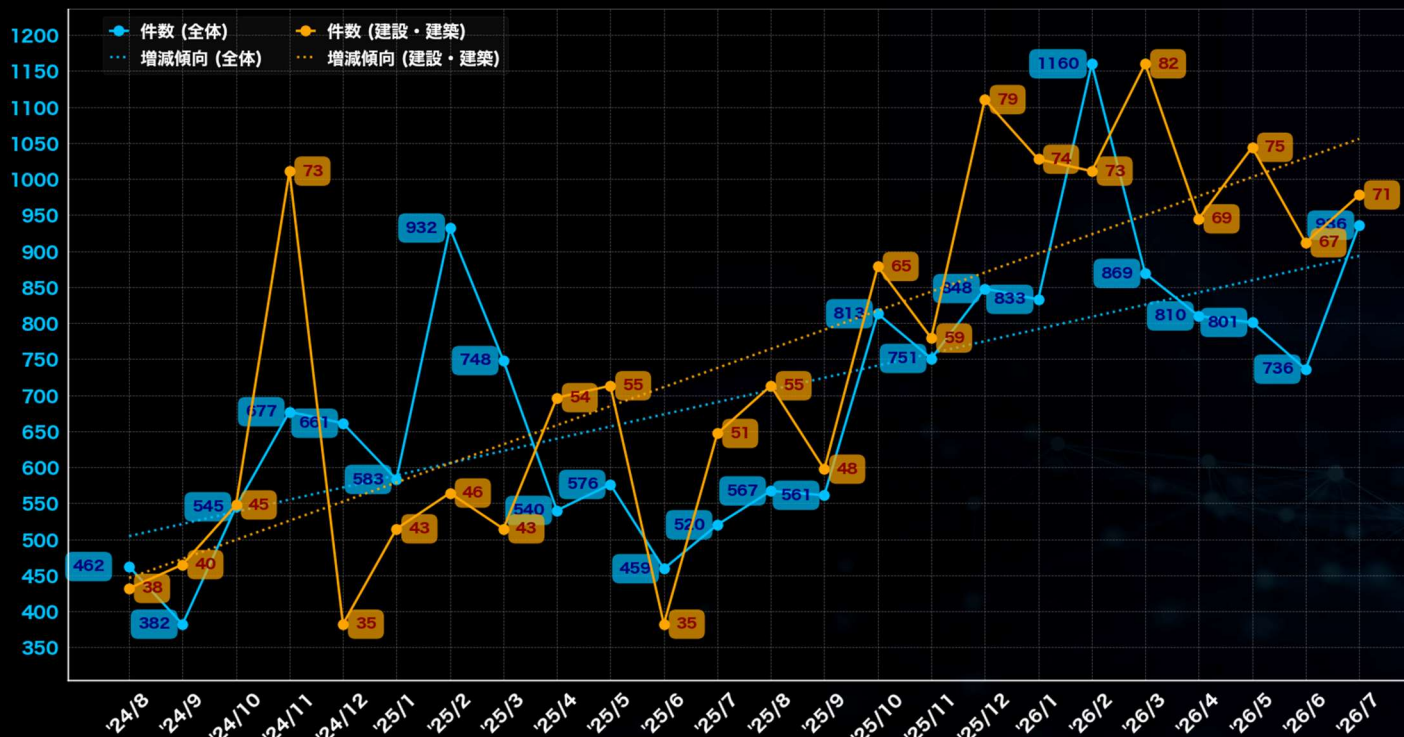
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

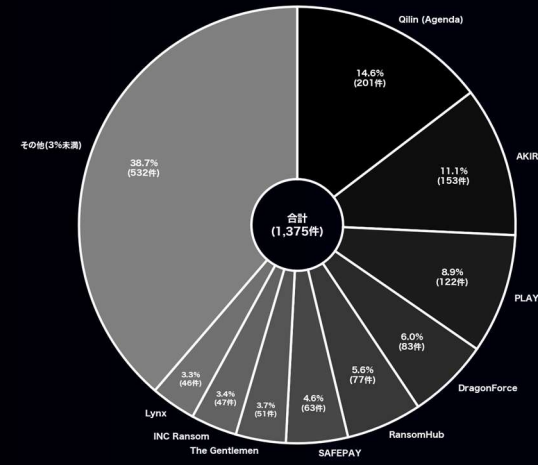
(過去2年間／2024年8月～2026年7月)

建設・建築

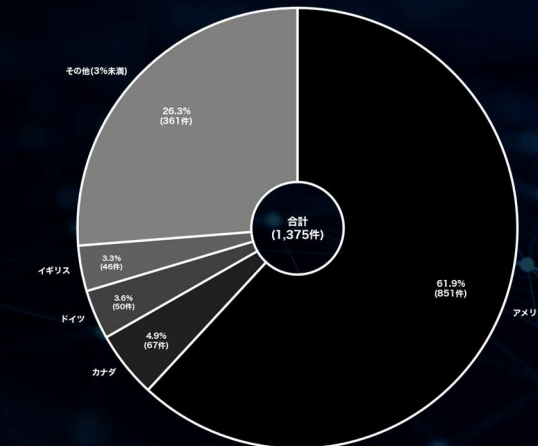
「建設・建築」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年3月で、82件の掲載があった。一方、最も少なかった月は2024年12月と2025年6月で、いずれも35件であった。被害組織の所在国の割合では、アメリカが約62%と最も多く、次いでカナダとドイツがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも114のグループが関与しており、特に「Qilin (Agenda)」が201件のリークサイト掲載を実施している。次いで「AKIRA」と「PLAY」がそれぞれ153件と122件の掲載を行っている。建設・建築業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



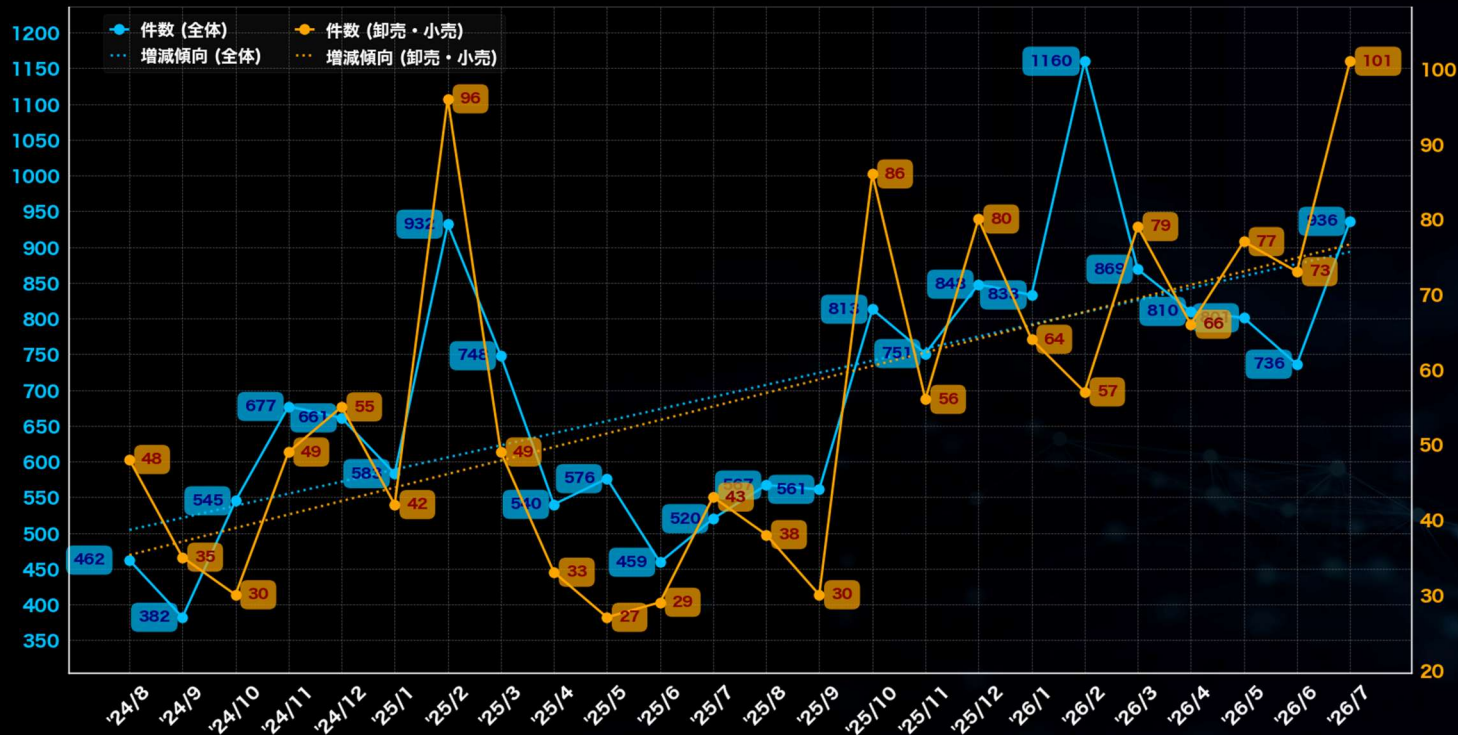
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

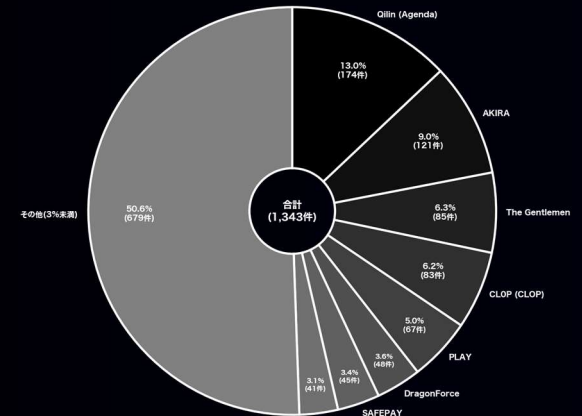
(過去2年間／2024年8月～2026年7月)

卸売・小売

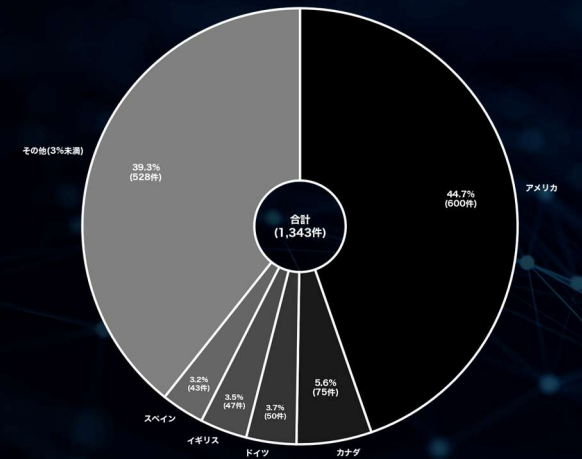
「卸売・小売」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年7月で、101件の掲載があった。一方、最も少なかった月は2025年5月で、27件であった。被害組織の所在国の割合では、アメリカが約45%と最も多く、次いでカナダとドイツがそれぞれ約6%と約4%である。攻撃グループについては、少なくとも123のグループが関与しており、特に「Qilin (Agenda)」が174件のリークサイト掲載を実施している。次いで「AKIRA」と「The Gentlemen」がそれぞれ121件と85件の掲載を行っている。卸売・小売業界は最大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



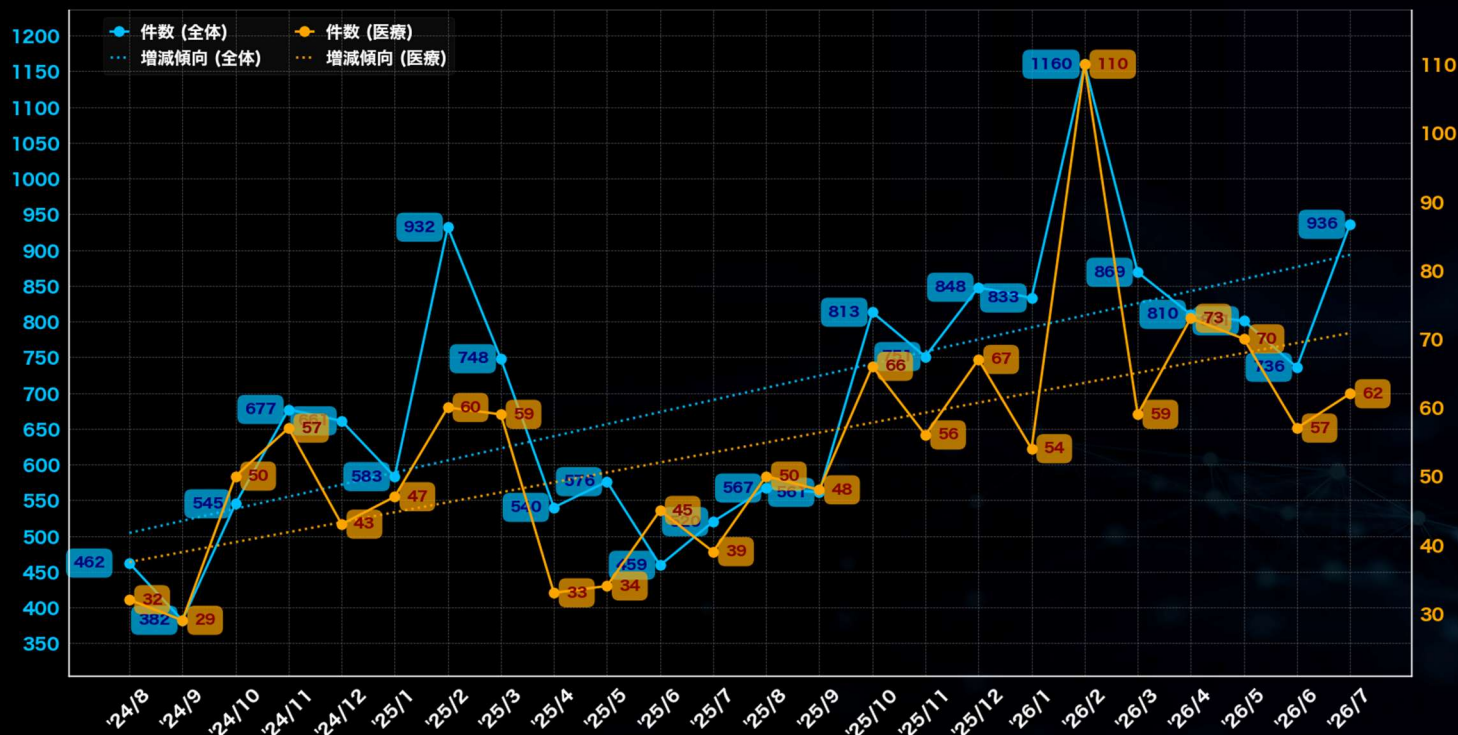
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

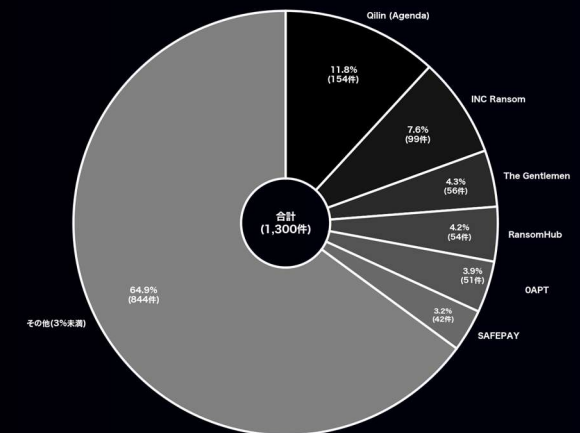
(過去2年間／2024年8月～2026年7月)

医療

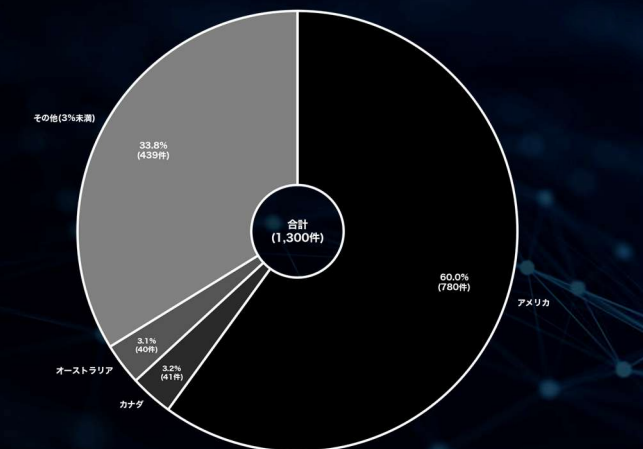
「医療」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年2月で、110件の掲載があった。一方、最も少なかった月は2024年9月で、29件であった。被害組織の所在国の割合では、アメリカが約60%と最も多く、次いでカナダとオーストラリアがそれぞれ約3%である。攻撃グループについては、少なくとも131のグループが関与しており、特に「Qilin (Agenda)」が154件のリークサイト掲載を実施している。次いで「INC Ransom」と「The Gentlemen」がそれぞれ99件と56件の掲載を行っている。医療業界は患者情報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



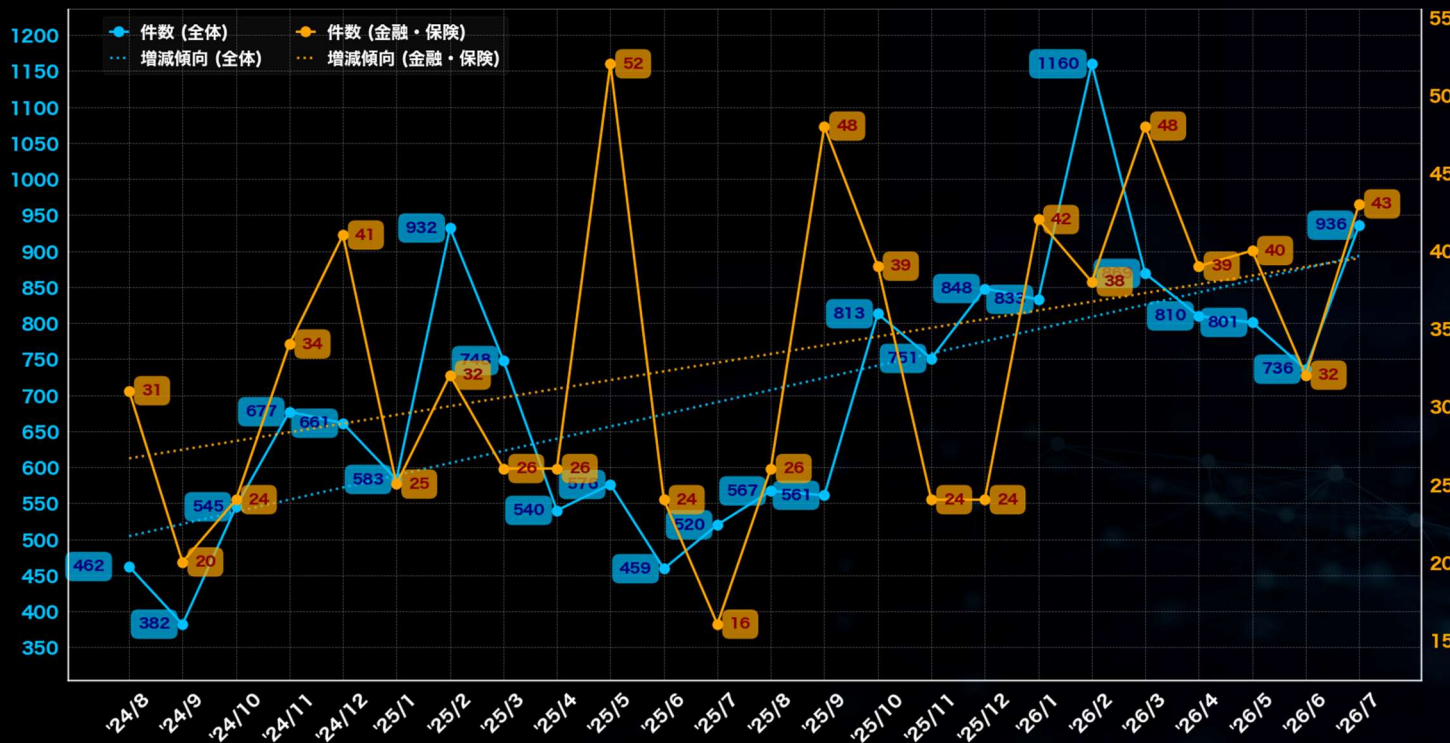
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

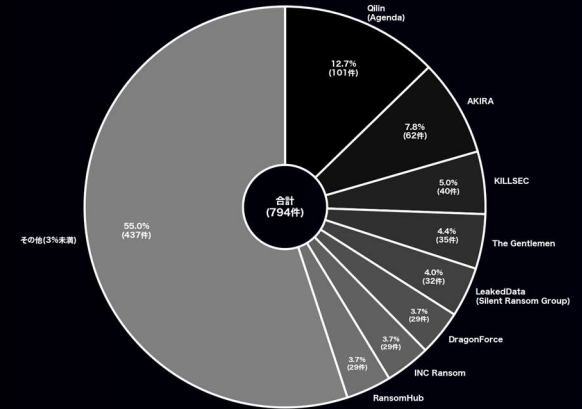
(過去2年間／2024年8月～2026年7月)

金融・保険

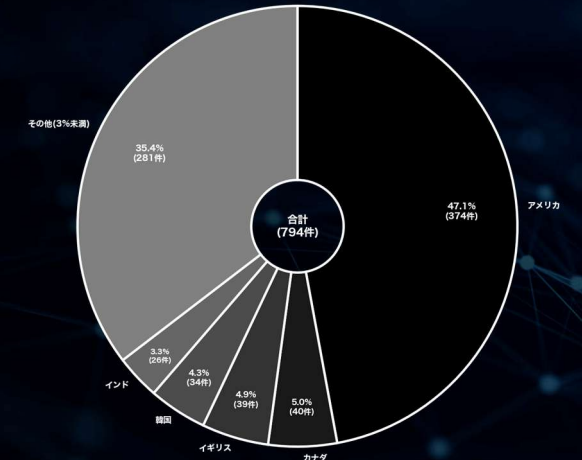
「金融・保険」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年5月で、52件の掲載があった。一方、最も少なかった月は2025年7月で、16件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いでカナダとイギリスがそれぞれ約5%である。攻撃グループについては、少なくとも122のグループが関与しており、特に「Qilin (Agenda)」が101件のリークサイト掲載を実施している。次いで「AKIRA」と「KILLSEC」がそれぞれ62件と40件の掲載を行っている。金融・保険業界は被害件数こそ他業界に比べ少ないものの、関与する攻撃グループは122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



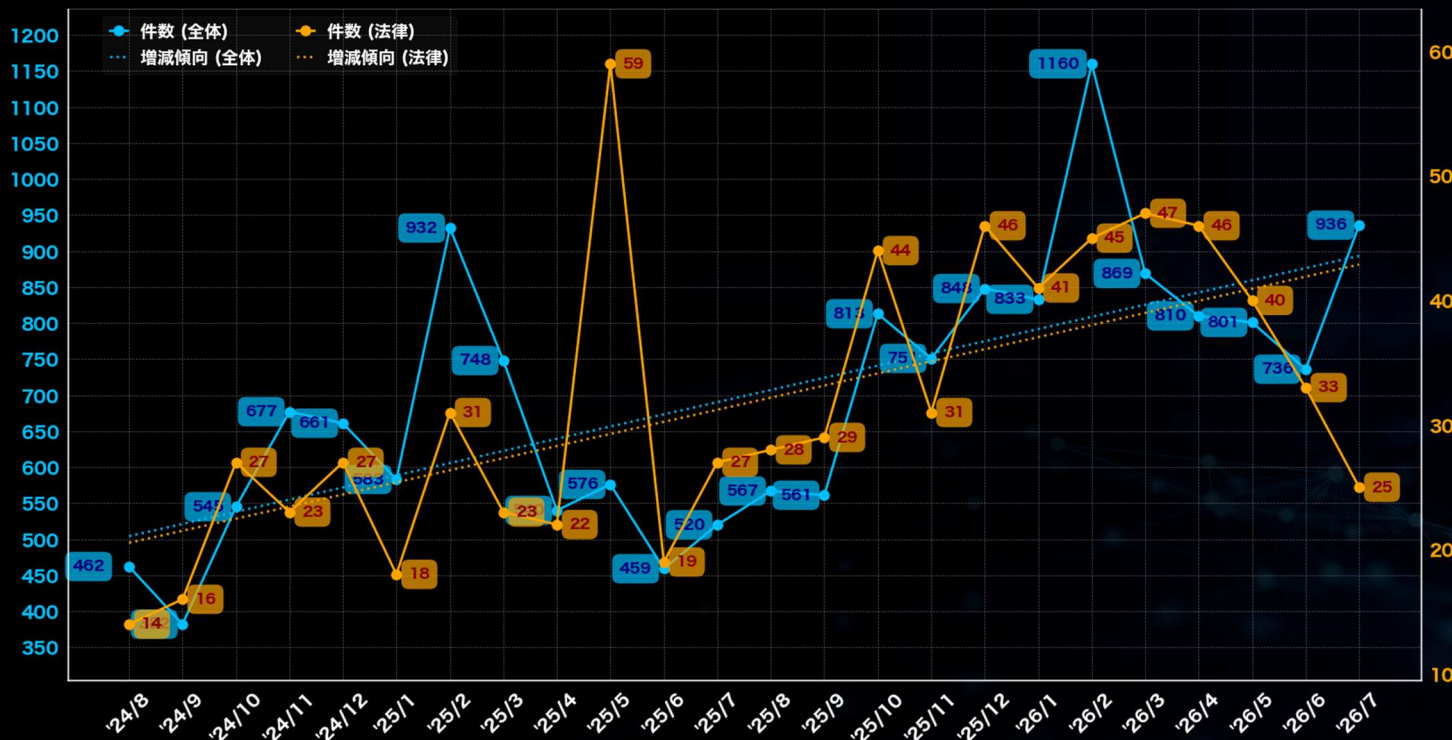
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

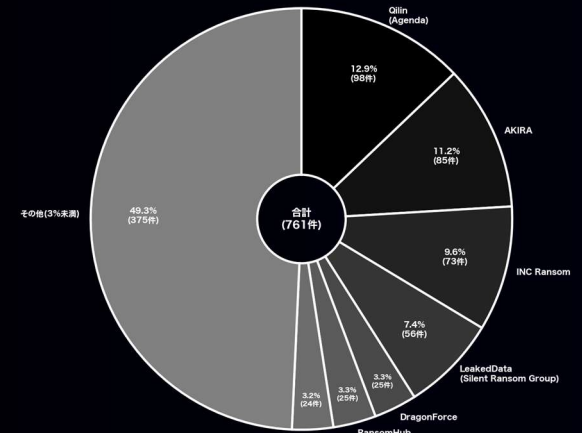
(過去2年間／2024年8月～2026年7月)

法律

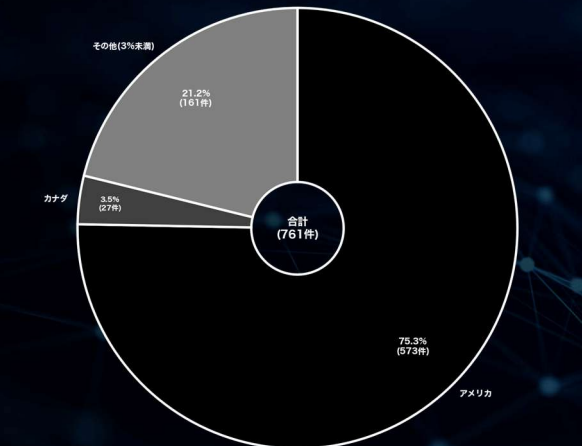
「法律」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年5月で、59件の掲載があった。一方、最も少なかった月は2024年8月で、14件であった。被害組織の所在国の割合では、アメリカが約75%と最も多く、次いでカナダが約4%である。攻撃グループについては、少なくとも95のグループが関与しており、特に「Qilin (Agenda)」が98件のリークサイト掲載を実施している。次いで「AKIRA」と「INC Ransom」がそれぞれ85件と73件の掲載を行っている。法律業界はアメリカの被害が極端に集中している点も特徴である。



▼攻撃グループ別



▼国別



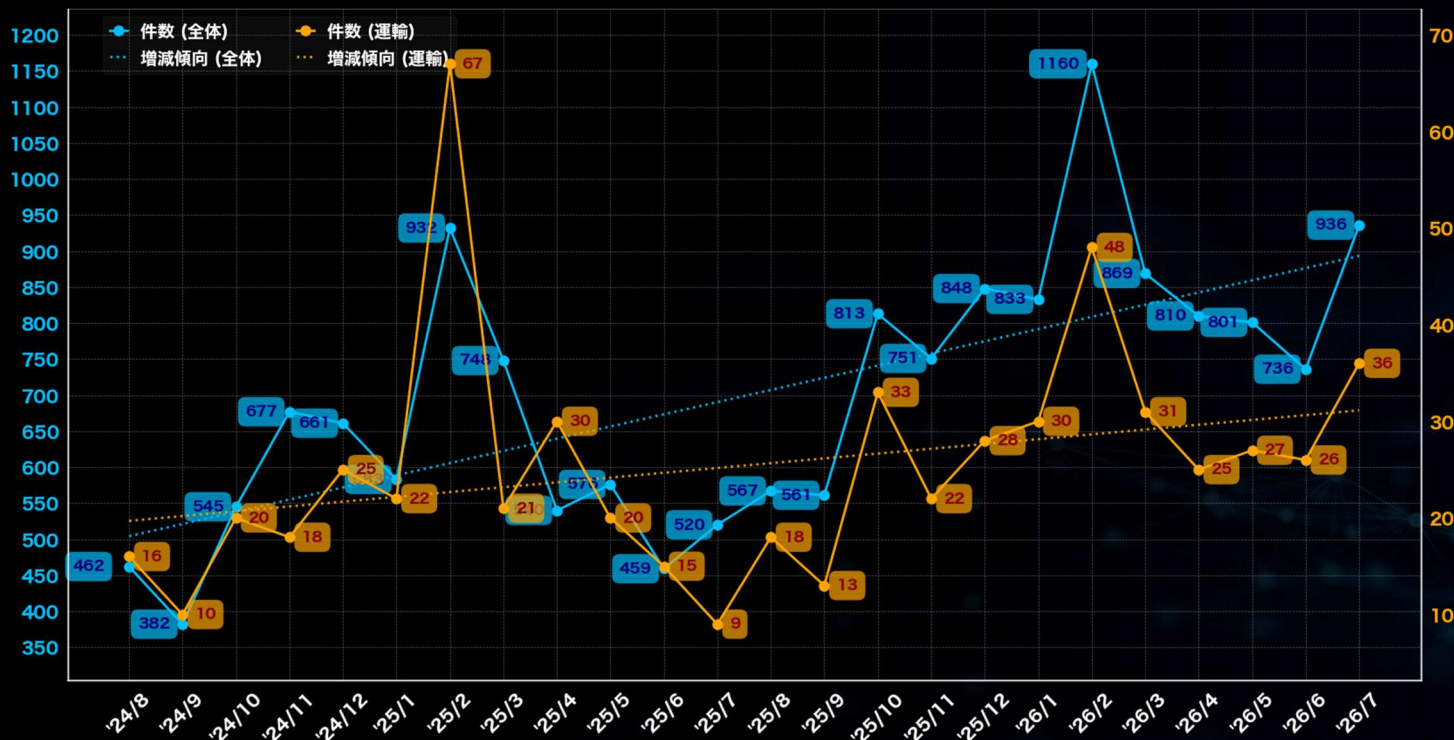
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

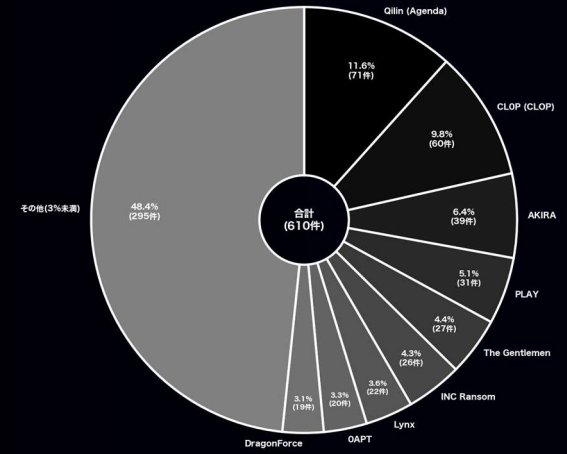
(過去2年間／2024年8月～2026年7月)

運輸

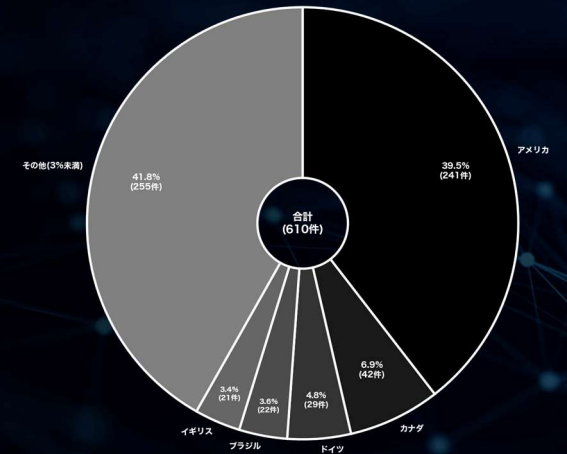
「運輸」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、67件の掲載があった。一方、最も少なかった月は2025年7月で、9件であった。被害組織の所在国の割合では、アメリカが約40%と最も多く、次いでカナダとドイツがそれぞれ7%と約5%である。攻撃グループについては、少なくとも105のグループが関与しており、特に「Qilin (Agenda)」が71件のリークサイト掲載を実施している。次いで「CLOP (CLOP)」と「AKIRA」がそれぞれ60件と39件の掲載を行っている。運輸関係は全体件数に対する割合こそ低いものの、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



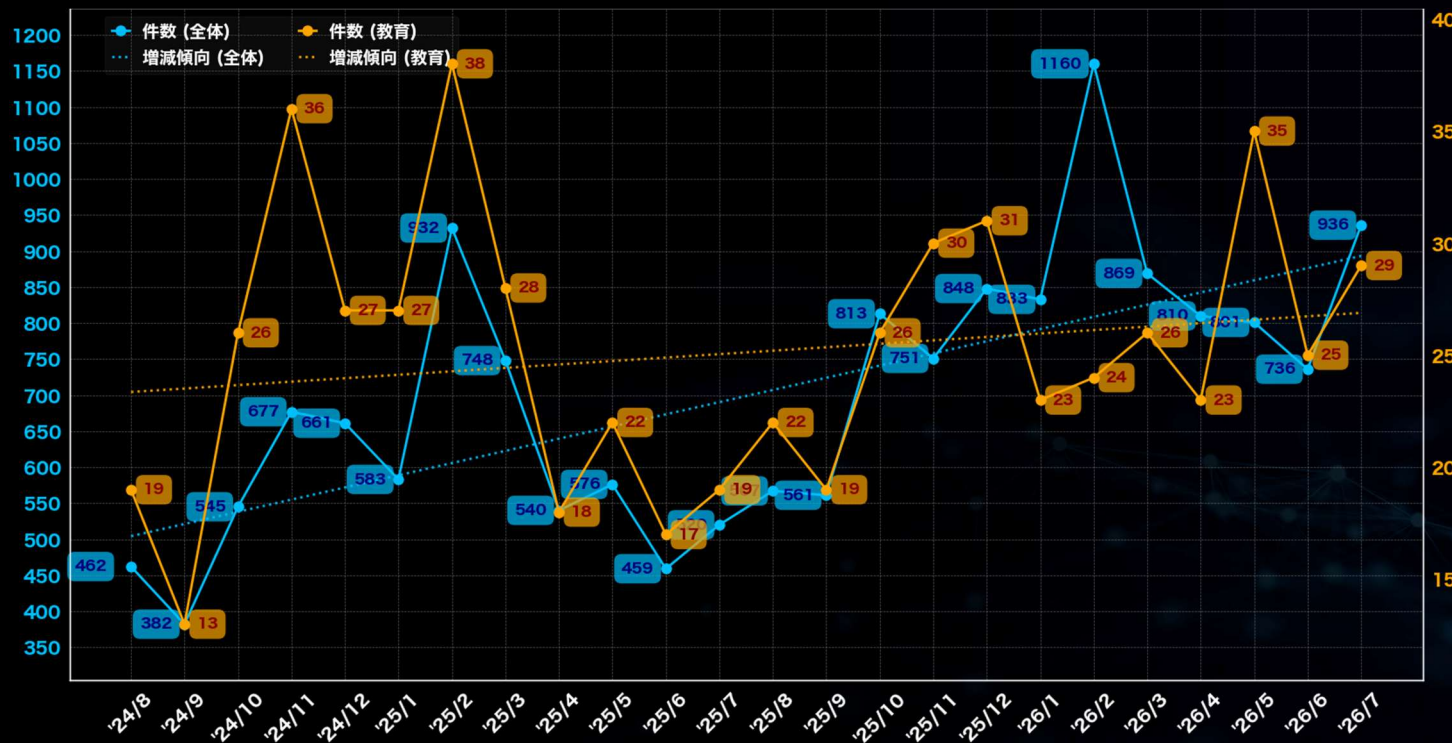
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

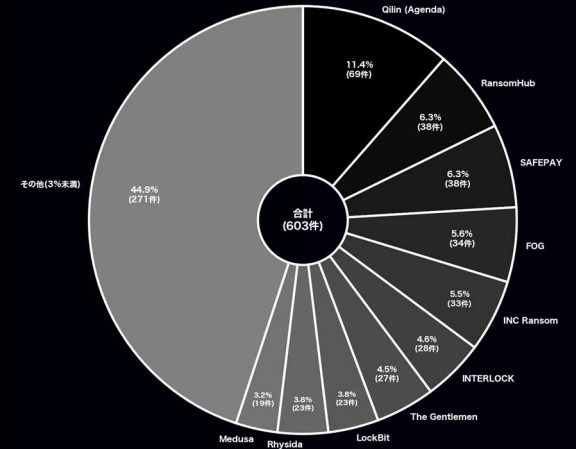
(過去2年間／2024年8月～2026年7月)

教育

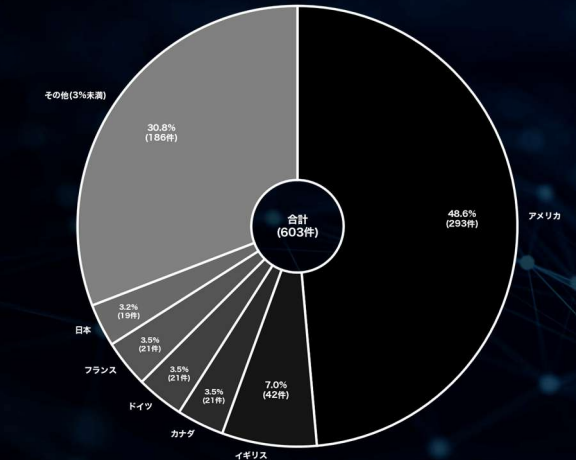
「教育」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、38件の掲載があった。一方、最も少なかった月は2024年9月で、13件であった。被害組織の所在国の割合では、アメリカが約49%と最も多く、次いでイギリスとカナダがそれぞれ約7%と約4%である。攻撃グループについては、少なくとも94のグループが関与しており、特に「Qilin (Agenda)」が69件のリークサイト掲載を実施している。次いで「RansomHub」と「SAFEPAY」がそれぞれ38件の掲載を行っている。教育業界は他業界に比べ被害件数は限定的であるものの、関与する攻撃グループは94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)

CIGのコンテンツ紹介

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

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

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

- CIGランサム統計だより :

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

- 技術ブログ :

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

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

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

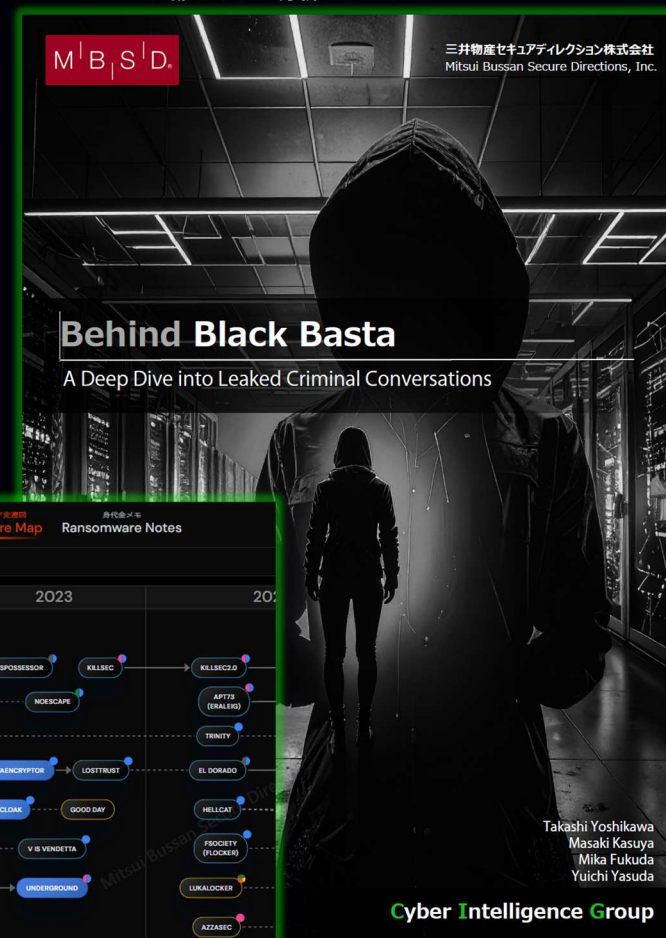
<https://www.mbsd.jp/research/s.urata/>

<https://www.mbsd.jp/research/y.yasuda/>

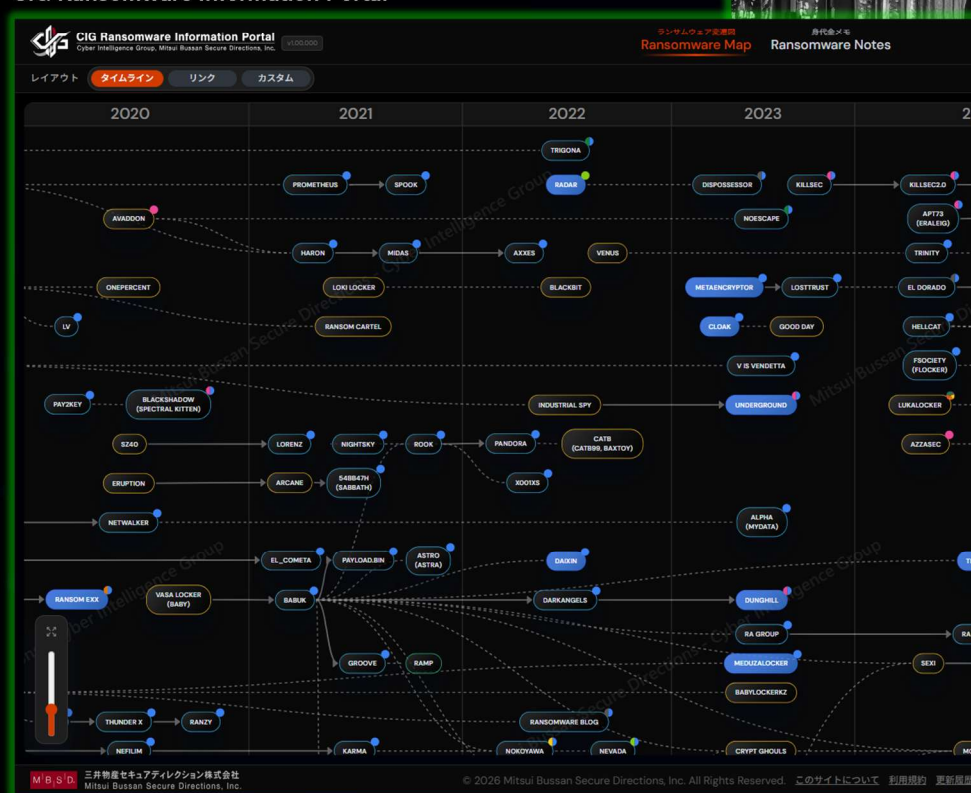
- 分析レポート :

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

Black Basta 内部チャット分析レポート



CIG Ransomware Information Portal



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/>

Mitsui Bussan Secure Directions

M|B|S|D.

Cyber Intelligence Group

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

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