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4月号 Rev 1.00
(2026年3月分)

2026
3

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

総括と監視対象

2026

3

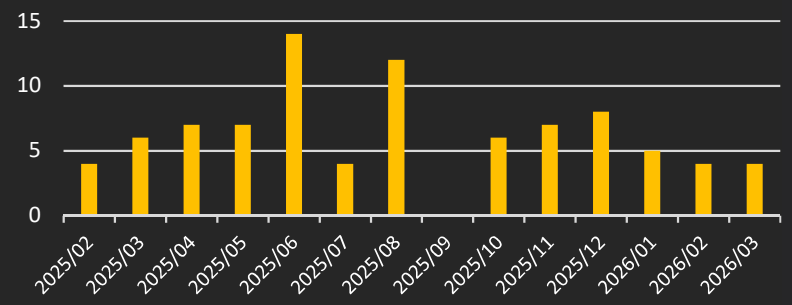
今月のハイライト

Interlock ランサムウェアを展開する Hive0163 が AI を用いてマルウェアを作成

Interlock ランサムウェアを用いる金銭目的の脅威アクター Hive0163 が、AI を用いて生成したとされる悪意あるスクリプト「Slopoly」を攻撃に使用したことが報告されている。解析の結果、このスクリプトは定期的に生存確認用のリクエストを送信し、C2 サーバに対して被害者の環境で実行すべきコマンドの有無を問い合わせるバックドアとして機能していることが判明した。Interlock ランサムウェアによる被害企業の掲載数はランサムウェア全体と比較して少数にとどまるが、攻撃者が AI をランサムウェア攻撃に活用した新たな事例※1, ※2として注目に値する。

Interlock の掲載数

※ CIGによる集計分析



Slopoly: AI で作成したとされる悪意あるスクリプト

サイバー攻撃で利用されるスクリプトは、全容把握を困難にするために難読化したり、耐解析の工夫を行う傾向がある。しかし、Slopoly にはこれに当てはまらない以下の 2 点の特徴が見られた。

- 役割を解説するコメントが随所にある
- 変数名から機能を推測しやすい

AI で特別な指示なしにコードを出力させると人間が理解しやすいように上記の特徴を反映させる傾向があり、Slopoly が AI を利用して作成されたという説は一定の妥当性がある。

近年、攻撃者も AI を活用していると言われているが、本件はその認識を裏付ける事例の一つである。ランサムウェア攻撃につながる悪意あるプログラムを容易に作成できる状況にあることを改めて認識し、適切な対策を講じることが求められる。

Slopoly のコード冒頭

※ CIGによる解析結果

```
# Polymorphic C2 Persistence Client
# Generated: <redacted timestamp>
# Session ID: <redacted>

# Initialize script scope variables
$script:SessionId = "<redacted>"
$script:MutexHandle = [System.Threading.Mutex]::new($false, "<redacted>")
if (-not $script:MutexHandle.WaitOne(0, $false)) { exit }
$script:C2Url = "https://p                              'api/commands"
$script:HeartbeatInterval = 30  # Heartbeat every 30 seconds
$script:CommandPollInterval = 50  # Command polling every 50 seconds
```

役割を解説するコメント

分かりやすい変数名

Slopoly のコードのメイン部分

```
# Main execution loop
function DumbFetch {
    ShortWeak

    RejectLow "Polymorphic C2 client started - Session: $script:SessionId"

    $script:StartTime = Get-Date

    while ($true) {
        # Always do heartbeat every 30 seconds
        StartFetch

        # Check if it's time to poll commands (every 50 seconds)
        $currentTime = (Get-Date) - $script:StartTime
        if ($currentTime.TotalSeconds - $script:LastCommandPoll -ge $script:CommandPollInterval) {
            PoorStrong
            $script:LastCommandPoll = $currentTime.TotalSeconds
        }

        # Sleep for 30 seconds before next heartbeat
        Start-Sleep -Seconds $script:HeartbeatInterval
    }
}
```

役割を解説するコメント

※1: (参考情報) https://www.ibm.com/think/x-force/slopoly-start-ai-enhanced-ransomware-attacks
※2: (参考情報) https://hivepro.com/threat-advisory/ai-assisted-slopoly-backdoor-powers-interlock-ransomware-intrusion/

※ 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3月18日～2026年4月8日）

【Interlock、Cisco脆弱性を1月からゼロデイ悪用】（BleepingComputer: 2026/3/18）
Interlockランサムウェアが Ciscoのゼロデイ脆弱性をパッチ公開の約1か月前から悪用していたことをAmazonが確認。ClickFix・NodeSnake・Slopolyも駆使し、医療・大学・行政機関などが標的となっている。
https://www.bleepingcomputer.com/news/security/interlock-ransomware-exploited-secure-fmc-flaw-in-zero-day-attacks-since-january/

【米企業侵害と大規模恐喝を支援したロシア人に禁固81カ月】（米司法省: 2026/3/23）
26歳のロシア人Aleksei Volkovが「初期アクセスブローカー」としてYanluowang等のランサムウェア集団に侵入経路を販売。ローマで逮捕、米国に身柄引渡しの上、900万ドル超の実損害で禁錮81カ月。
https://www.justice.gov/opa/pr/russian-citizen-sentenced-prison-hacking-us-companies-and-enabling-major-cybercrime-groups

【イラン系ランサムウェア集団、軍事衝突下で米医療機関を標的化】（The Record: 2026/3/24）
Pay2Keyランサムウェアが米 - イラン軍事衝突と同時期に米国医療機関を攻撃。金銭だけでなく破壊効果も重視する傾向があり、イラン政府寄りの活動と収益獲得を併せ持つ「二重目的」の運営が指摘されている。
https://therecord.media/iran-linked-ransomware-gang-targeted-us-healthcare-org

【M-Trends 2026：最前線からのデータ、インサイト、戦略】（Google Cloud Blog: 2026/3/24）
Mandiantが2025年に実施したインシデント対応調査を基にまとめた年次レポートを公開。ランサムウェアはバックアップ、IDサービス、仮想化管理基盤を狙って復旧能力そのものを奪う方向へシフトしている。
https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026

【ロシア人ボットネット運用者に米国で実刑判決】（米司法省: 2026/3/24）
ミシガン東部連邦地裁がロシア人Ilya Angelovに禁固24ヶ月・罰金10万ドルの判決。運用したボットネットがBitPaymerランサムウェア感染を支援し、米国の70社以上に1,400万ドル超の身代金被害を与えた。
https://www.justice.gov/usao-edmi/pr/russian-cybercriminal-sentenced-prison-using-botnet-steal-millions-american-businesses

【RSAC 2026：AIエージェント型サイバー犯罪の次世代脅威】（Trend Micro: 2026/3/31）
エージェント型AIを活用し、偵察から恐喝までの犯罪工程を自動化する攻撃手法が台頭しつつあり、窃取データの分析や被害組織ごとの恐喝文生成の自動化が実証例とともにRSAC 2026で報告。
https://www.trendmicro.com/en_us/research/26/c/trendai-research-at-rsac-2026.html

【ランサムウェアは医療機関を標的に、防御の鍵は訓練の実施】（Dark Reading: 2026/4/2）
病院へのランサムウェア攻撃は避けられない前提で、紙ベース運用への切り替え訓練や「グレーゾーン障害」を含む段階的なリハーサルが被害拡大防止の鍵と、San Joaquin General HospitalのCMIOが強調。
https://www.darkreading.com/cybersecurity-operations/ransomware-hospitals-preparation-key-defense

【BKA、ドイツ国内130件のランサムウェア攻撃に関与したREvil首謀者を特定】（The Hacker News: 2026/4/6）
ドイツ連邦刑事局（BKA）が現在は活動停止したREvil（Sodinokibi）の幹部2名のロシア人を特定し国際手配。2人はドイツ国内で130件の攻撃に関与し、被害総額は3,540万ユーロ超とされる。
https://thehackernews.com/2026/04/bka-identifies-revil-leaders-behind-130.html

【Storm-1175、公開Web資産を狙う高頻度Medusa攻撃を展開】（Microsoft Security Blog: 2026/4/6）
Storm-1175はN-dayおよびゼロデイ脆弱性を悪用し、開示から最短1日でMedusaランサムウェアを展開。RMMツールや資格情報窃取を駆使し、医療・教育・金融セクターを中心に被害が拡大している。
https://www.microsoft.com/en-us/security/blog/2026/04/06/storm-1175-focuses-gaze-on-vulnerable-web-facing-assets-in-high-tempo-medusa-ransomware-operations/

【QilinおよびWarlockランサムウェア、300種以上のEDRツールを無効化】（The Hacker News: 2026/4/6）
QilinとWarlockがBYOVD手法で300以上のEDR製品を無効化してからランサムウェアを展開する手口をCisco TalosとTrend Microが報告。初期侵入から実行まで平均約6日であり、早期検知と展開阻止が重要。
https://thehackernews.com/2026/04/qilin-and-warlock-ransomware-use.html

【RSAC 2026：サイバー保険とランサムウェアの台頭】（TechTarget: 2026/4/8）
攻撃者がサイバー保険のカバー額に合わせて身代金を設定する手口がRSAC 2026で報告された。保険加入企業は未加入の2.8倍の身代金を要求されており、保険が逆に攻撃者の収益最大化に利用されている。
https://www.techtarget.com/searchsecurity/feature/RSAC-2026-Cyber-insurance-and-the-rise-of-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）（※2）：314

→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：61

※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）

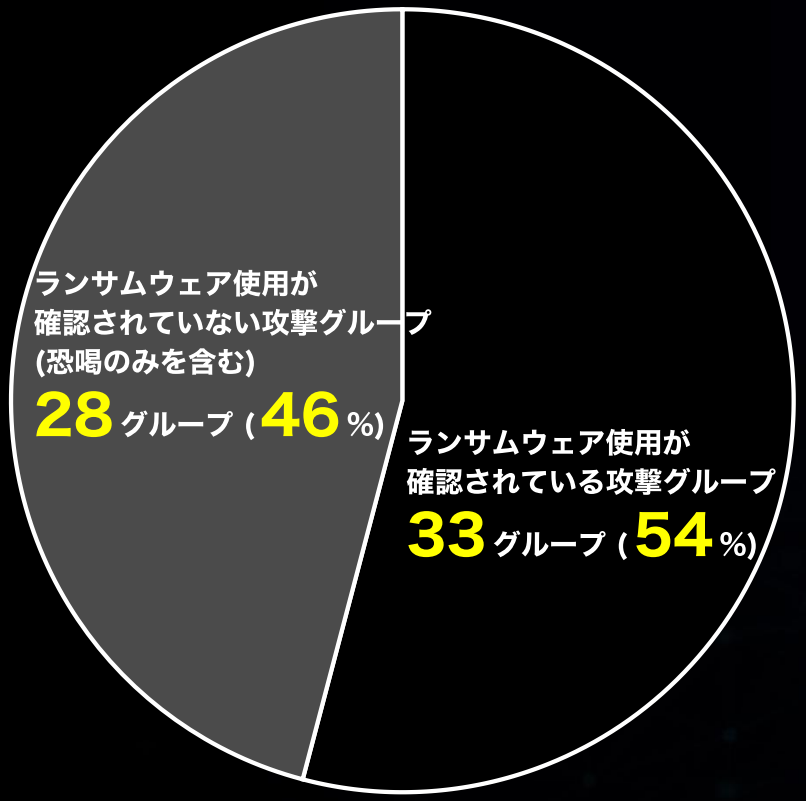
0APT
0mega (Omega)
8BASE
Abyss
● AiLock
AKIRA
AKO
● ALP-001
Alpha (MYDATA)
AlphV (BlackCat)
Anubis
Apos Security
APT73 (Eraleig)
ARACHNA
ARCUS MEDIA
Argonauts
Arkana
ArvinClub
Astro (Astra)
Atomsilo
Avaddon
AvosLocker
AWARE
Axxes
AzzaSec
Babuk
Babuk (2025)
BASHE
BEAST
Benzona
BERT
BianLian
BL0ODY (BLOODY)
Bl4ckt0r (BlackTor)
Black Basta
BlackByte
BlackDolphin
BlackField
BlackLock
BlackMatter
Black Nevas
Blackout
BLACKSHRANTAC
BlackSuit
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
ICEFIRE
IMN Crew
INC Ransom
Insane
INSOMNIA
INTERLOCK
J GROUP
KAIROS
Karakurt
Karma
Kawa4096
Kazu
KILLSEC
Kittykatkrew
Knight
Kraken (HelloKitty)
Kryptos
Kyber
LAMBDA
La Piovra
LAPSUS$
LAPSUS$ Group
LeakedData (Silent Ransom Group)
LEAKNET
LILITH
Linkc
LockBit
● LOKI
Lorenz
LostTrust
LunaLock
LV
LYNX
MADCAT
MAD LIBERATOR
MALAS
MalekTeam
Mallox
Mamona RIP
MBC
Medusa
MEDUZA LOCKER
MEOW
Metaencryptor
Midas
MIGA
Mindware
Minteye
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
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)
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 3月）

（※当月にリークサイト掲載を確認した攻撃グループ全61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3月に活動中である事が確認された全61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

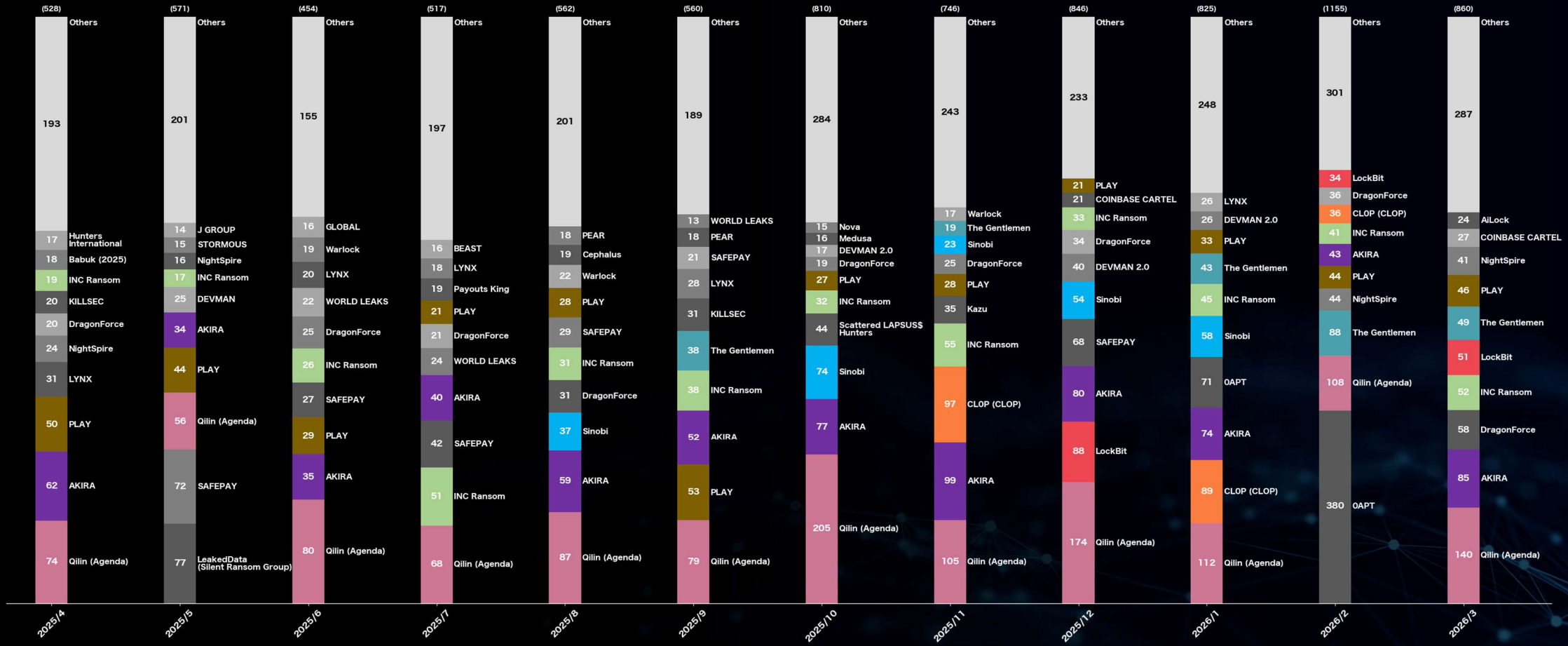
年間 統計
（全世界）

2026

3

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4月～2026年3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

3

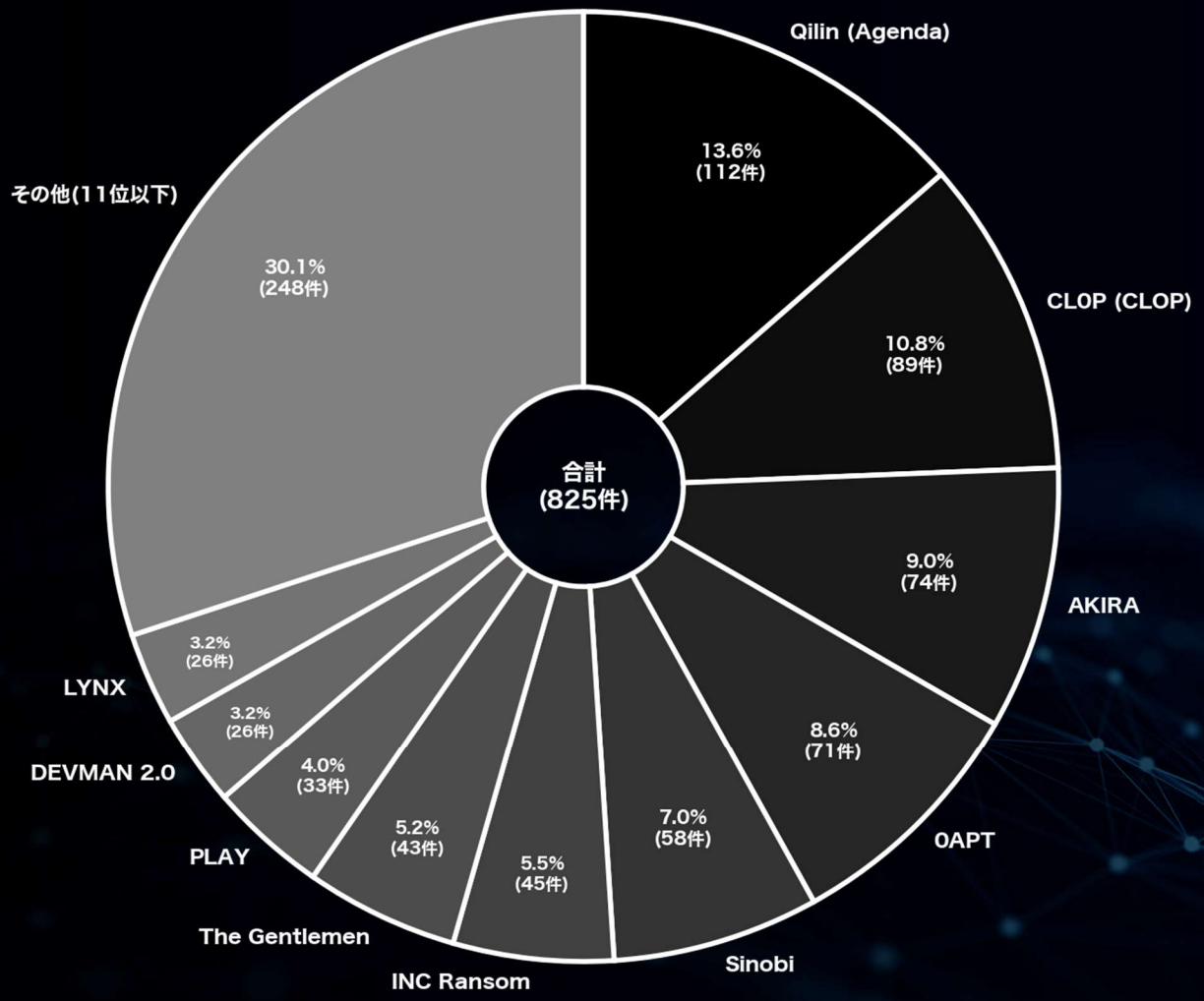
月別内訳 攻撃グループ TOP10（全世界）

（2026年 1月）

※件数順に降順／同件数のものが含まれる場合は名前順でTOP10までを記載

攻撃グループ名	件数	割合(%)	前月比(件数)
Qilin (Agenda)	112	13.6	- 62
CL0P (CLOP)	89	10.8	+ 88
AKIRA	74	9.0	- 6
0APT	71	8.6	+ 71
Sinobi	58	7.0	+ 4
INC Ransom	45	5.5	+ 12
The Gentlemen	43	5.2	+ 32
PLAY	33	4.0	+ 12
DEVMAN 2.0	26	3.2	- 14
LYNX	26	3.2	+ 12

▼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

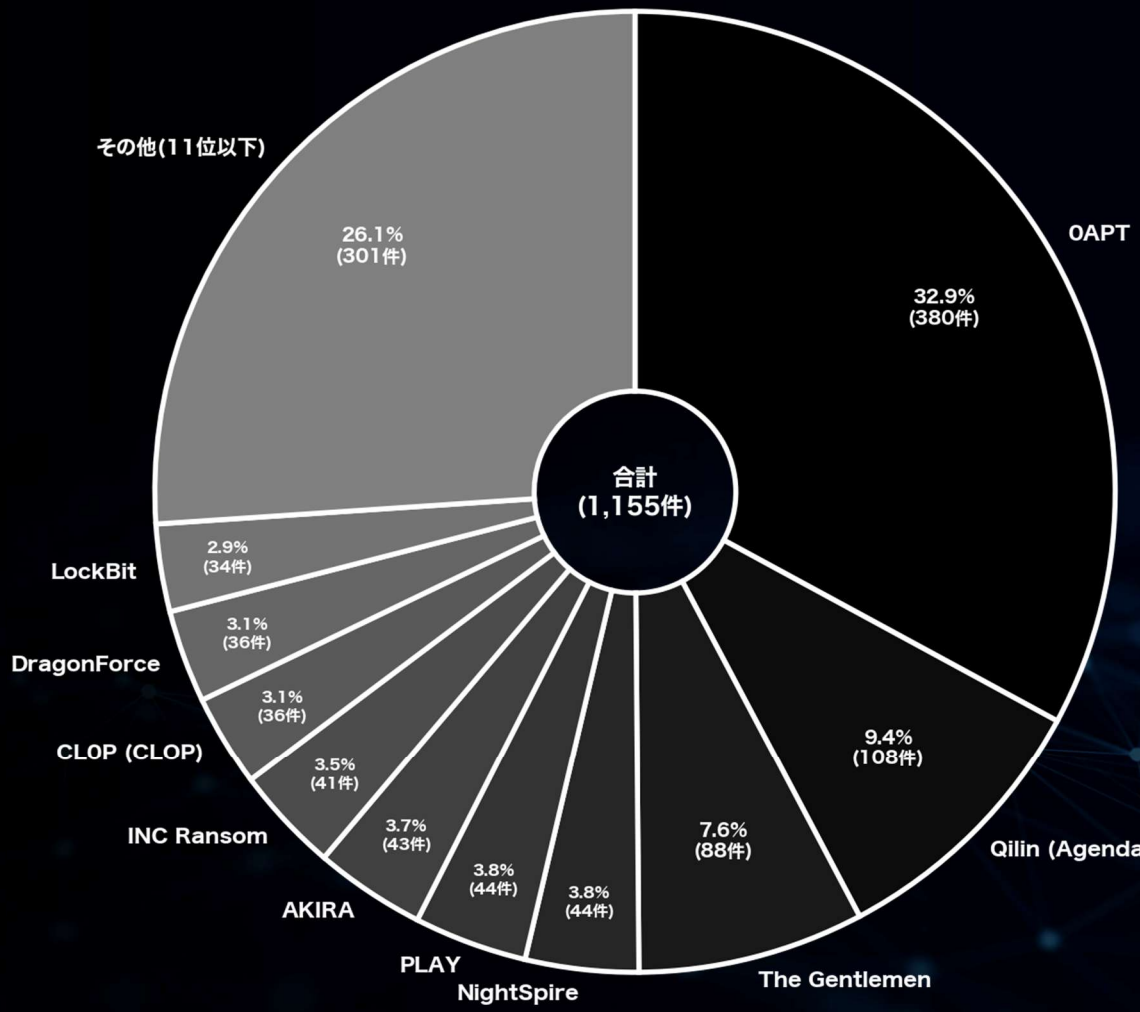
月別内訳 攻撃グループ TOP10（全世界）

（2026年 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

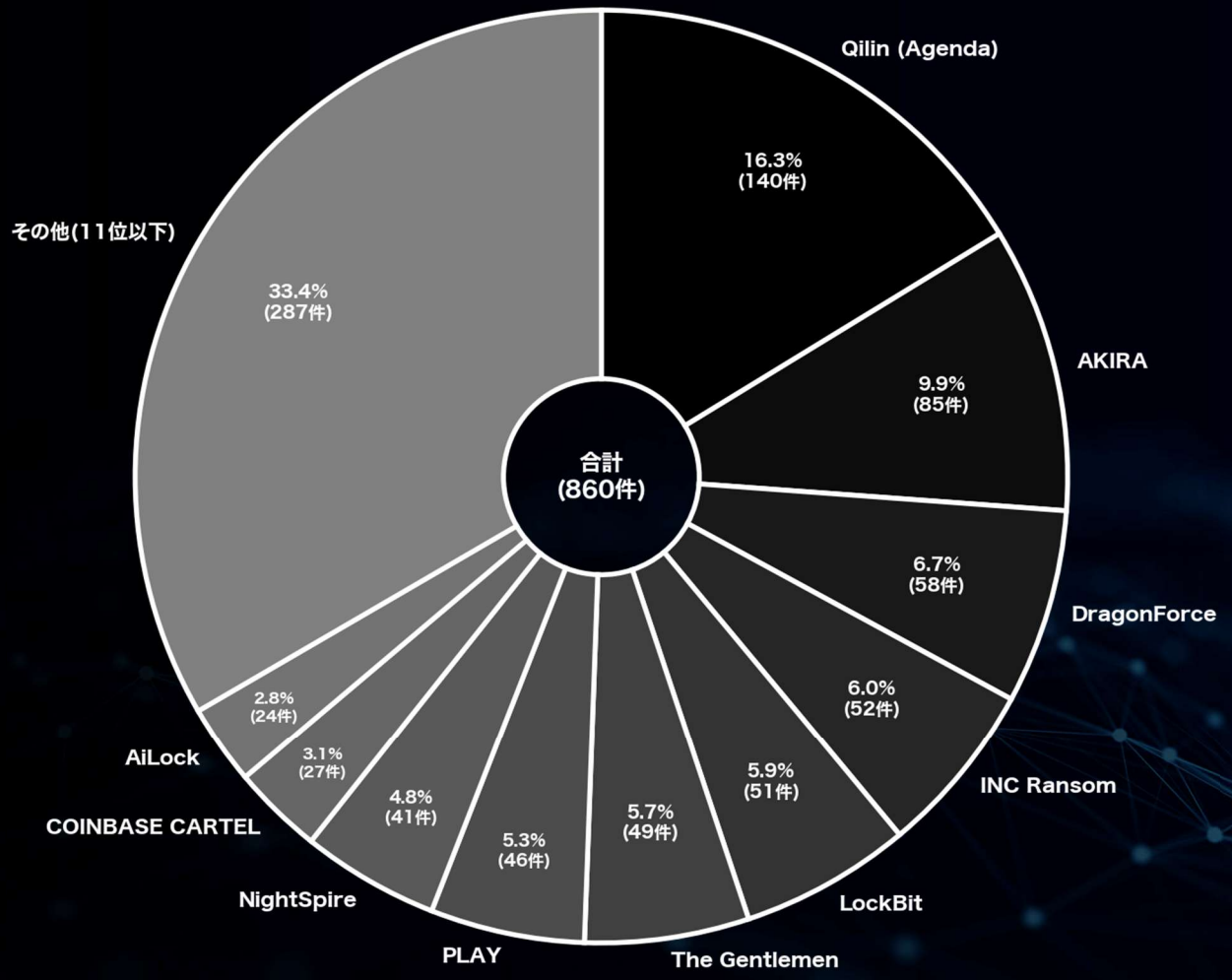
月別内訳 攻撃グループ TOP10（全世界）

（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	16.3	+ 32
AKIRA	85	9.9	+ 42
DragonForce	58	6.7	+ 22
INC Ransom	52	6.0	+ 11
LockBit	51	5.9	+ 17
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

被害国 月別統計
（全世界）（過去3ヶ月分）

2026
3

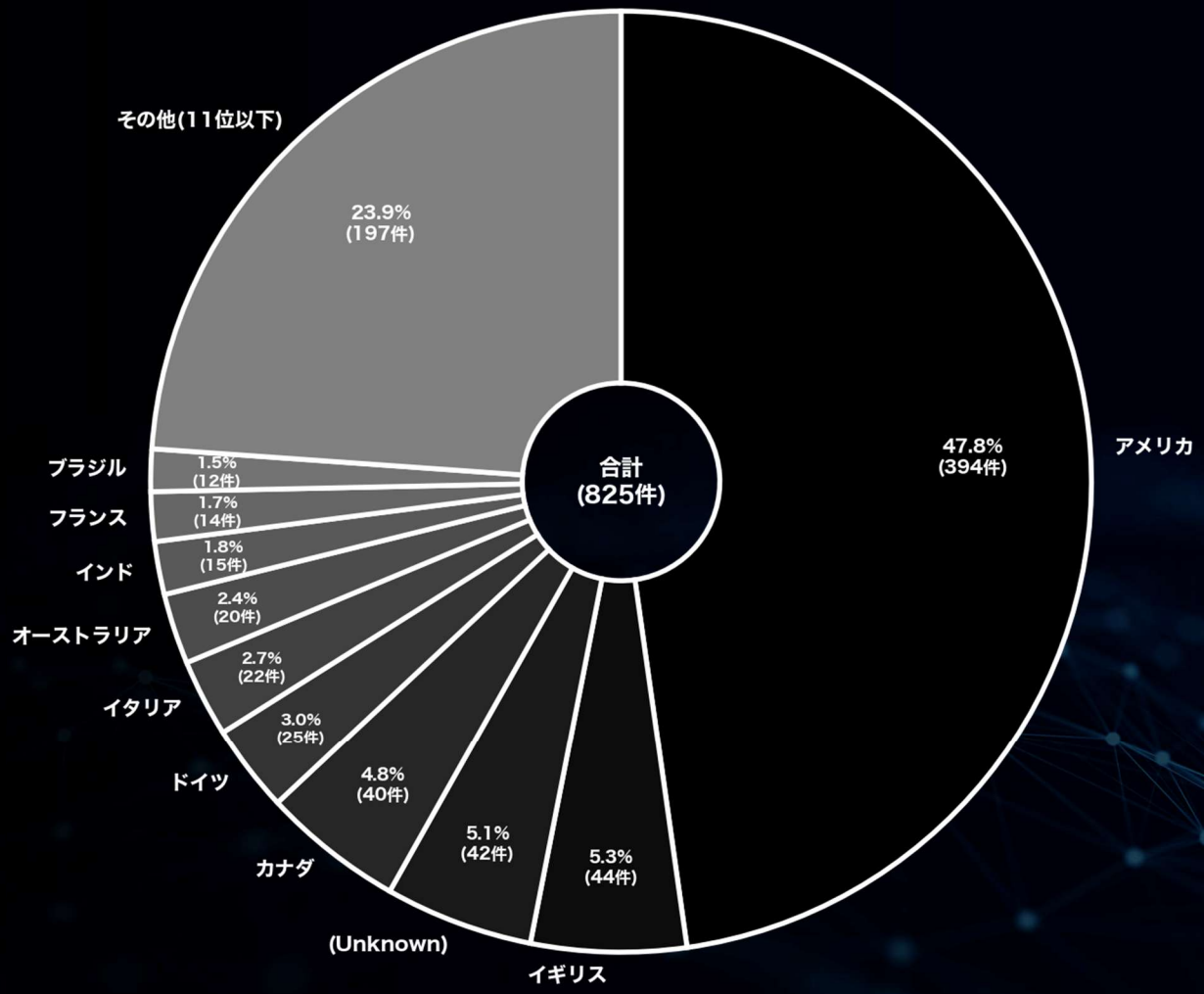
月別内訳 被害国TOP10（全世界）

（2026年 1月）

※件数順に降順／同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
アメリカ	394	47.8	+ 22
イギリス	44	5.3	+ 16
(Unknown)	42	5.1	+ 15
カナダ	40	4.8	± 0
ドイツ	25	3.0	- 14
イタリア	22	2.7	+ 2
オーストラリア	20	2.4	+ 9
インド	15	1.8	- 2
フランス	14	1.7	- 10
ブラジル	12	1.5	- 7

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



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

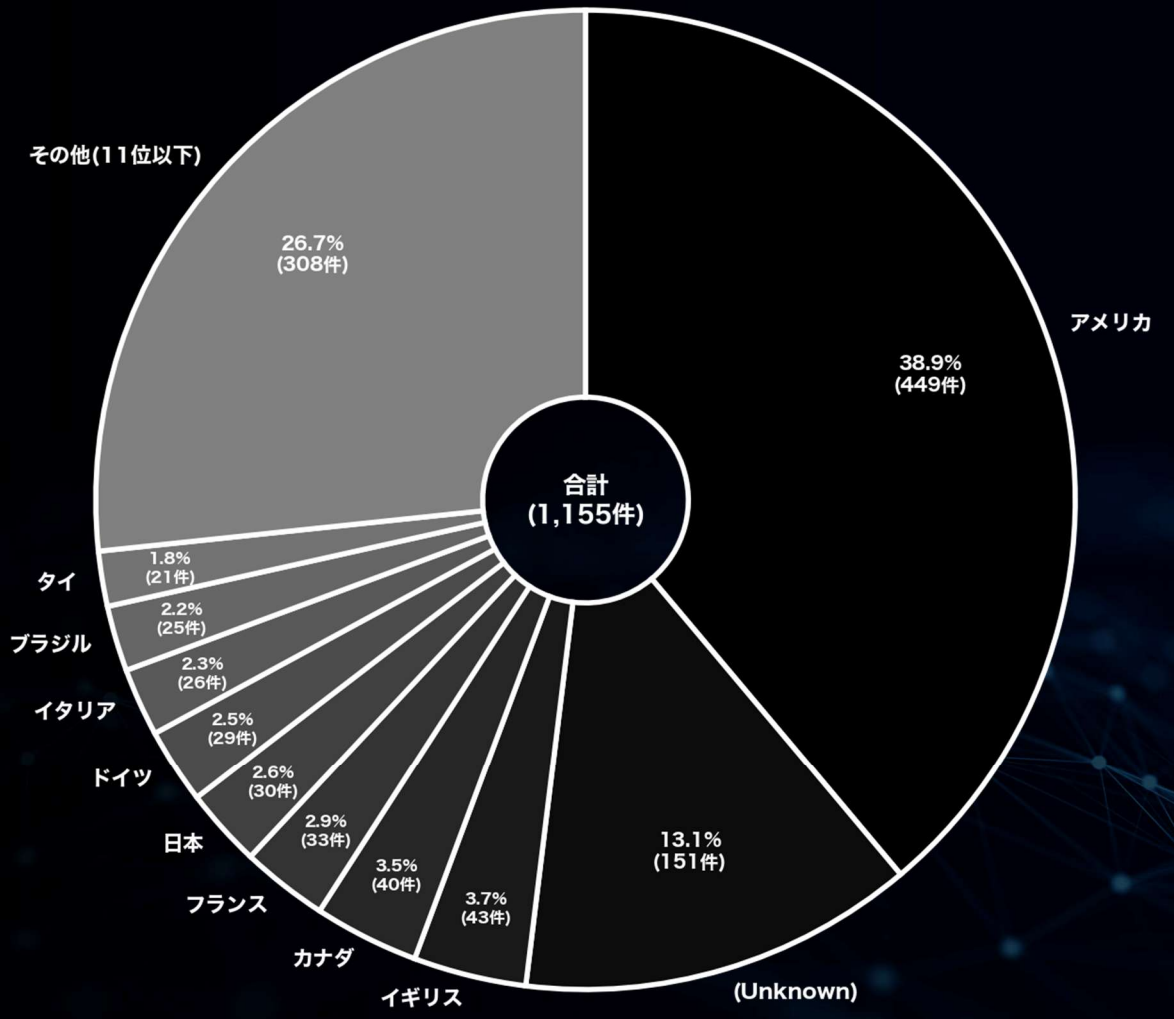
月別内訳 被害国TOP10（全世界）

（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

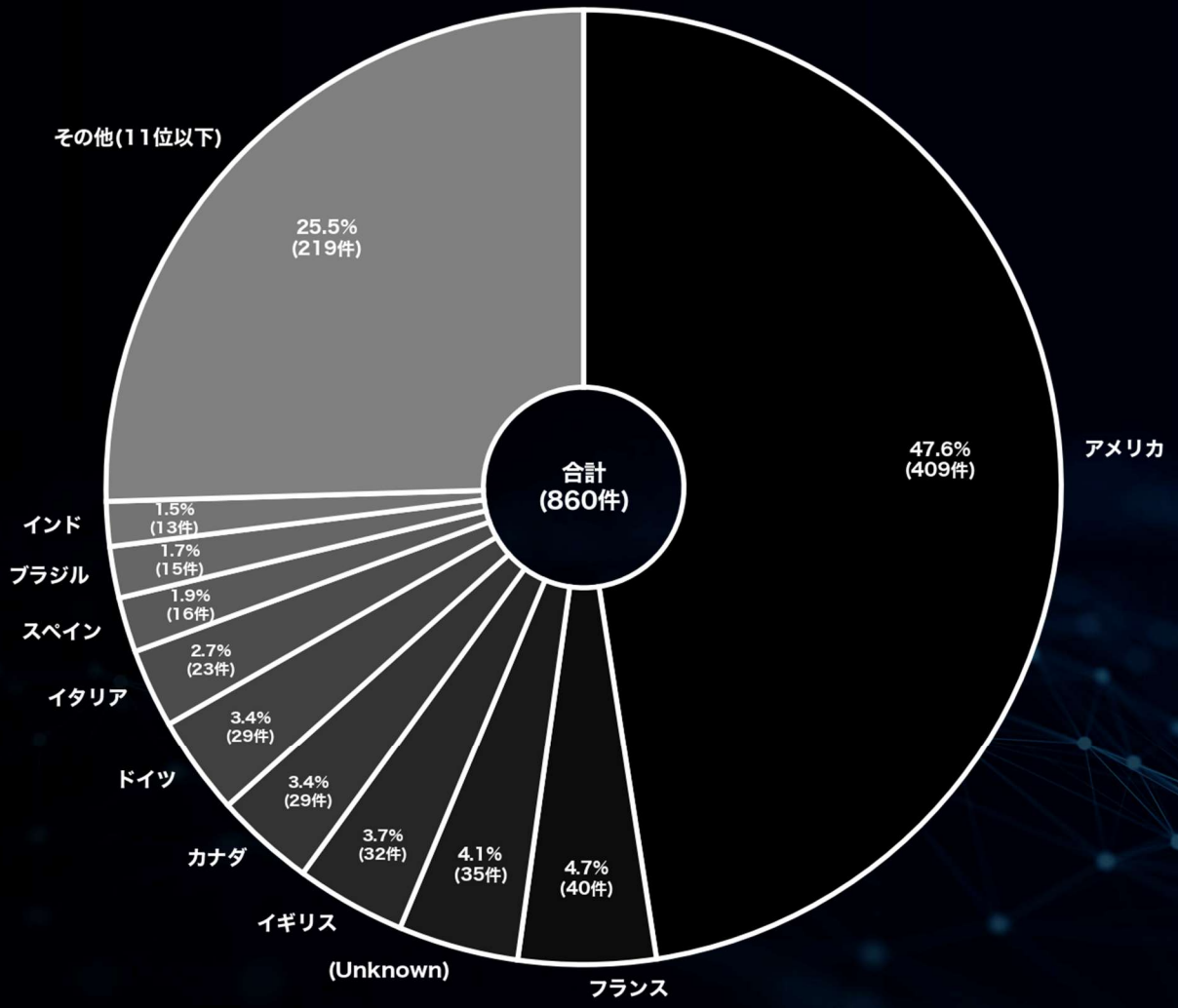
月別内訳 被害国TOP10（全世界）

（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	47.6	- 40
フランス	40	4.7	+ 7
(Unknown)	35	4.1	- 116
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

被害国 月別統計
（アジア）　（過去3ヶ月分）

2026

3

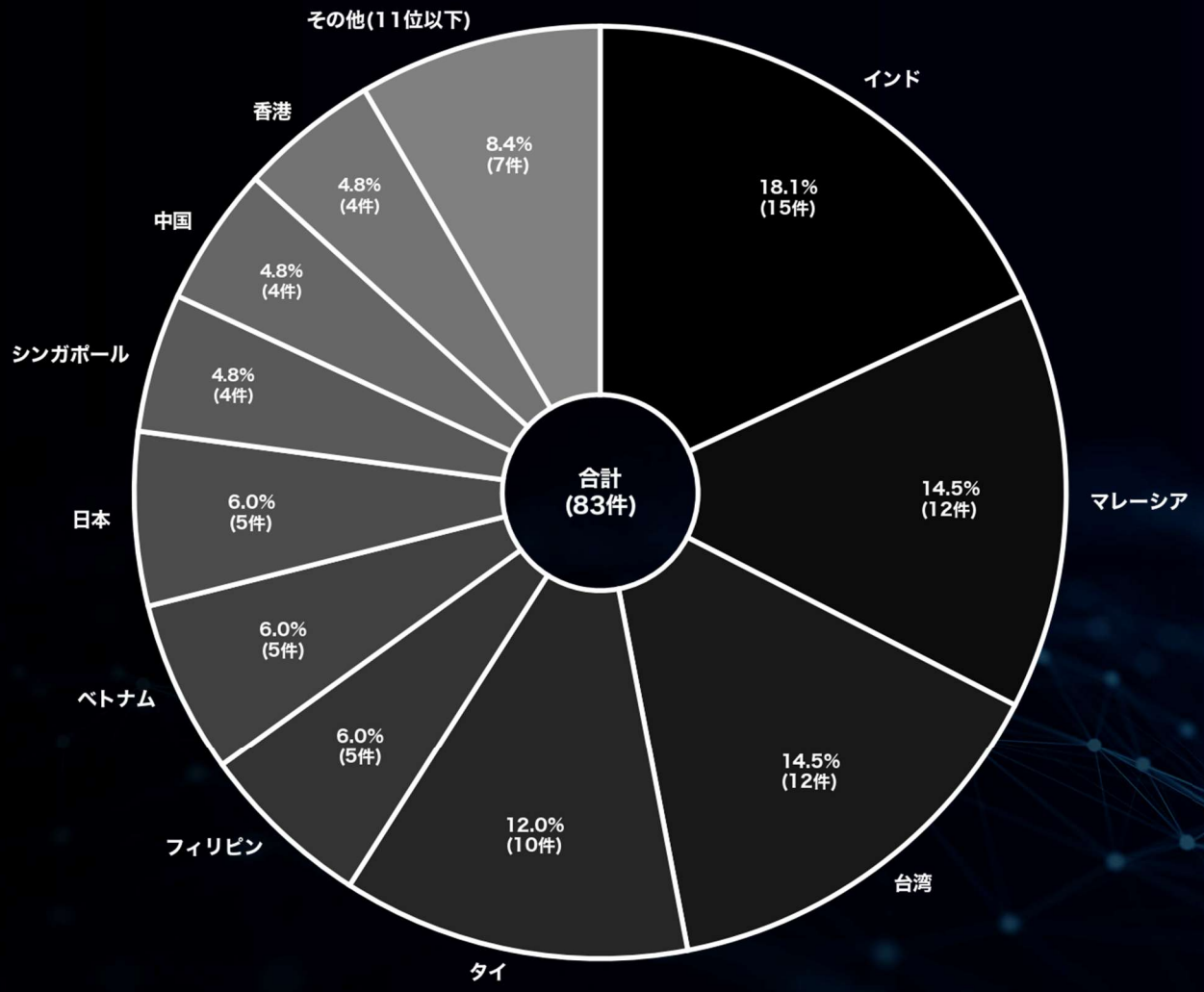
月別内訳 被害国TOP10（アジア）

（2026年 1月）

※件数順に降順／同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
インド	15	18.1	- 2
マレーシア	12	14.5	+ 4
台湾	12	14.5	+ 7
タイ	10	12.0	+ 3
フィリピン	5	6.0	± 0
ベトナム	5	6.0	+ 3
日本	5	6.0	- 10
シンガポール	4	4.8	- 3
中国	4	4.8	+ 3
香港	4	4.8	+ 3

▼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

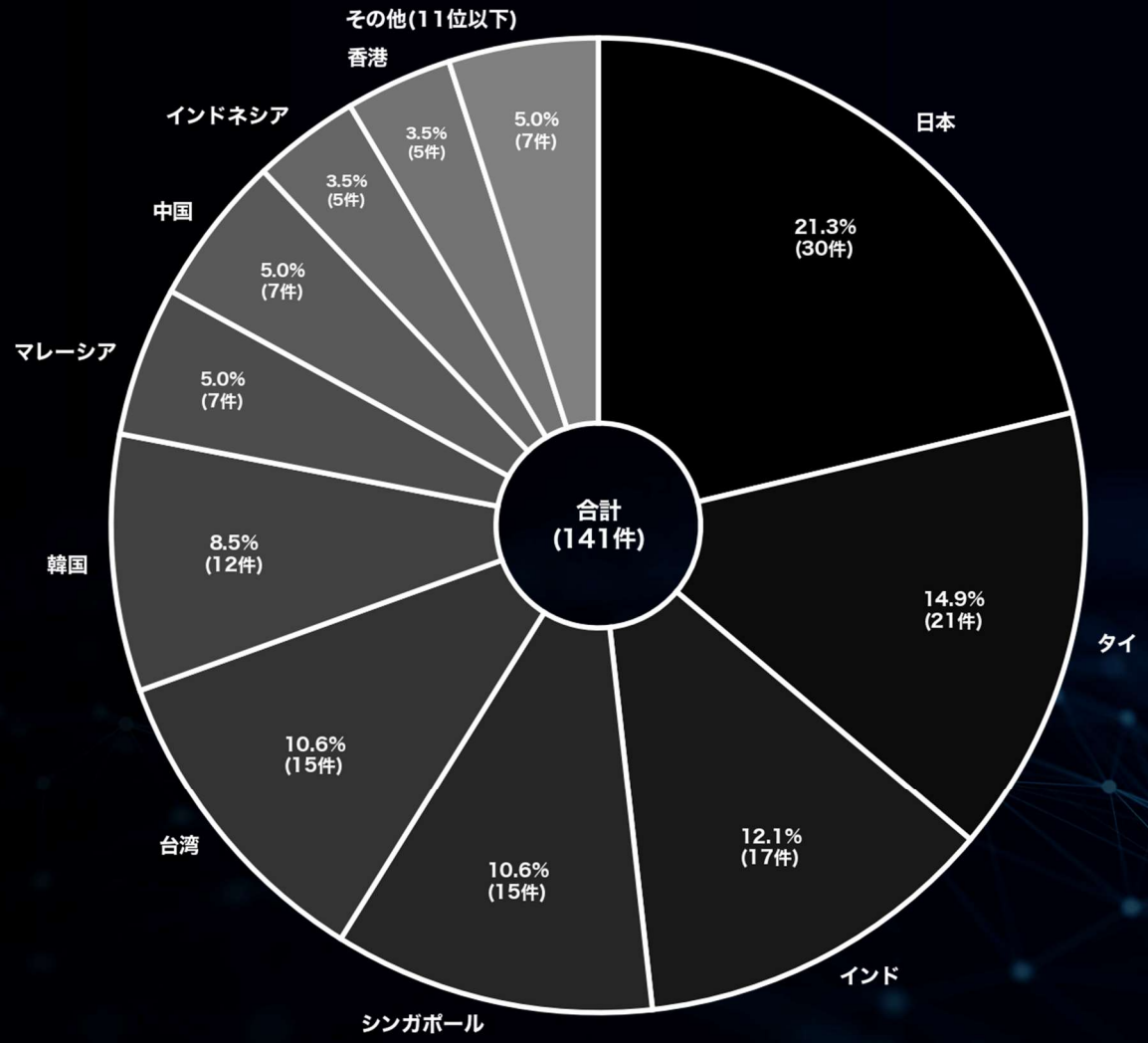
月別内訳 被害国TOP10（アジア）

（2026年 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

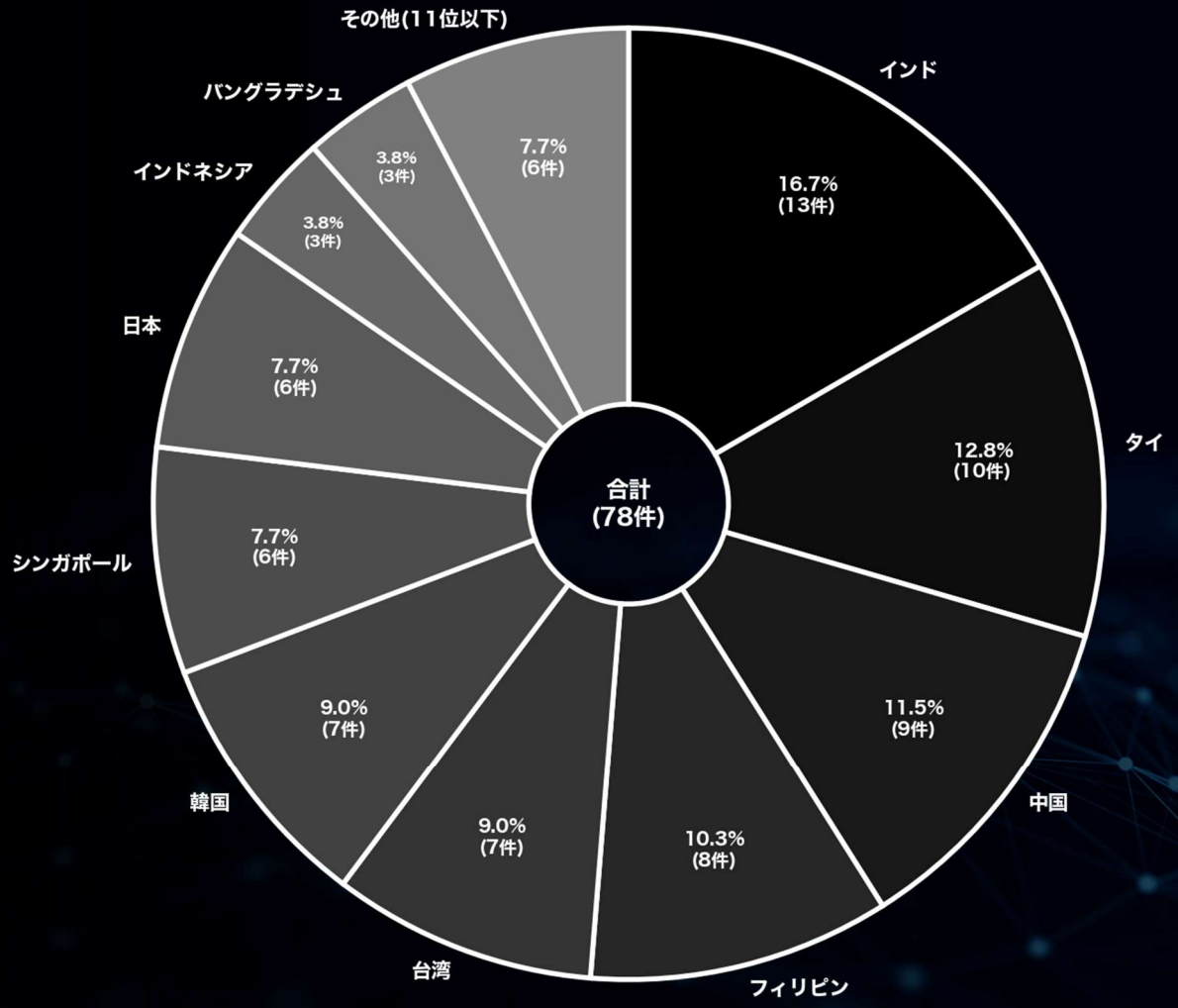
月別内訳 被害国TOP10（アジア）

（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

業種 月別統計
（全世界） （過去3ヶ月分）

2026
3

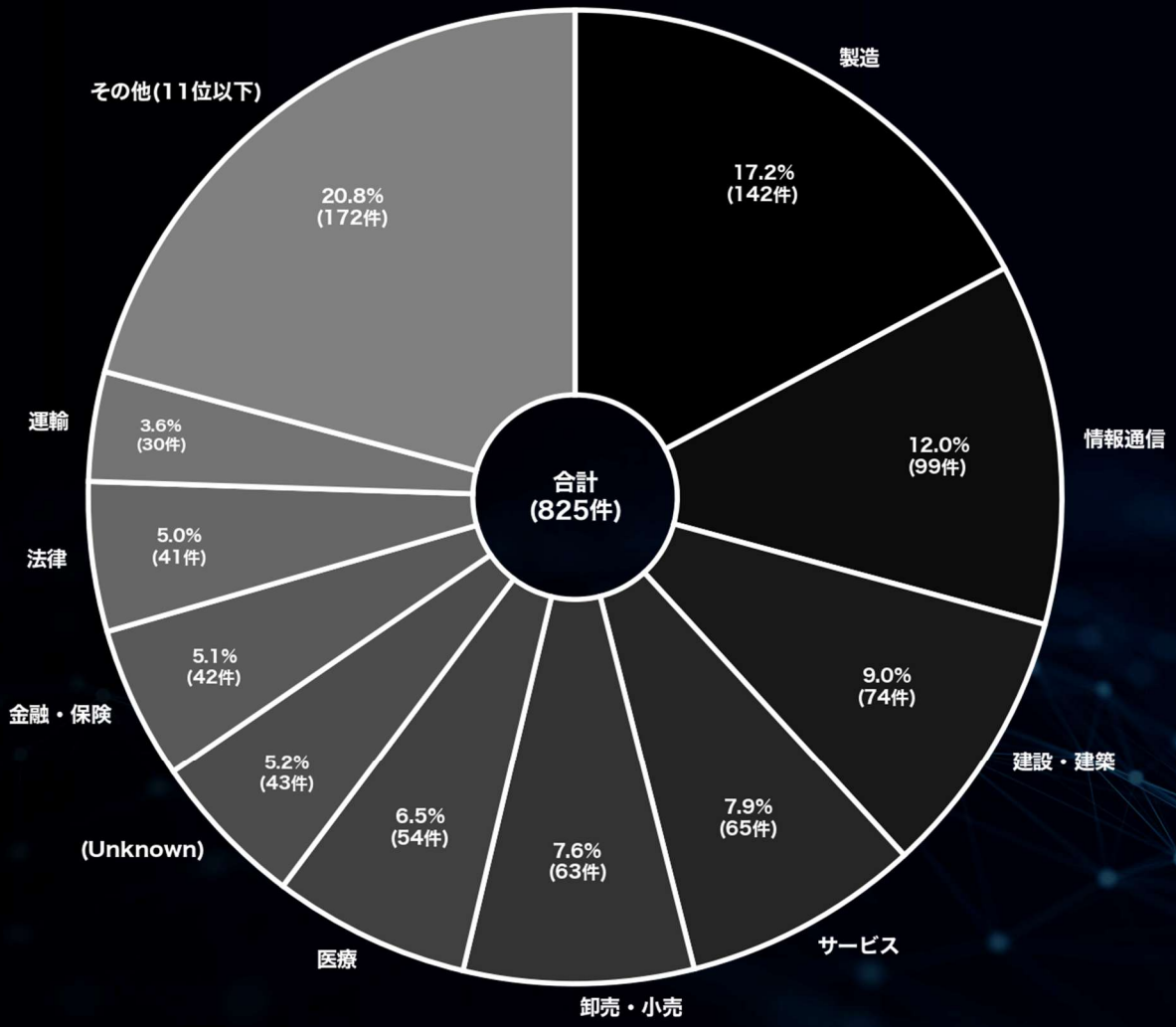
月別内訳 業種 TOP10（全世界）

（2026年 1月）

※件数順に降順／同件数のものが含まれる場合は名前順でTOP10までを記載

業種	件数	割合(%)	前月比(件数)
製造	142	17.2	+ 1
情報通信	99	12.0	+ 27
建設・建築	74	9.0	- 6
サービス	65	7.9	- 45
卸売・小売	63	7.6	- 17
医療	54	6.5	- 13
(Unknown)	43	5.2	+ 16
金融・保険	42	5.1	+ 17
法律	41	5.0	- 5
運輸	30	3.6	+ 2

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



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

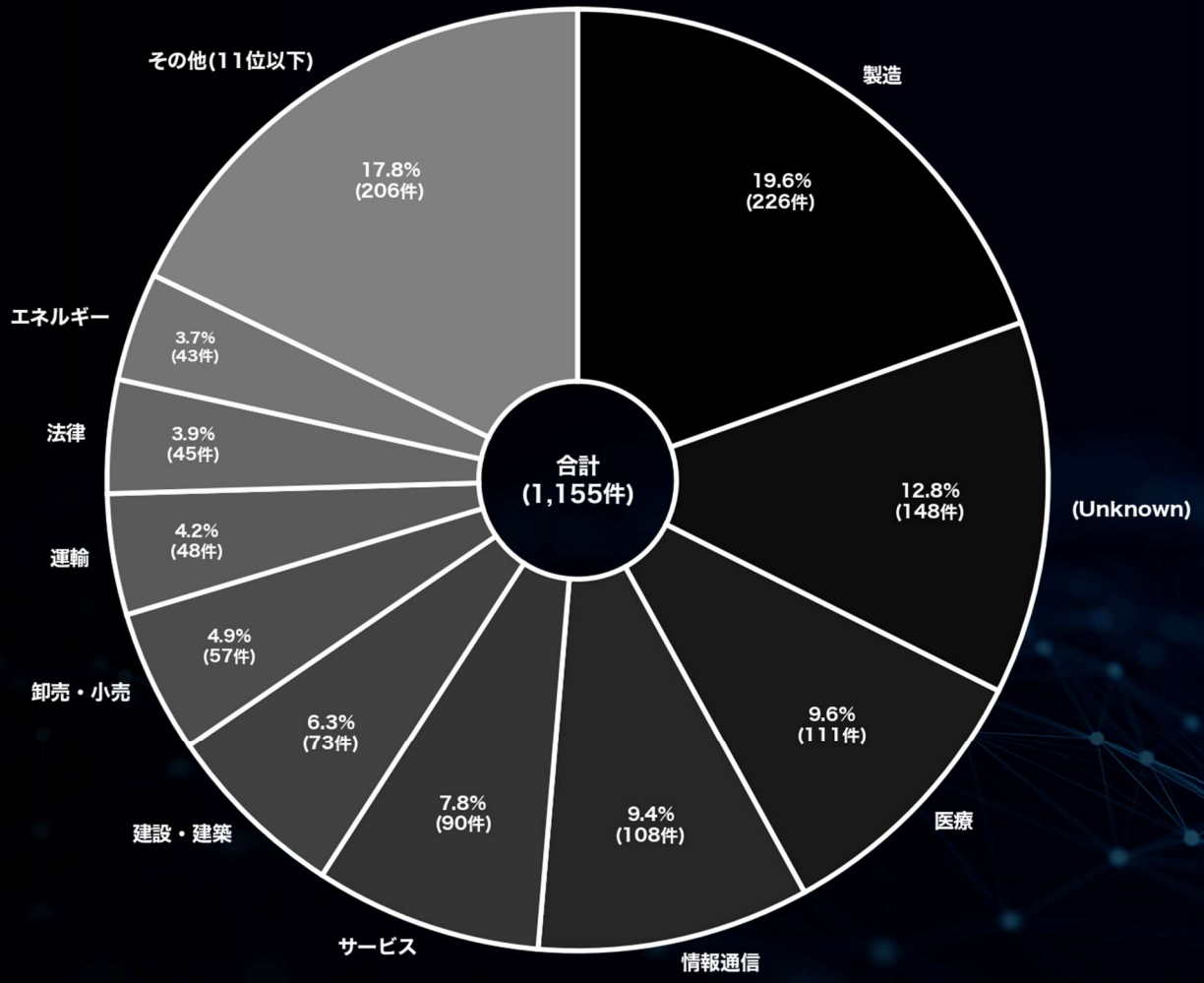
月別内訳 業種 TOP10（全世界）

（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

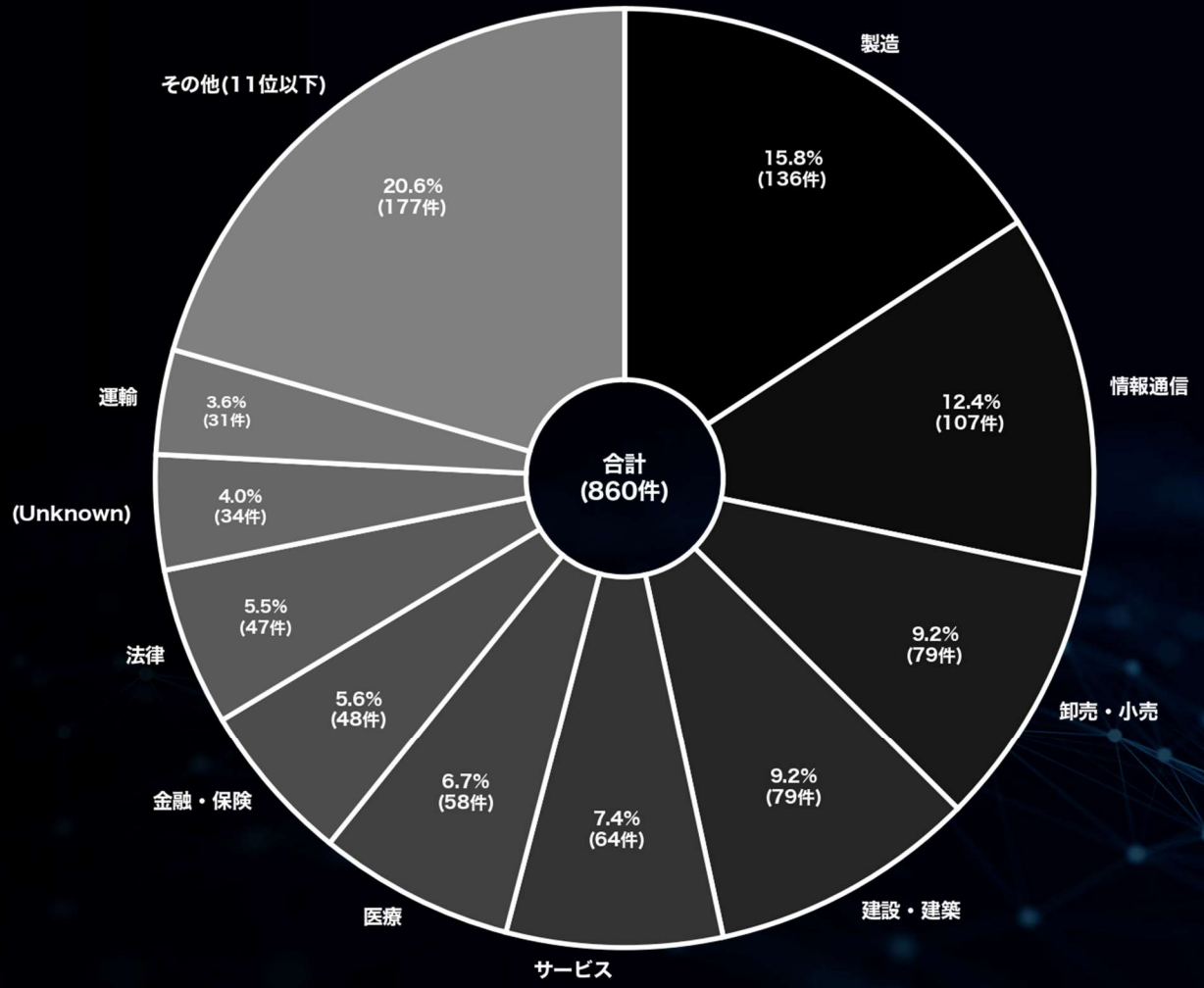
月別内訳 業種 TOP10（全世界）

（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	136	15.8	- 90
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	64	7.4	- 26
医療	58	6.7	- 53
金融・保険	48	5.6	+ 10
法律	47	5.5	+ 2
(Unknown)	34	4.0	- 114
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

被害数の推移に関する統計
（全世界及び国内）

2026

3

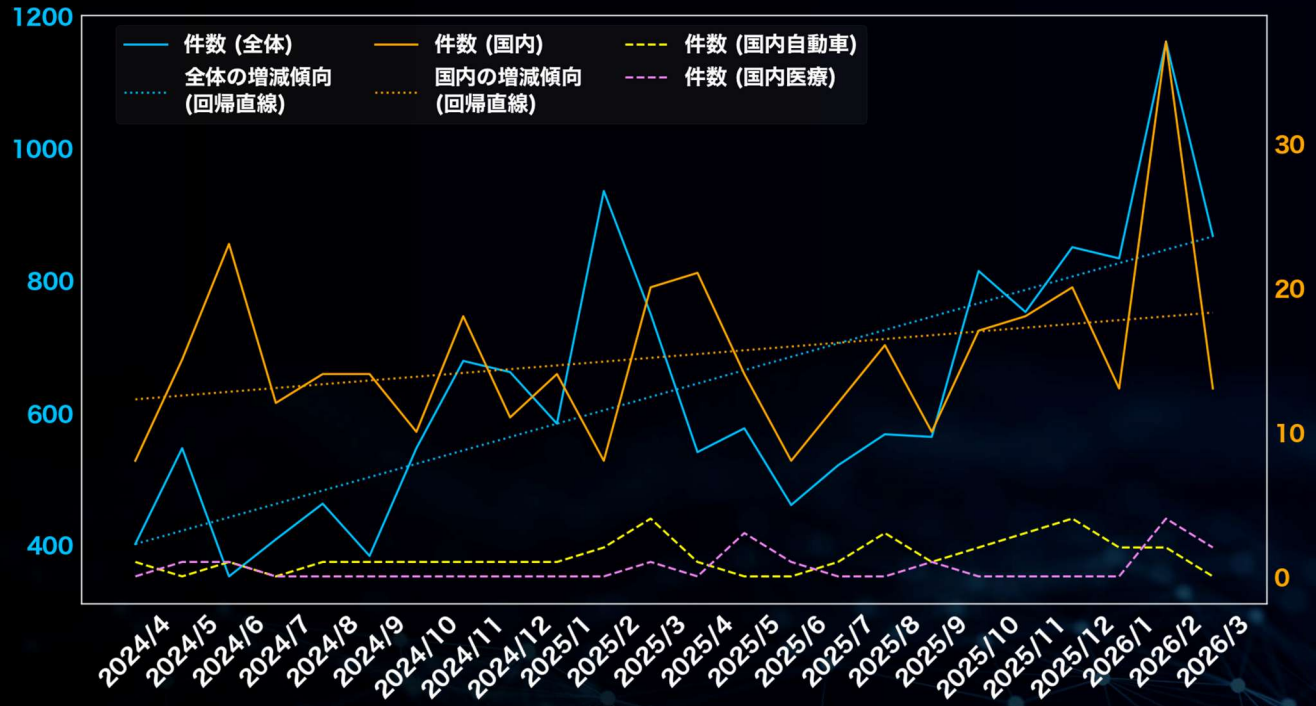
被害数の推移（全世界及び国内）
（過去2年間／2024年4月～2026年3月）

※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）
2024/4	401	8	1	0
2024/5	546	15	0	1
2024/6	352	23	1	1
2024/7	408	12	0	0
2024/8	462	14	1	0
2024/9	383	14	1	0
2024/10	546	10	1	0
2024/11	678	18	1	0
2024/12	661	11	1	0
2025/1	583	14	1	0
2025/2	935	8	2	0
2025/3	749	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	18	3	0
2025/12	850	20	4	0
2026/1	833	13	2	0
2026/2	1161	37	2	4
2026/3	867	13	0	2
合計	15207	366	33	14

▼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

3

資本金別の統計
（国内）

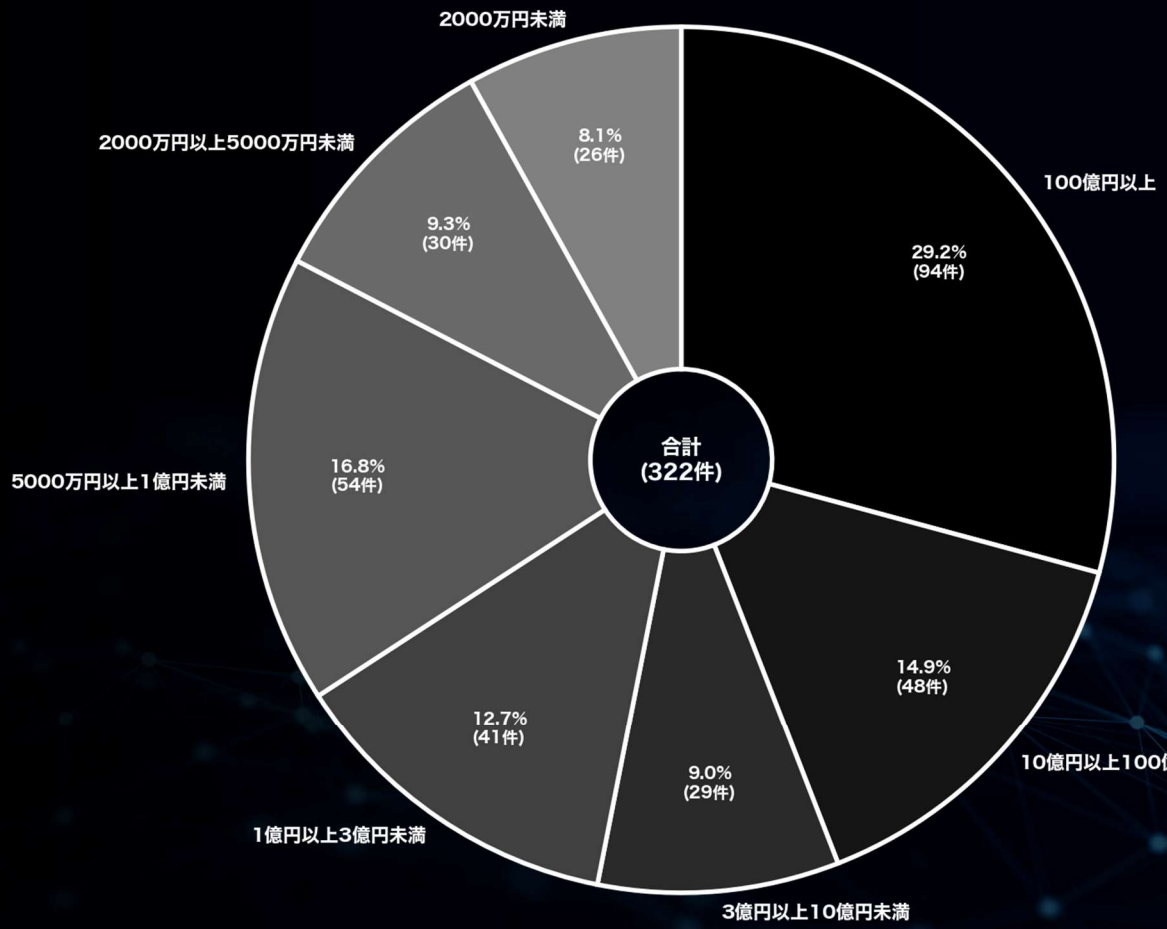
資本金別（国内）
（過去2年間／2024年4月～2026年3月）

※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	29.2
10億円以上100億円未満	48	14.9
3億円以上10億円未満	29	9.0
1億円以上3億円未満	41	12.7
5000万円以上1億円未満	54	16.8
2000万円以上5000万円未満	30	9.3
2000万円未満	26	8.1

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

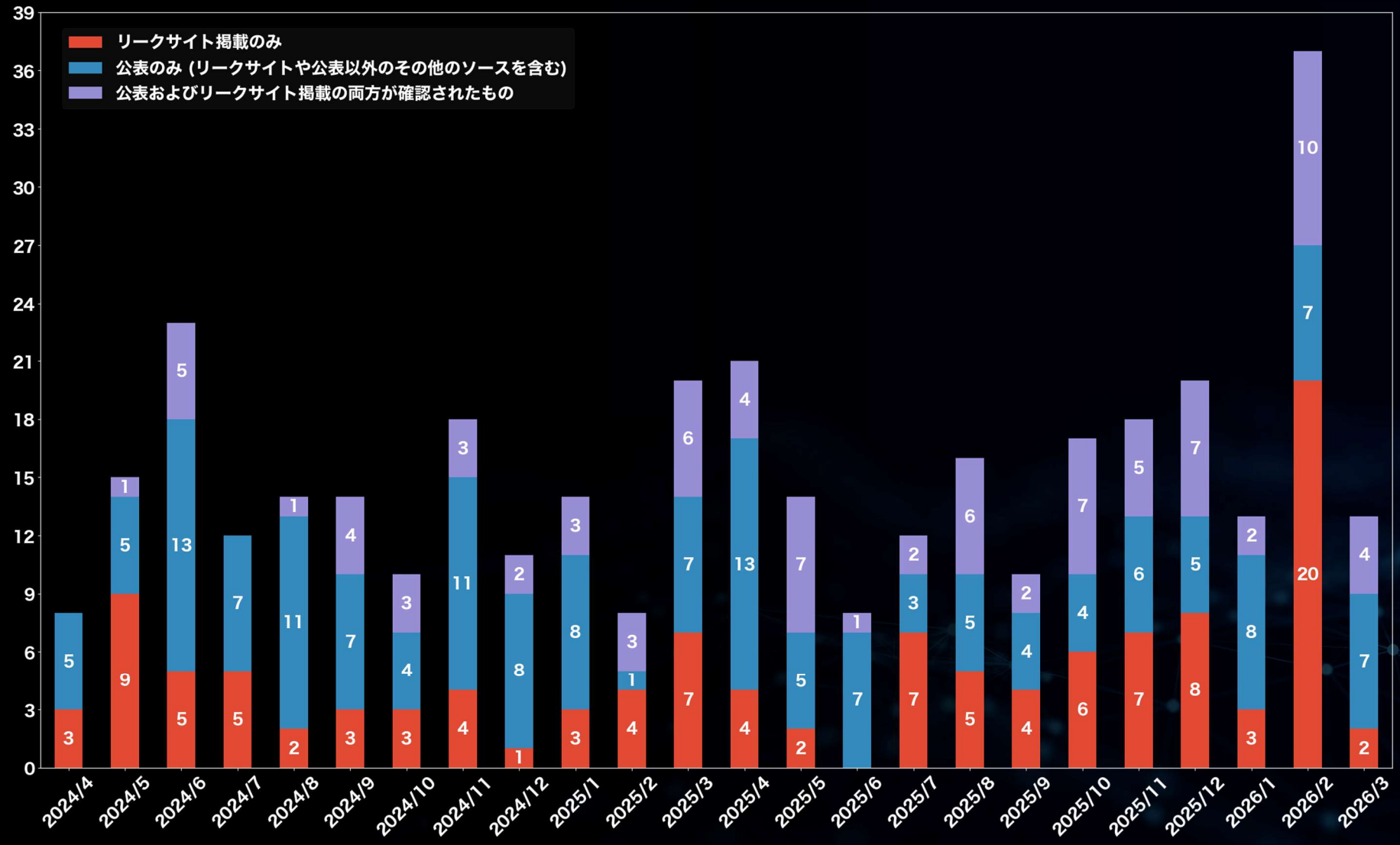
2026

3

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4月～2026年3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

3

公となった国内被害組織概要一覧（国内）

（過去1年間／2025年4月～2026年3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
2025/4	KILLSEC	情報機器メーカー(海外拠点)
2025/4	AKIRA	大手総合印刷・電子材料メーカー(海外拠点)
2025/4	SARCOMA	大手総合化学メーカー(海外拠点)
2025/4	AKIRA	自動化装置メーカ(海外拠点)
2025/4	(Unknown)	総合エンジニアリング企業
2025/4	(Unknown)	トラック・バス等販売
2025/4	Night Spire	センサ・電子部品メーカー
2025/4	(Unknown)	総合建設業
2025/4	(Unknown)	総合物流事業者
2025/4	Qilin (Agenda)	精密機械製造(海外拠点)
2025/4	(Unknown)	エネルギーコンサルティング
2025/4	(Unknown)	ガソリンスタンド運営
2025/4	(Unknown)	私立大学
2025/4	(Unknown)	総合建設業
2025/4	(Unknown)	総合建設業
2025/4	(Unknown)	コンクリートの劣化調査
2025/4	(Unknown)	総合物流事業者
2025/4	Gunra	不動産会社
2025/4	(Unknown)	情報通信機器製造業(海外拠点)
2025/4	(Unknown)	ワイヤーハーネス製造
2025/4	Termite	光応用製品メーカー(海外拠点)
2025/5	LYNX	食品物流業事業者
2025/5	Gunra	総合包装メーカー
2025/5	Gunra	船舶内装・総合建設業
2025/5	SAFEPAY	経営コンサルティング
2025/5	(Unknown)	学校法人
2025/5	Qilin (Agenda)	医薬品開発支援(海外拠点)
2025/5	(Unknown)	医療機器・介護用品商社
2025/5	(Unknown)	医療機器・消耗品商社
2025/5	BlackLock	大手映画制作・配給業
2025/5	DEVMAN	大手映画制作・配給業
2025/5	(Unknown)	化学メーカー
2025/5	(Unknown)	特殊鋼・合金メーカー
2025/5	Space Bears	ゴム製品メーカー(海外拠点)

被害月	攻撃グループ	業種概要
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

被害月	攻撃グループ	業種概要
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

（※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4月～2026年3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
2025/11	Warlock	サスペンションメーカー
2025/11	Qilin (Agenda)	弁理士法人
2025/11	(Unknown)	システムインテグレーター
2025/11	Qilin (Agenda)	通信機器メーカー
2025/11	(Unknown)	雑貨・アパレル小売
2025/11	CRYPTO24	電子部品メーカー
2025/11	CL0P (CLOP)	ラベル印刷機器メーカー
2025/11	INC Ransom	自動車部品メーカー(海外拠点)
2025/11	(Unknown)	教育委員会
2025/11	(Unknown)	私立学校
2025/11	CL0P (CLOP)	大手精密機器メーカー(海外拠点)
2025/11	CL0P (CLOP)	大手自動車メーカー
2025/11	CL0P (CLOP)	大手総合化学メーカー
2025/11	Sinobi	警報装置メーカー
2025/11	Qilin (Agenda)	大手建設会社(海外拠点)
2025/11	(Unknown)	精密部品製造
2025/12	(Unknown)	エレクトロニクス専門商社(海外拠点)
2025/12	(Unknown)	教育系ITサービス提供
2025/12	AKIRA	食用油脂メーカー(海外拠点)
2025/12	Payouts King	プラスチック精密工業部品メーカー(海外拠点)
2025/12	COINBASE CARTEL	大手半導体メーカー
2025/12	INC Ransom	ワイヤーハーネスメーカー
2025/12	LYNX	総合デベロッパー
2025/12	Qilin (Agenda)	空調・衛生設備工事(海外拠点)
2025/12	(Unknown)	総合色材・機能性化学メーカー(海外拠点)
2025/12	root	金融商品取引所
2025/12	Qilin (Agenda)	大手テクノロジー企業(海外拠点)
2025/12	Rhysida	私立学校
2025/12	Qilin (Agenda)	電気機械部品メーカー(海外拠点)
2025/12	DragonForce	自動車部品メーカー(海外拠点)
2025/12	(Unknown)	公立大学
2025/12	(Unknown)	私立大学
2025/12	LYNX	映像制作

被害月	攻撃グループ	業種概要
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	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

被害月	攻撃グループ	業種概要
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
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)	美容室向け化粧品メーカー
2026/3	ALP-001	国立研究開発法人

（※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4月～2026年3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	88	44.2
海外拠点	44	22.1
不明	67	33.7

▼ランサムウェア攻撃を受けた日本関連組織の拠点別割合

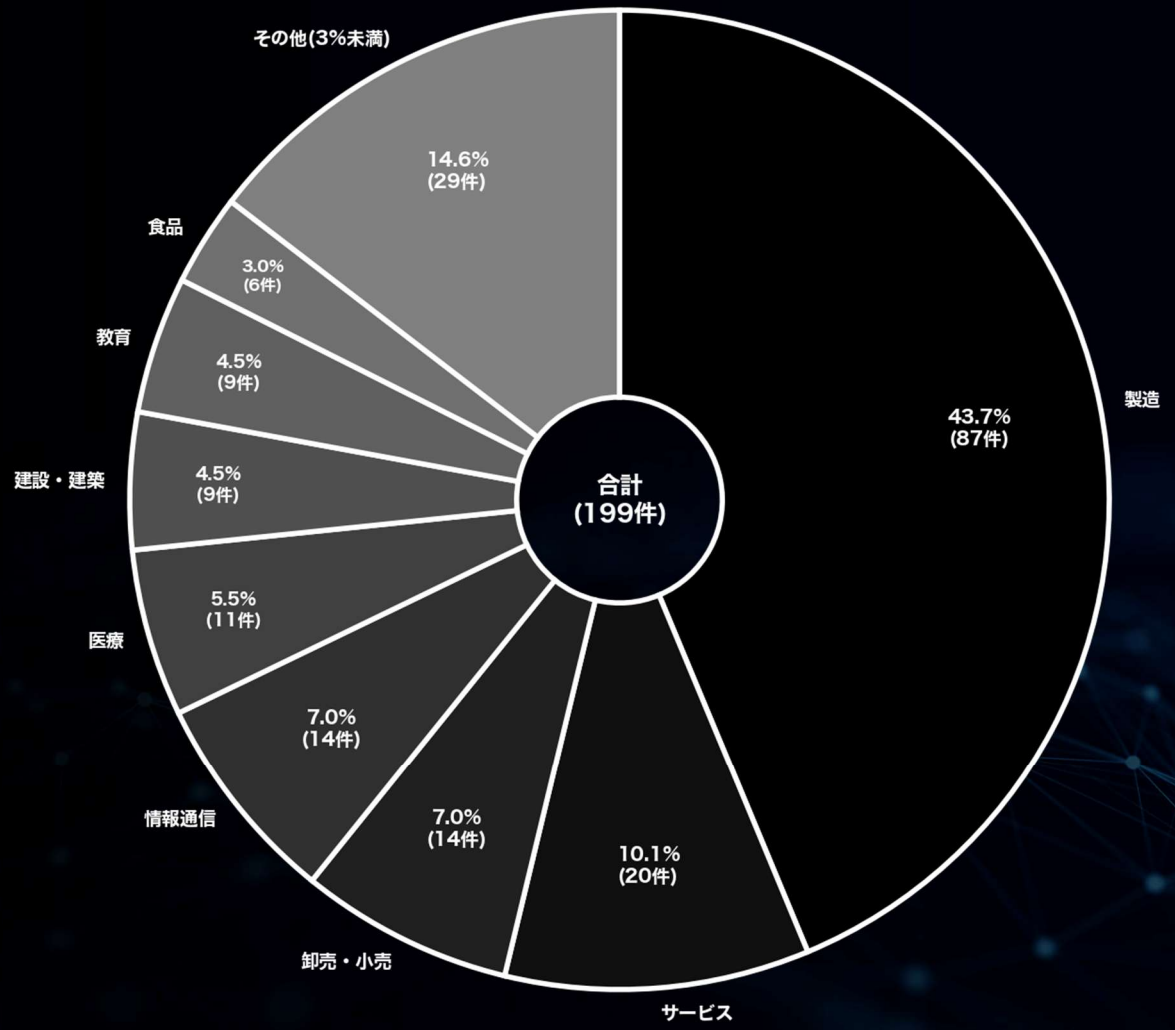
（※本ページの表／グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している）

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

公となった国内被害組織における業種割合（国内）
（過去1年間／2025年4月～2026年3月）

業種	件数	割合(%)
製造	87	43.7
サービス	20	10.1
卸売・小売	14	7.0
情報通信	14	7.0
医療	11	5.5
建設・建築	9	4.5
教育	9	4.5
食品	6	3.0
その他(3%未満)	29	14.6

▼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

3

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

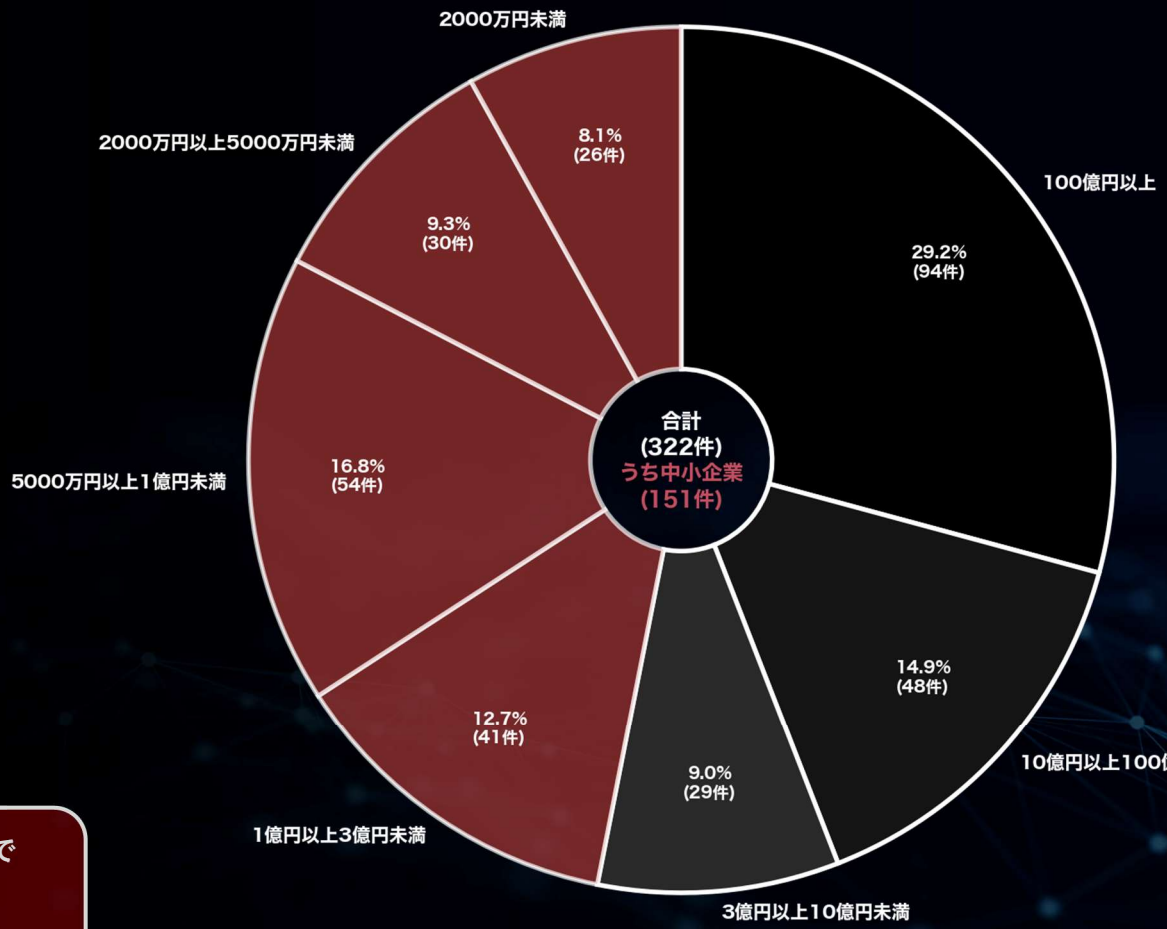
資本金別（国内-中小企業）
（過去2年間／2024年4月～2026年3月）

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	29.2
10億円以上100億円未満	48	14.9
3億円以上10億円未満	29	9.0
1億円以上3億円未満	41	12.7
5000万円以上1億円未満	54	16.8
2000万円以上5000万円未満	30	9.3
2000万円未満	26	8.1

▼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151件にのぼり、全体の46.9%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）

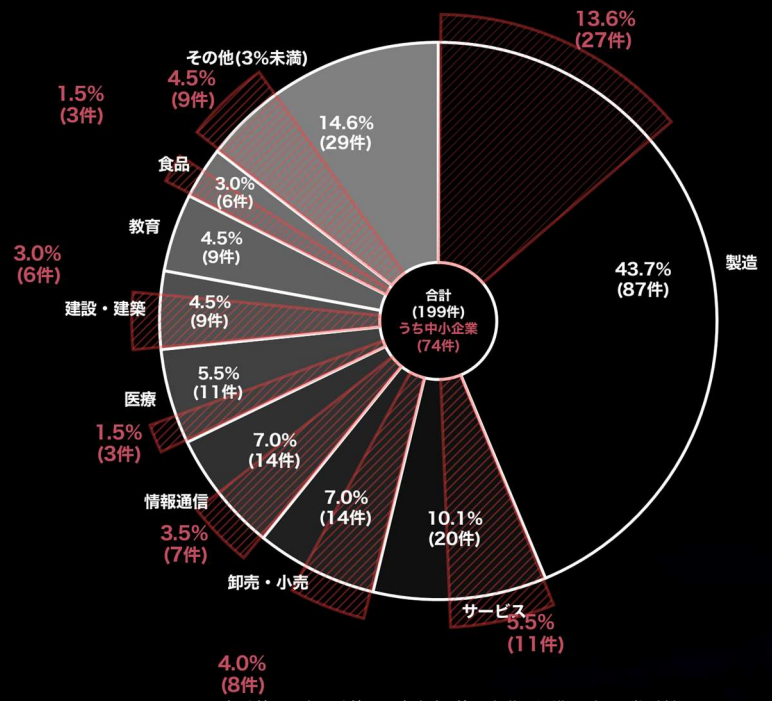
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

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4月～2026年3月）

赤色は中小企業を示す

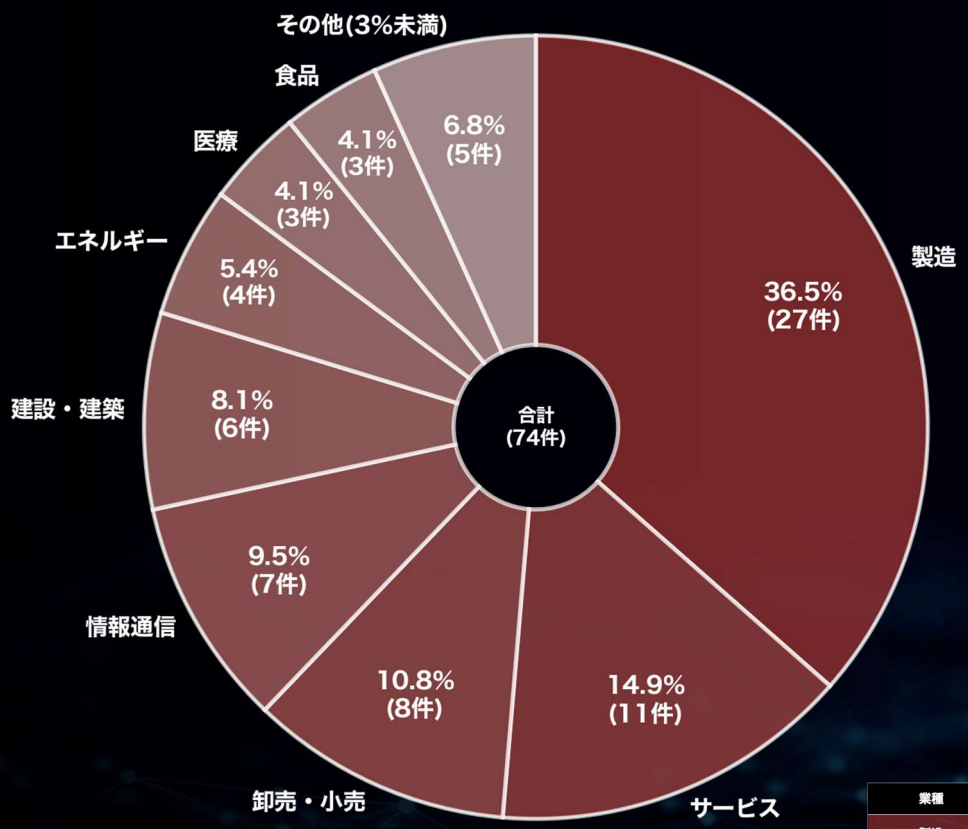
▼全体割合



※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	87 (27)	43.7 (13.6)
サービス	20 (11)	10.1 (5.5)
卸売・小売	14 (8)	7.0 (4.0)
情報通信	14 (7)	7.0 (3.5)
医療	11 (3)	5.5 (1.5)
建設・建築	9 (6)	4.5 (3.0)
教育	9	4.5
食品	6 (3)	3.0 (1.5)
その他(3%未満)	29 (9)	14.6 (4.5)

▼中小企業のみの割合



業種	件数	割合(%)
製造	27	36.5
サービス	11	14.9
卸売・小売	8	10.8
情報通信	7	9.5
建設・建築	6	8.1
エネルギー	4	5.4
医療	3	4.1
食品	3	4.1
その他(3%未満)	5	6.8

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

※医療や教育、行政機関など資本金が不明な一部の組織については集計から除外

（※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）

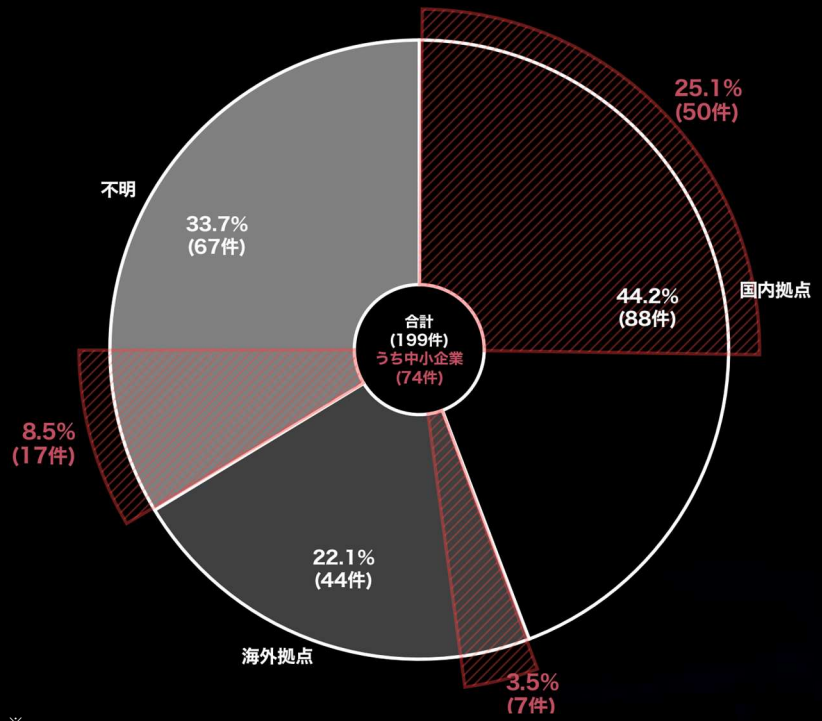
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

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）

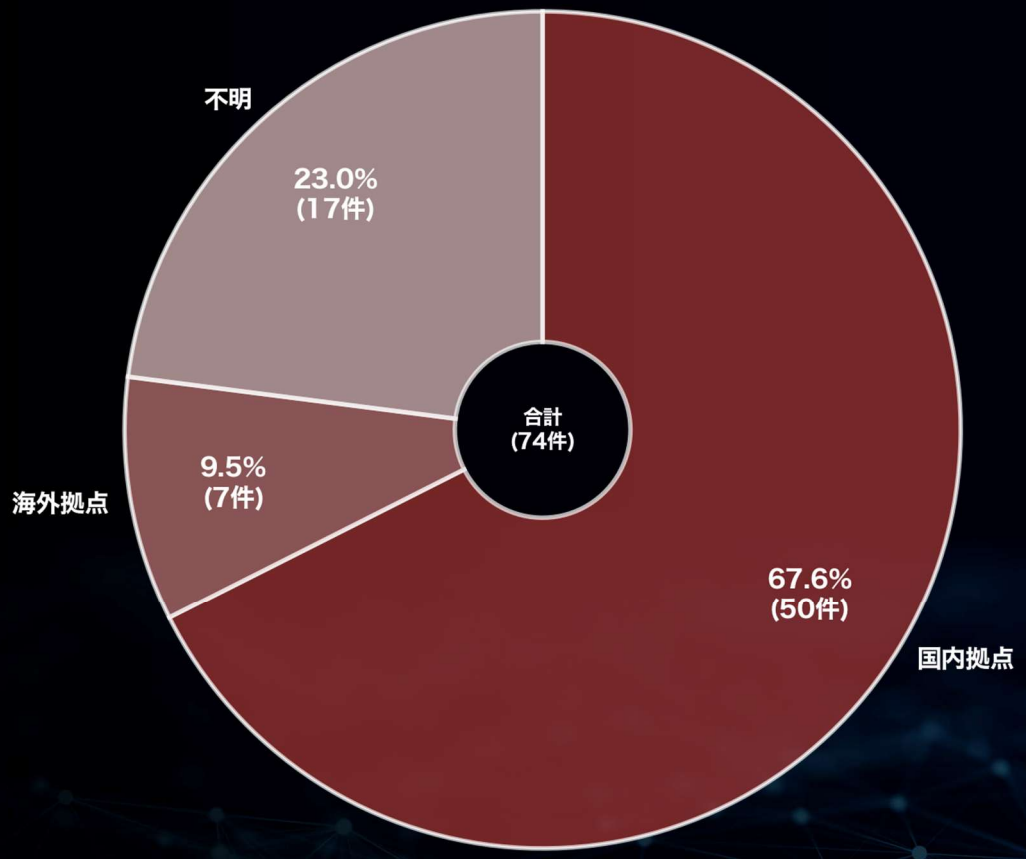
（過去1年間／2025年4月～2026年3月）

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	88 (50)	44.2 (25.1)
海外拠点	44 (7)	22.1 (3.5)
不明	67 (17)	33.7 (8.5)
合計	199 (74)	100 (37.1)

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

※医療や教育、行政機関など資本金が不明な一部の組織については集計から除外

拠点	件数 (中小企業)	割合(%)
国内拠点	50	67.6
海外拠点	7	9.5
不明	17	23.0

（※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4月～2026年3月）

赤色は中小企業を示す

被害月	攻撃グループ	業種概要
2025/4	KILLSEC	情報機器メーカー(海外拠点)
2025/4	AKIRA	大手総合印刷・電子材料メーカー(海外拠点)
2025/4	SARCOMA	大手総合化学メーカー(海外拠点)
2025/4	AKIRA	自動化装置メーカ(海外拠点)
2025/4	(Unknown)	総合エンジニアリング企業
2025/4	(Unknown)	トラック・バス等販売
2025/4	Night Spire	センサ・電子部品メーカー
2025/4	(Unknown)	総合建設業
2025/4	(Unknown)	総合物流事業者
2025/4	Qilin (Agenda)	精密機械製造(海外拠点)
2025/4	(Unknown)	エネルギーコンサルティング
2025/4	(Unknown)	ガソリンスタンド運営
2025/4	(Unknown)	私立大学
2025/4	(Unknown)	総合建設業
2025/4	(Unknown)	総合建設業
2025/4	(Unknown)	コンクリートの劣化調査
2025/4	(Unknown)	総合物流事業者
2025/4	Gunra	不動産会社
2025/4	(Unknown)	情報通信機器製造業(海外拠点)
2025/4	(Unknown)	ワイヤーハーネス製造
2025/4	Termite	光応用製品メーカー(海外拠点)
2025/5	LYNX	食品物流業事業者
2025/5	Gunra	総合包装メーカー
2025/5	Gunra	船舶内装・総合建設業
2025/5	SAFEPAY	経営コンサルティング
2025/5	(Unknown)	学校法人
2025/5	Qilin (Agenda)	医薬品開発支援(海外拠点)
2025/5	(Unknown)	医療機器・介護用品商社
2025/5	(Unknown)	医療機器・消耗品商社
2025/5	BlackLock	大手映画制作・配給業
2025/5	DEVMAN	大手映画制作・配給業
2025/5	(Unknown)	化学メーカー
2025/5	(Unknown)	特殊鋼・合金メーカー
2025/5	Space Bears	ゴム製品メーカー(海外拠点)

被害月	攻撃グループ	業種概要
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

被害月	攻撃グループ	業種概要
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

※（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4月～2026年3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
2025/11	Warlock	サスペンションメーカー
2025/11	Qilin (Agenda)	弁理士法人
2025/11	(Unknown)	システムインテグレーター
2025/11	Qilin (Agenda)	通信機器メーカー
2025/11	(Unknown)	雑貨・アパレル小売
2025/11	CRYPTO24	電子部品メーカー
2025/11	CL0P (CLOP)	ラベル印刷機器メーカー
2025/11	INC Ransom	自動車部品メーカー(海外拠点)
2025/11	(Unknown)	教育委員会
2025/11	(Unknown)	私立学校
2025/11	CL0P (CLOP)	大手精密機器メーカー(海外拠点)
2025/11	CL0P (CLOP)	大手自動車メーカー
2025/11	CL0P (CLOP)	大手総合化学メーカー
2025/11	Sinobi	警報装置メーカー
2025/11	Qilin (Agenda)	大手建設会社(海外拠点)
2025/11	(Unknown)	精密部品製造
2025/12	(Unknown)	エレクトロニクス専門商社(海外拠点)
2025/12	(Unknown)	教育系ITサービス提供
2025/12	AKIRA	食用油脂メーカー(海外拠点)
2025/12	Payouts King	プラスチック精密工業部品メーカー(海外拠点)
2025/12	COINBASE CARTEL	大手半導体メーカー
2025/12	INC Ransom	ワイヤーハーネスメーカー
2025/12	LYNX	総合デベロッパー
2025/12	Qilin (Agenda)	空調・衛生設備工事(海外拠点)
2025/12	(Unknown)	総合色材・機能性化学メーカー(海外拠点)
2025/12	root	金融商品取引所
2025/12	Qilin (Agenda)	大手テクノロジー企業(海外拠点)
2025/12	Rhysida	私立学校
2025/12	Qilin (Agenda)	電気機械部品メーカー(海外拠点)
2025/12	DragonForce	自動車部品メーカー(海外拠点)
2025/12	(Unknown)	公立大学
2025/12	(Unknown)	私立大学
2025/12	LYNX	映像制作

被害月	攻撃グループ	業種概要
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	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

被害月	攻撃グループ	業種概要
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
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)	美容室向け化粧品メーカー
2026/3	ALP-001	国立研究開発法人

※（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

多重被害に関する分析

2026

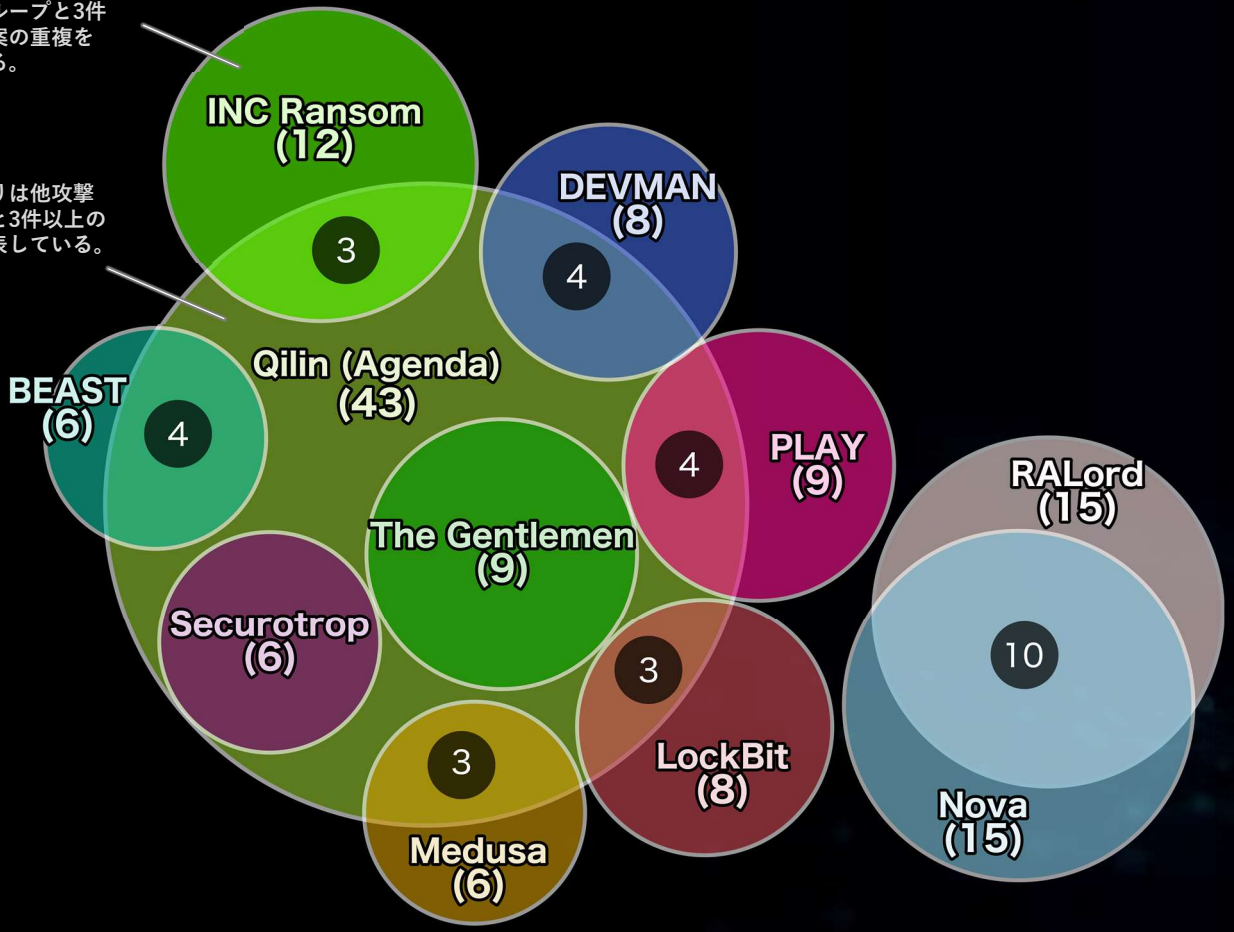
3

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4月～2026年3月）　（累計135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。

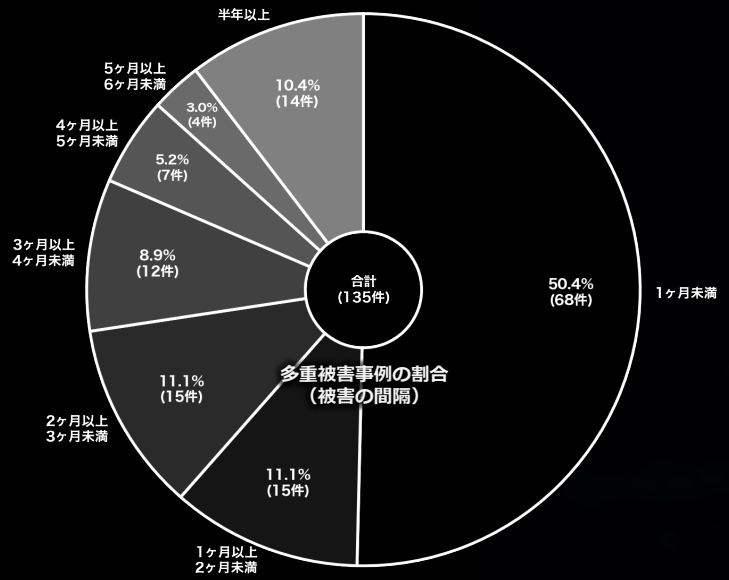
多重被害に遭った被害組織の傾向と分析（全世界）

（過去1年間／2025年4月～2026年3月）

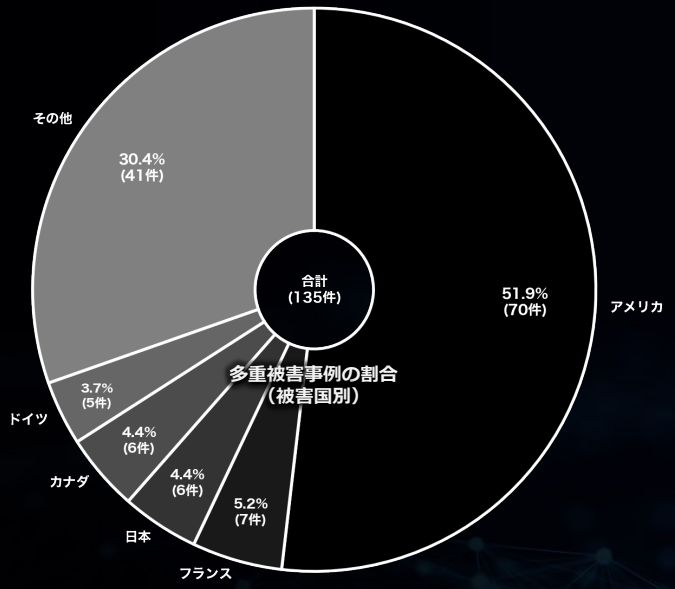
※多重被害：一度ランサムウェア攻撃の被害を受けた組織が異なる時期に異なる攻撃グループのリークサイトに再び掲載されるケース

▼被害の間隔

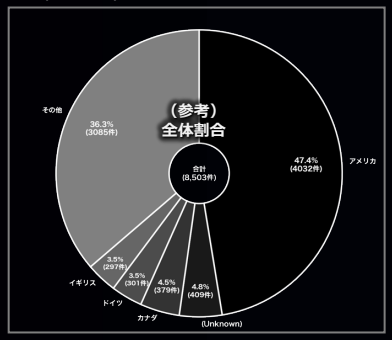
（一度目の被害から二度目の被害までの間隔）



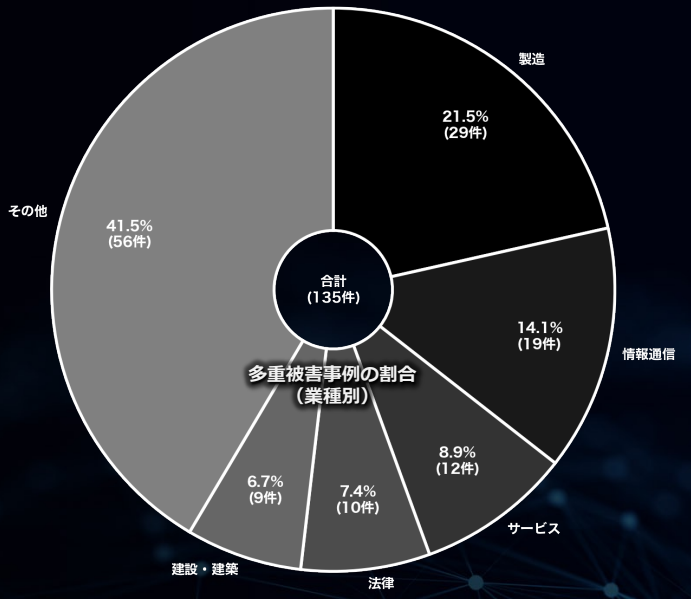
▼被害国別



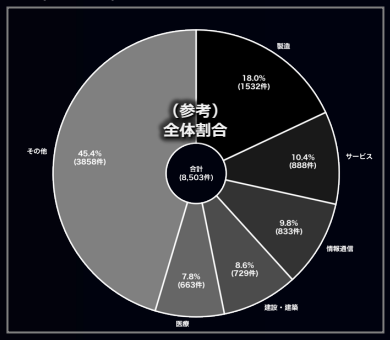
（参考比較）同期間の全データにおける割合



▼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：135件（全体8503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60%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

3

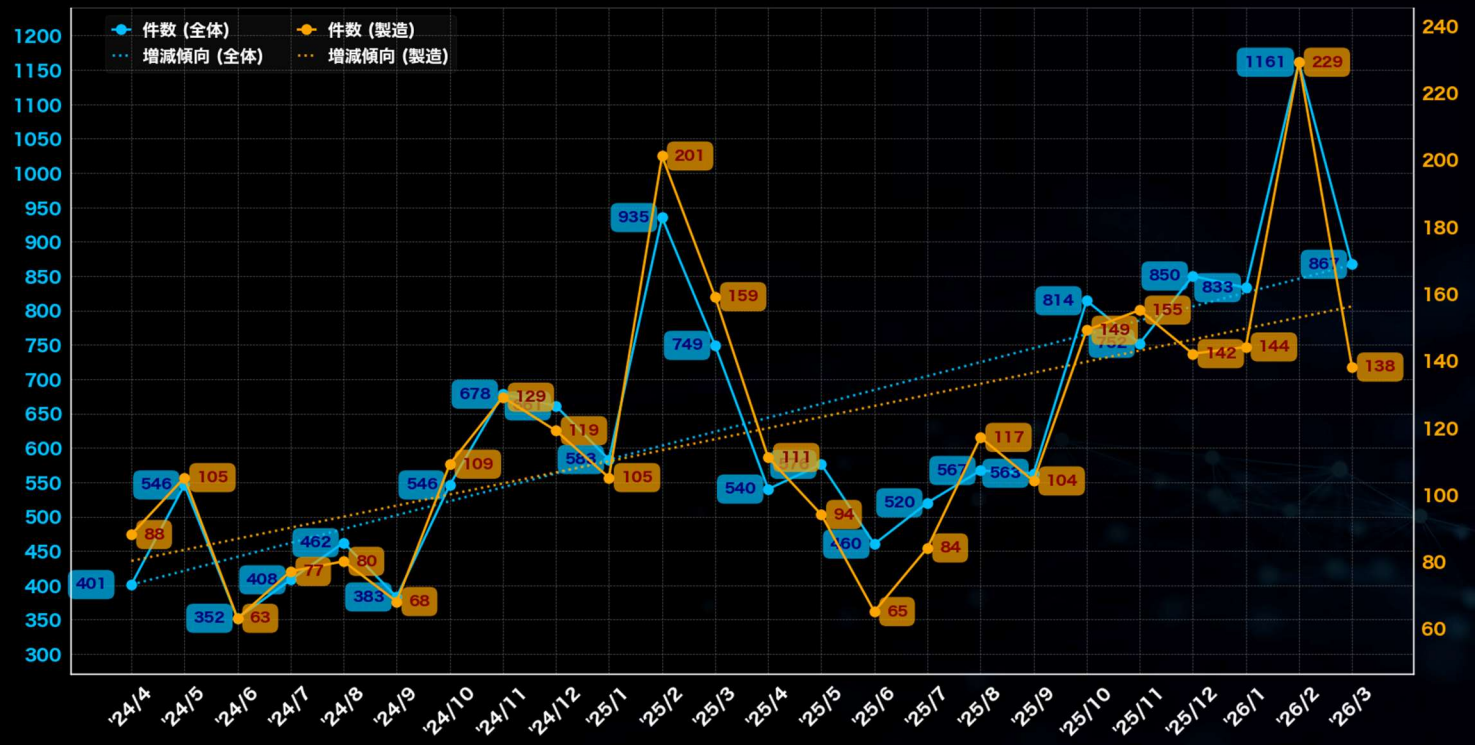
業種に関する分析

（過去2年間のリークサイト掲載上位10業種）

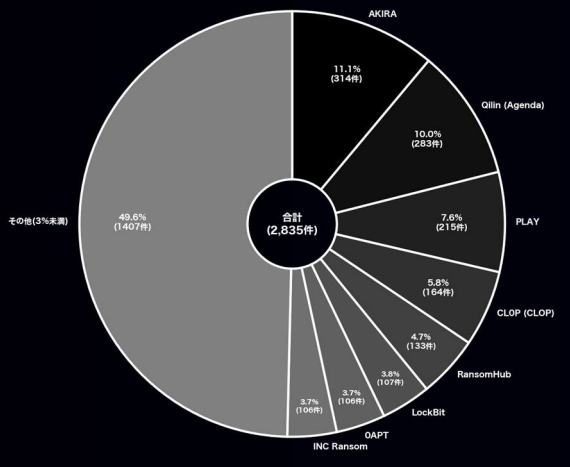
業種に関する分析（全世界）
（過去2年間／2024年4月～2026年3月）

製造

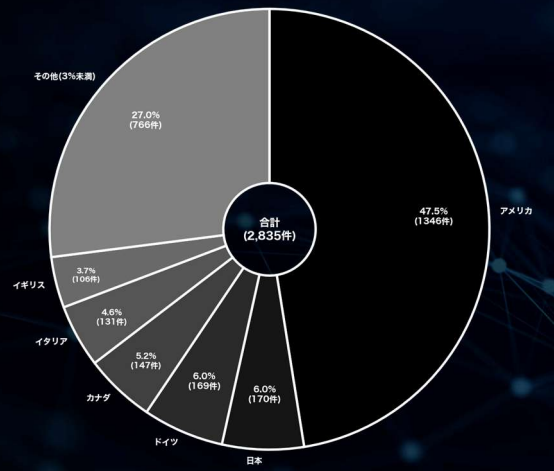
「製造」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年2月で、229件の掲載があった。一方、最も少なかった月は2024年6月で、63件であった。被害組織の所在国の割合では、アメリカが約48%と最も多く、次いで日本とドイツがそれぞれ約6%である。攻撃グループについては、少なくとも137のグループが関与しており、特に「AKIRA」が314件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「PLAY」がそれぞれ283件と215件の掲載を行っている。製造関連の件数は全体件数に対して高い割合で推移しており、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



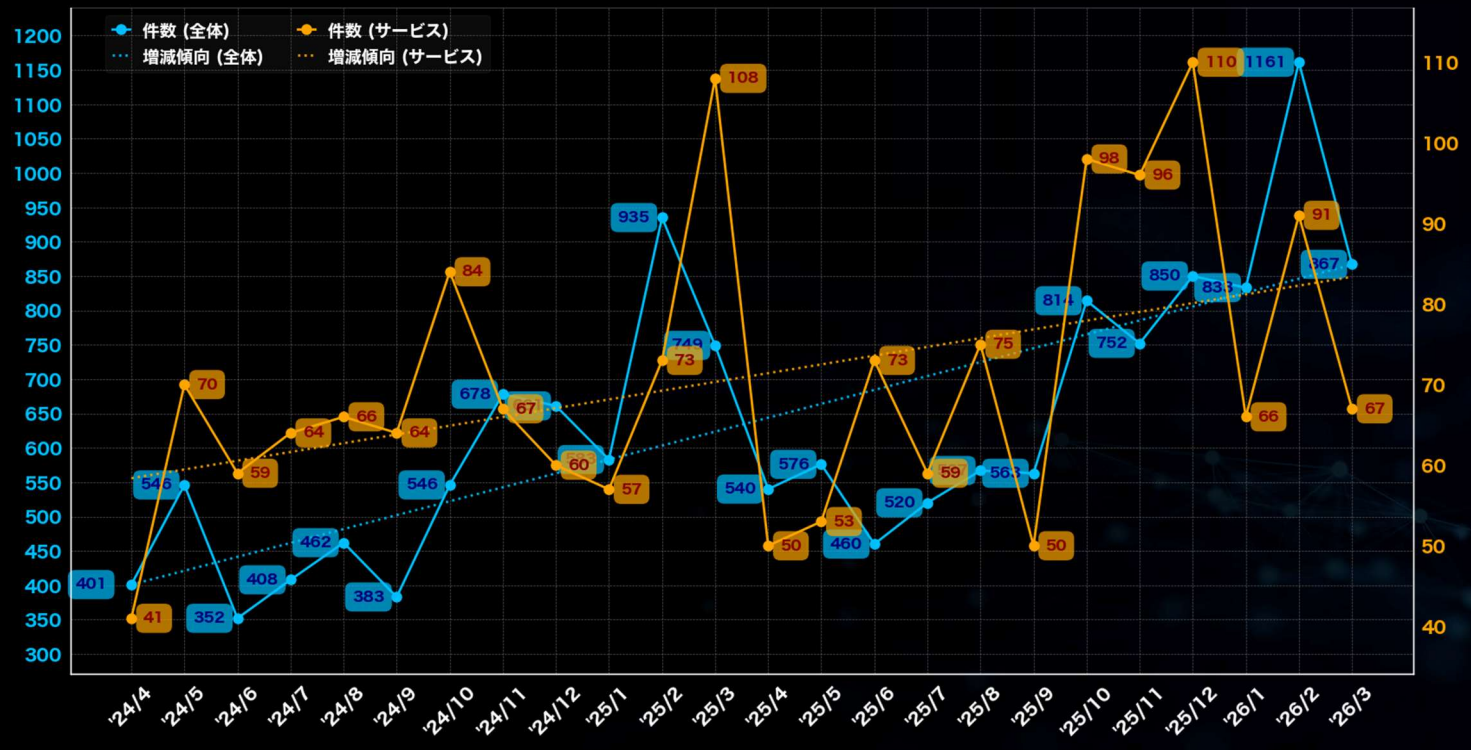
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて
国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

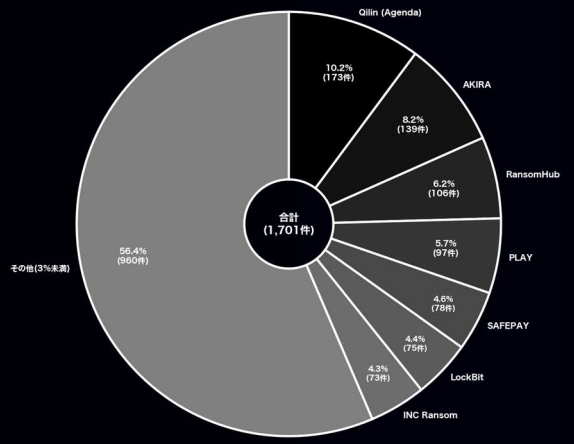
業種に関する分析（全世界）
（過去2年間／2024年4月～2026年3月）

サービス

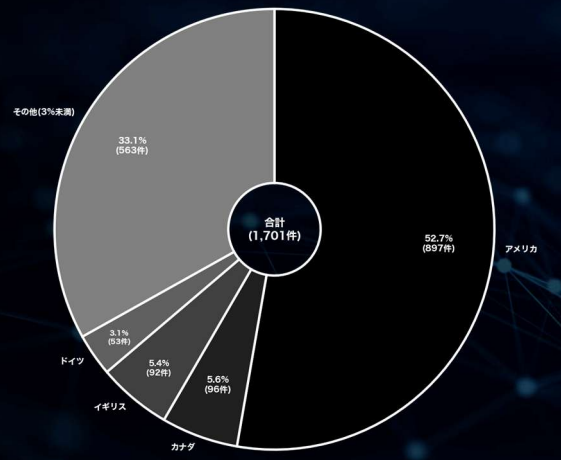
「サービス」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年12月で、110件の掲載があった。一方、最も少なかった月は2024年4月で、41件であった。被害組織の所在国の割合では、アメリカが約53%と最も多く、次いでカナダとイギリスがそれぞれ約6%と約5%である。攻撃グループについては、少なくとも129のグループが関与しており、特に「Qilin (Agenda)」が173件のリークサイト掲載を実施している。次いで「AKIRA」と「RansomHub」がそれぞれ139件と106件の掲載を行っている。サービス関連の件数は製造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



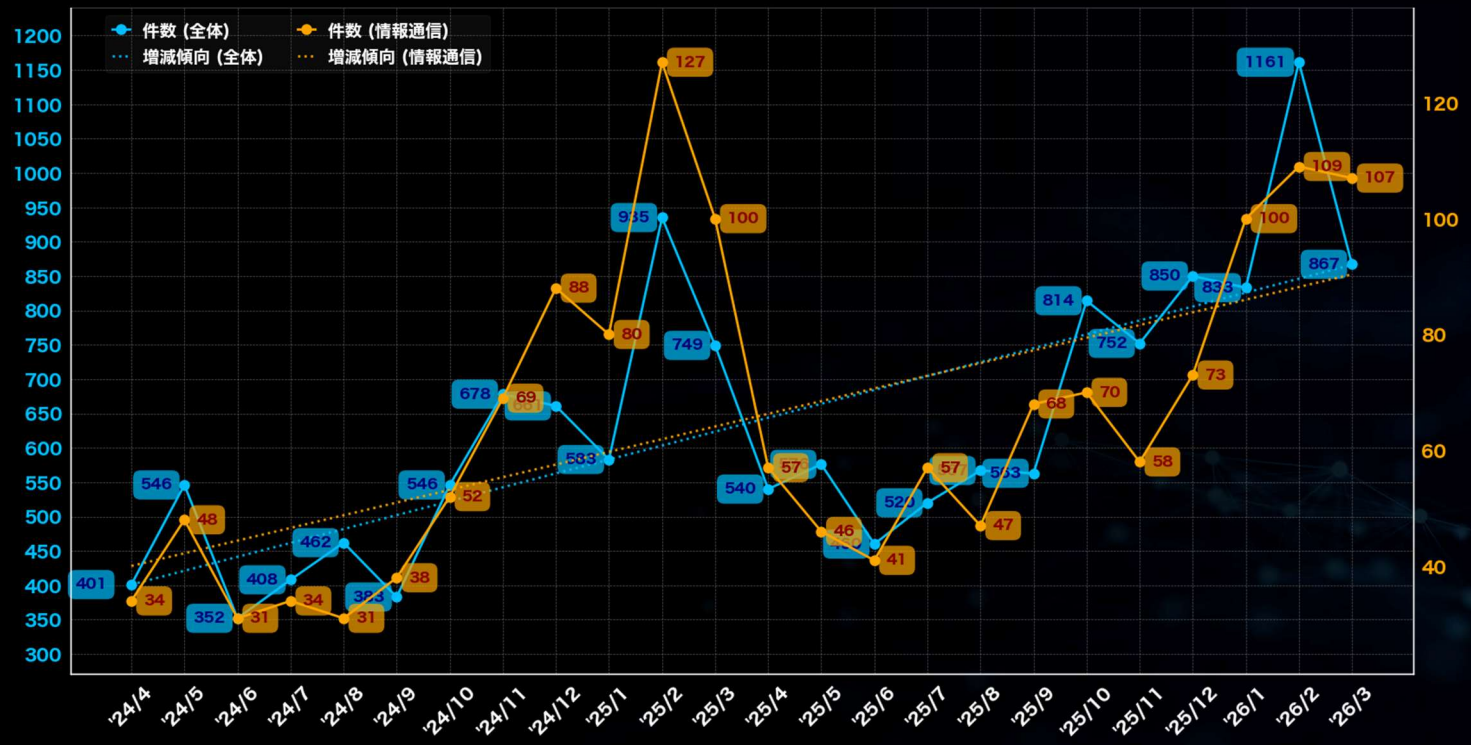
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

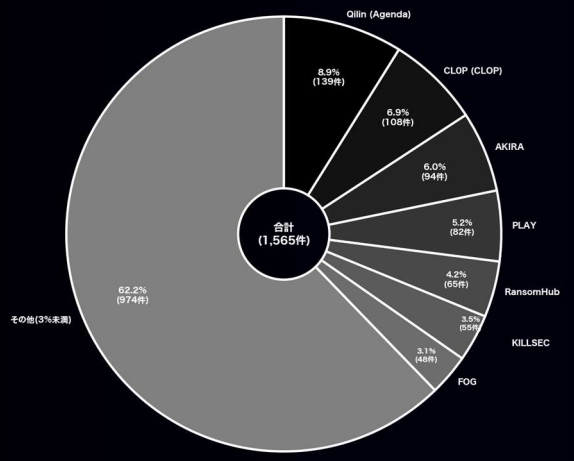
業種に関する分析（全世界）
（過去2年間／2024年4月～2026年3月）

情報通信

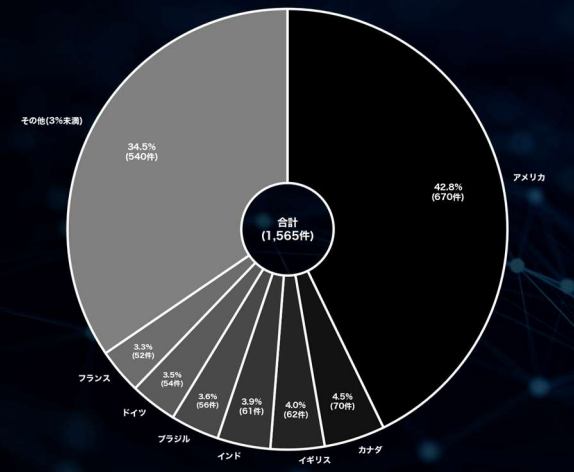
「情報通信」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、127件の掲載があった。一方、最も少なかった月は2024年6月および8月で、31件であった。被害組織の所在国の割合では、アメリカが約43%と最も多く、次いでカナダとイギリスがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも138のグループが関与しており、特に「Qilin（Agenda）」が139件のリークサイト掲載を実施している。次いで「CL0P（CLOP）」と「AKIRA」がそれぞれ108件と94件の掲載を行っている。過去2年間におけるリークサイト掲載件数は明確な増加傾向にある。



▼攻撃グループ別



▼国別



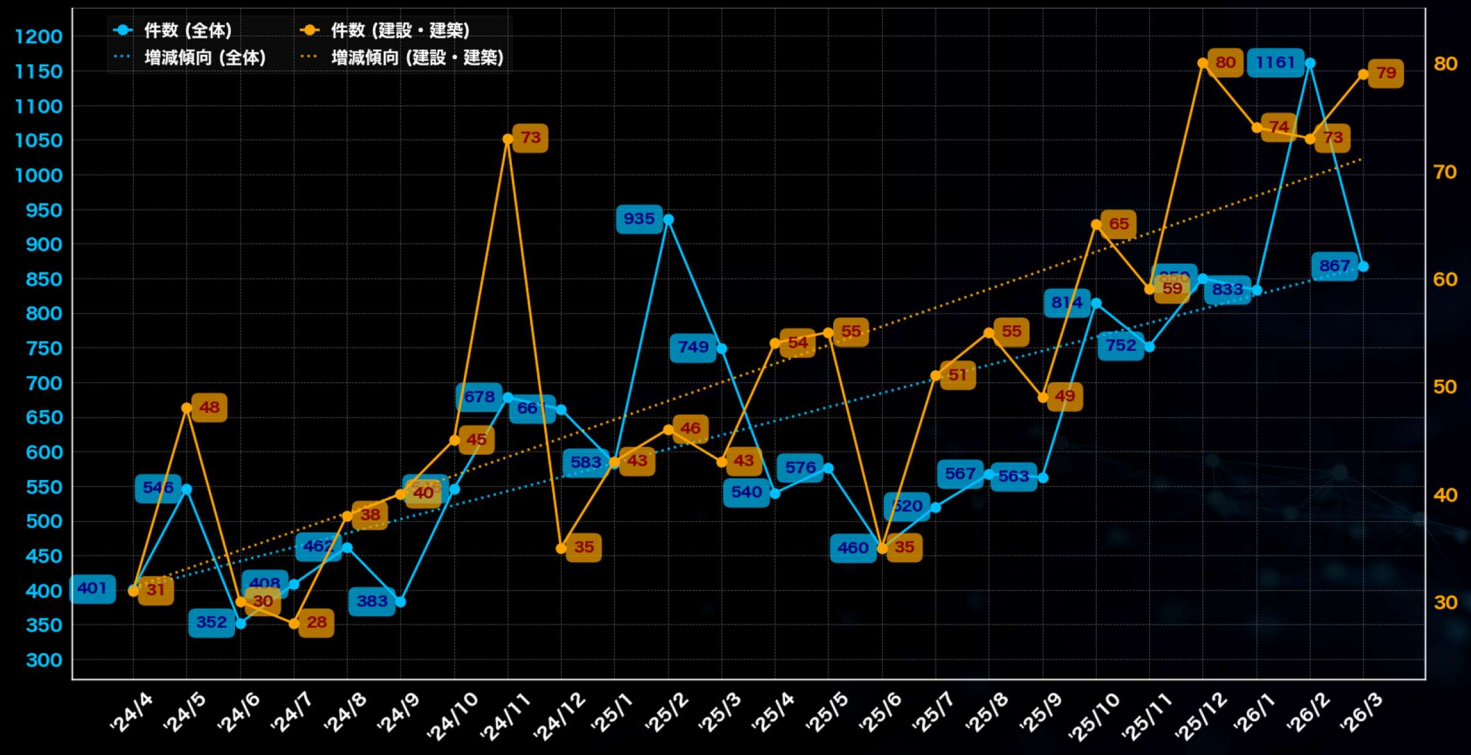
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

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

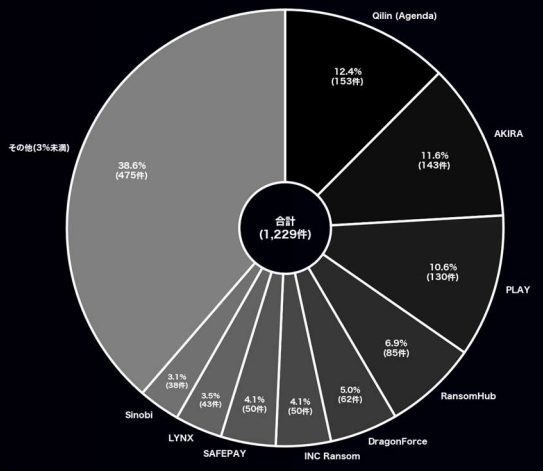
業種に関する分析（全世界）
（過去2年間／2024年4月～2026年3月）

建設・建築

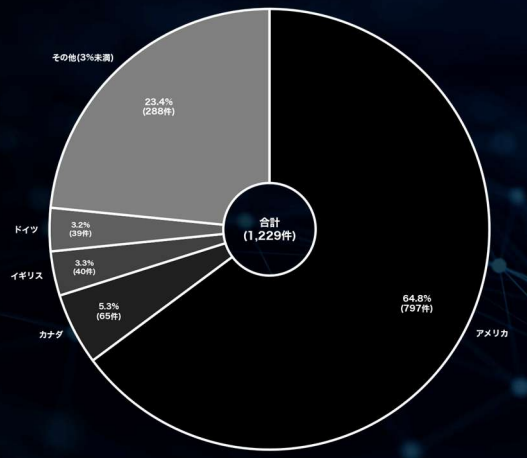
「建設・建築」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年12月で、80件の掲載があった。一方、最も少なかった月は2024年7月で、28件であった。被害組織の所在国の割合では、アメリカが約65%と最も多く、次いでカナダとイギリスがそれぞれ約5%と約3%である。攻撃グループについては、少なくとも101のグループが関与しており、特に「Qilin (Agenda)」が153件のリークサイト掲載を実施している。次いで「AKIRA」と「PLAY」がそれぞれ143件と130件の掲載を行っている。製造関連などと比べると件数は少ないものの、明確な増加傾向にある。



▼攻撃グループ別



▼国別



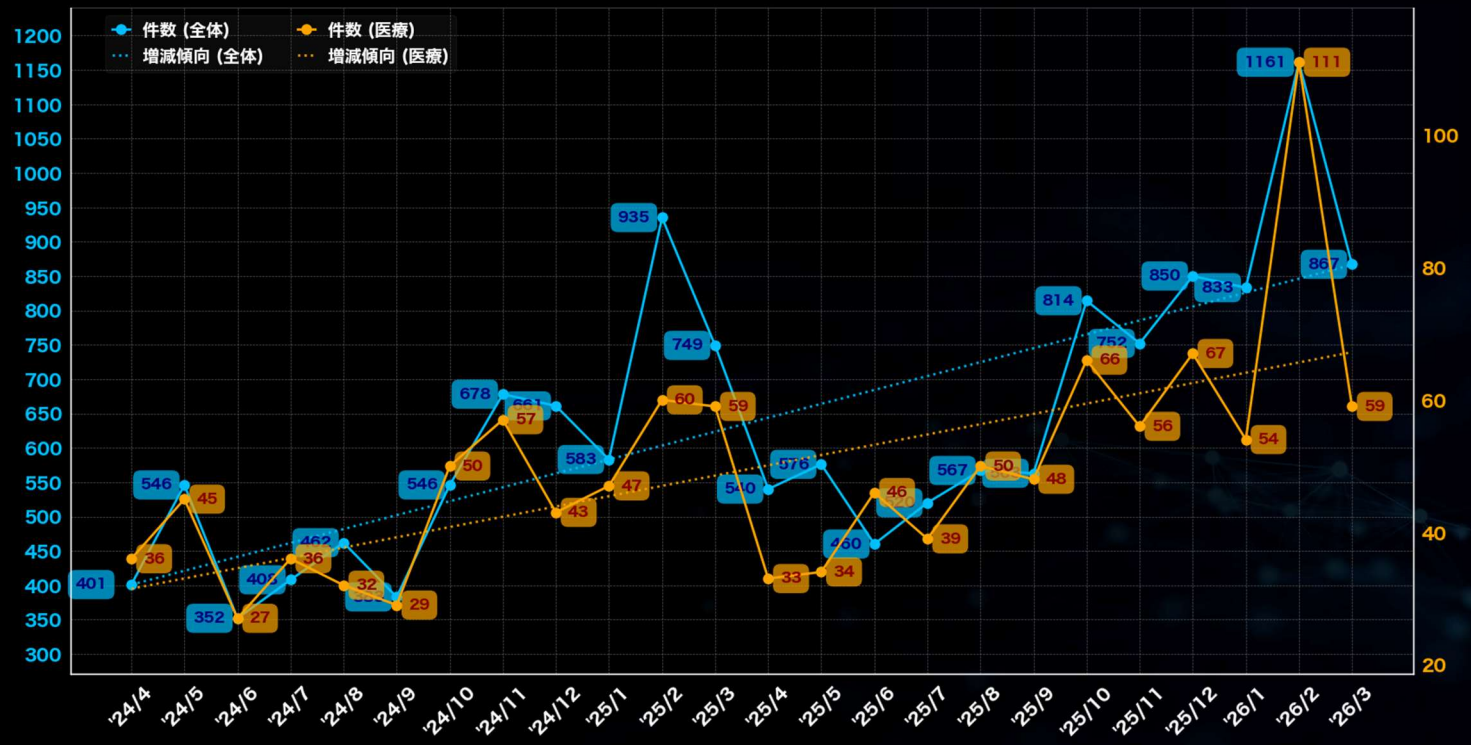
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

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

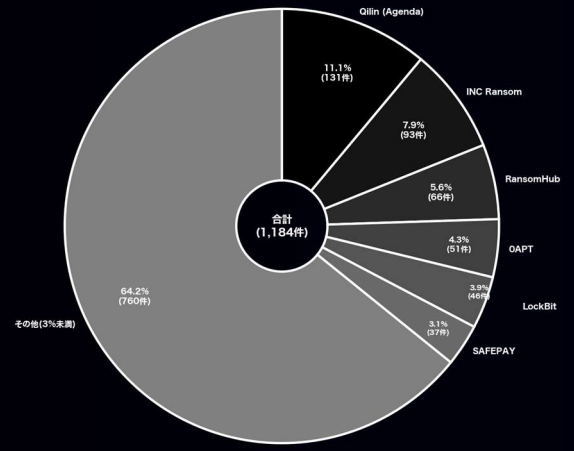
業種に関する分析（全世界）
（過去2年間／2024年4月～2026年3月）

医療

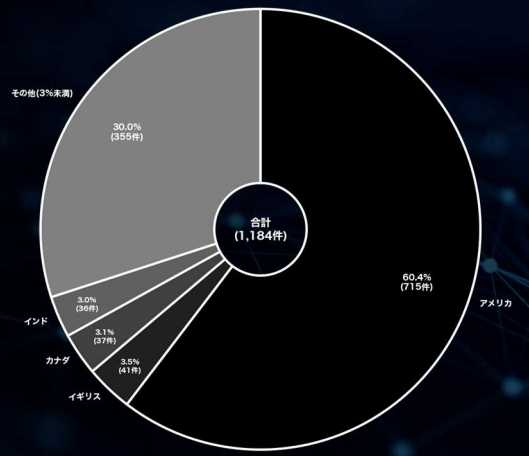
「医療」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年2月で、111件の掲載があった。一方、最も少なかった月は2024年6月で、27件であった。被害組織の所在国の割合では、アメリカが約60%と最も多く、次いでイギリス、カナダがそれぞれ約4%と約3%である。攻撃グループについては、少なくとも118のグループが関与しており、特に「Qilin (Agenda)」が131件のリークサイト掲載を実施している。次いで「INC Ransom」と「RansomHub」がそれぞれ93件と66件の掲載を行っている。かつては低水準だった医療関連の被害数は2023年3月頃に増加し、その後も増加傾向が続いている。この変化の背景には、攻撃グループが生存競争の中で業種を問わない攻撃へと方針を転換していった可能性も否定できない。また、国別に見る傾向としてアメリカにおける被害が非常に高い割合を占めている点が顕著である。



▼攻撃グループ別



▼国別



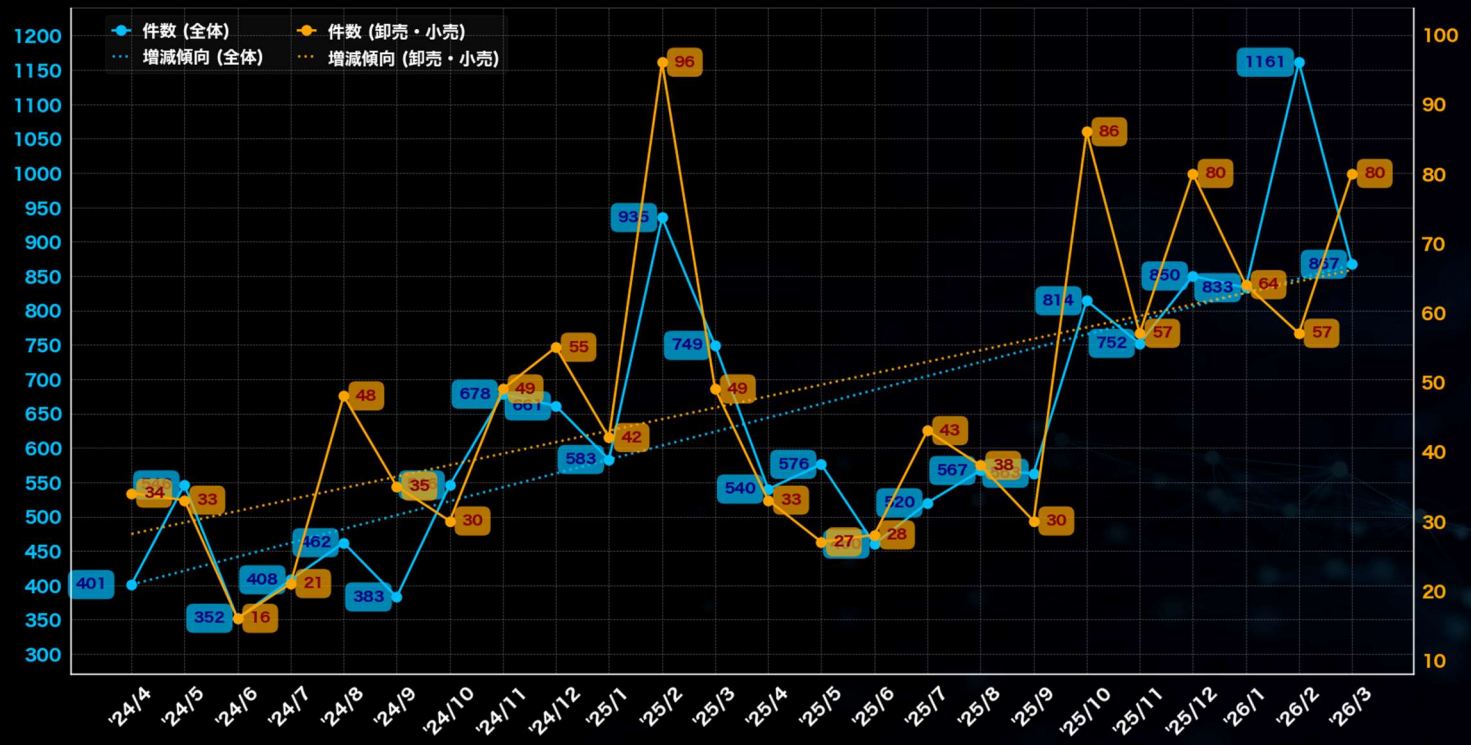
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

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

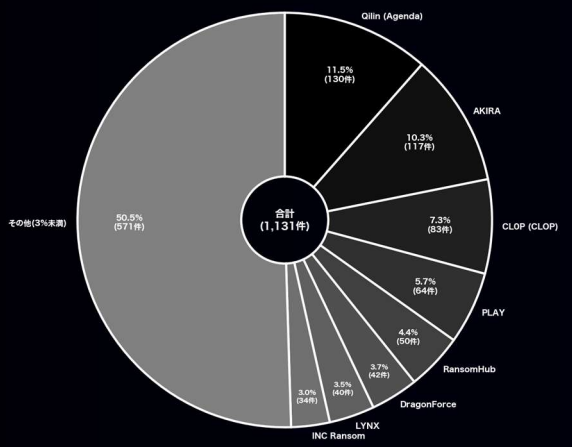
業種に関する分析（全世界）
（過去2年間／2024年4月～2026年3月）

卸売・小売

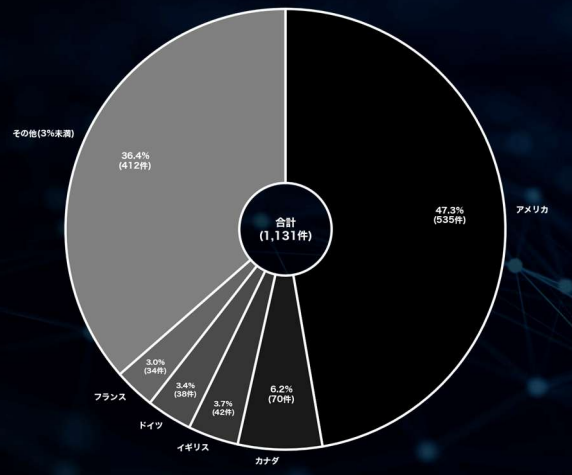
「卸売・小売」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、96件の掲載があった。一方、最も少なかった月は2024年6月で、16件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いでカナダとイギリスがそれぞれ約6%と約4%である。攻撃グループについては、少なくとも104のグループが関与しており、特に「Qilin (Agenda)」が130件のリークサイト掲載を実施している。次いで「AKIRA」と「CL0P (CLOP)」が117件と83件の掲載を行っている。卸売・小売関連は大きな増減の波があるものの、過去2年間の推移としては明確な増加傾向がある。



▼攻撃グループ別



▼国別



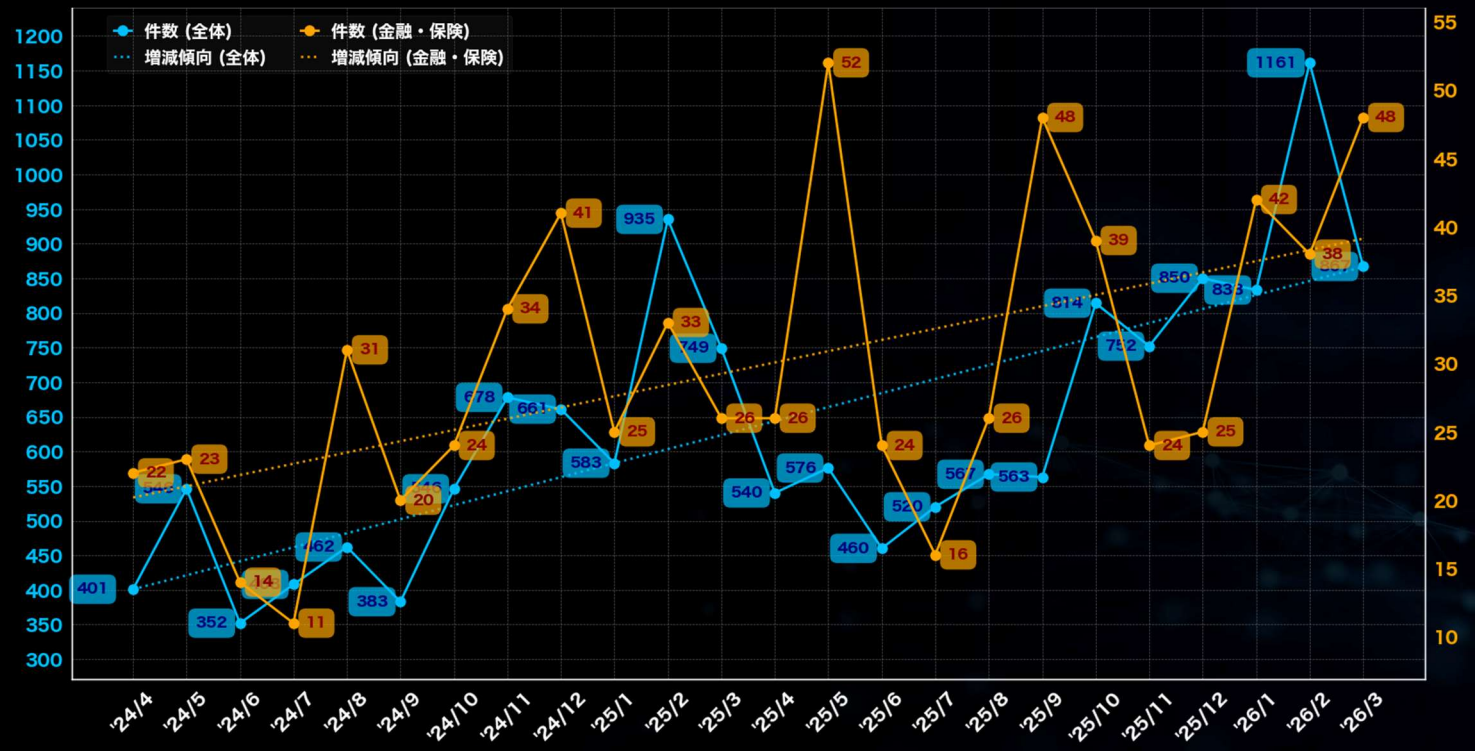
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

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

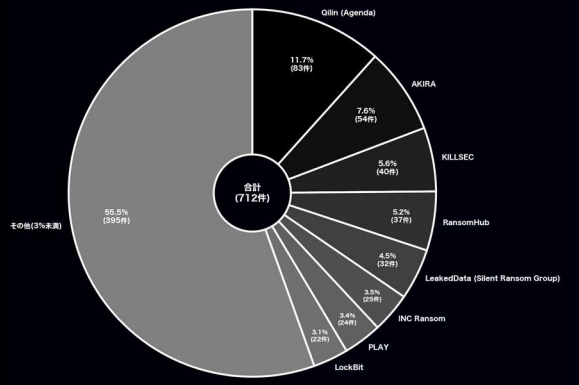
業種に関する分析（全世界）
（過去2年間／2024年4月～2026年3月）

金融・保険

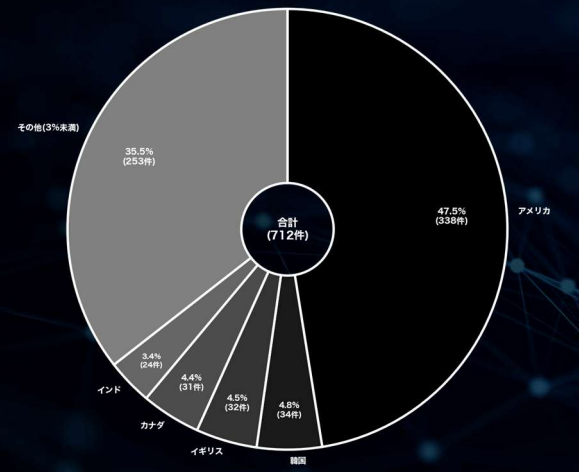
「金融・保険」業界に対するランサムウェア攻撃のリークサイト掲載件数は、最も多かった月が2025年5月で、52件の掲載があった。一方、最も少なかった月は2024年7月で、11件であった。被害組織の所在国の割合では、アメリカが約48%と最も多く、次いで韓国とイギリスがそれぞれ約5%である。攻撃グループについては、少なくとも111のグループが関与しており、特に「Qilin (Agenda)」が83件のリークサイト掲載を実施している。次いで「AKIRA」と「KILLSEC」がそれぞれ54件と40件の掲載を行っている。金融・保険関連は全体件数に対する割合は低いものの明確な増加傾向にある。



▼攻撃グループ別



▼国別



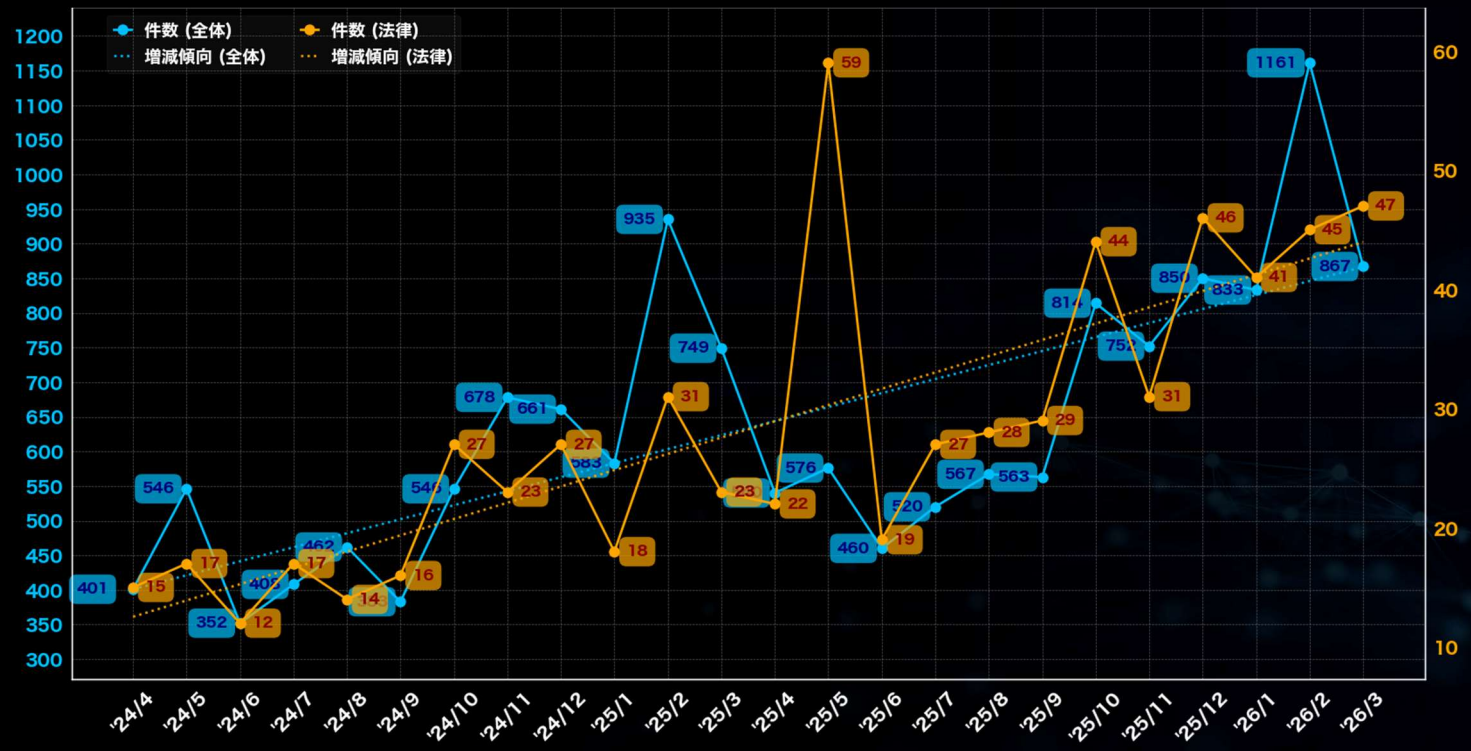
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

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

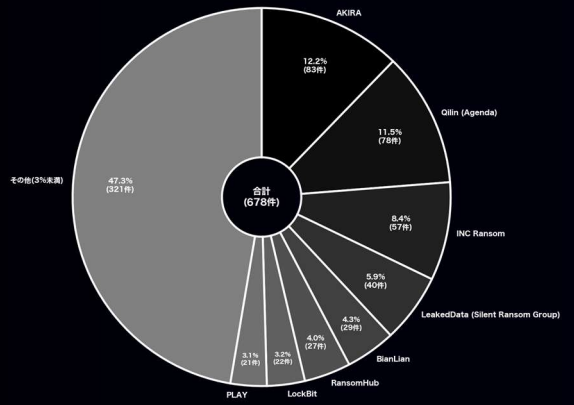
業種に関する分析（全世界）
（過去2年間／2024年4月～2026年3月）

法律

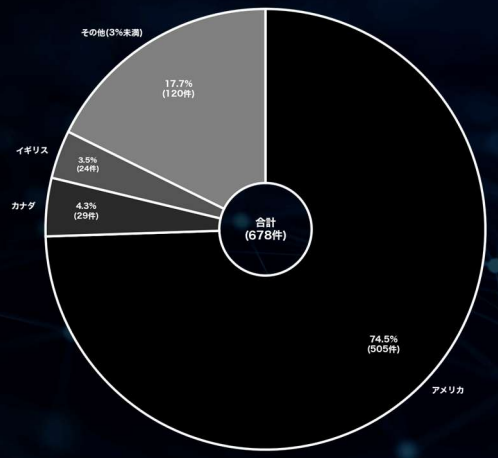
「法律」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年5月で、59件の掲載があった。一方、最も少なかった月は2024年6月で、12件であった。被害組織の所在国の割合では、アメリカが約75%と最も多く、次いでカナダとイギリスがそれぞれ約4%である。攻撃グループについては、少なくとも88のグループが関与しており、特に「AKIRA」が83件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「INC Ransom」がそれぞれ78件と57件の掲載を行っている。法律関連は2023年末以降、減少傾向が見られたが、2024年9月から10月、2025年4月から5月のように突発的に大きく件数を伸ばす時期があることを確認している。過去2年間においては明確な増加傾向にある。



▼攻撃グループ別



▼国別



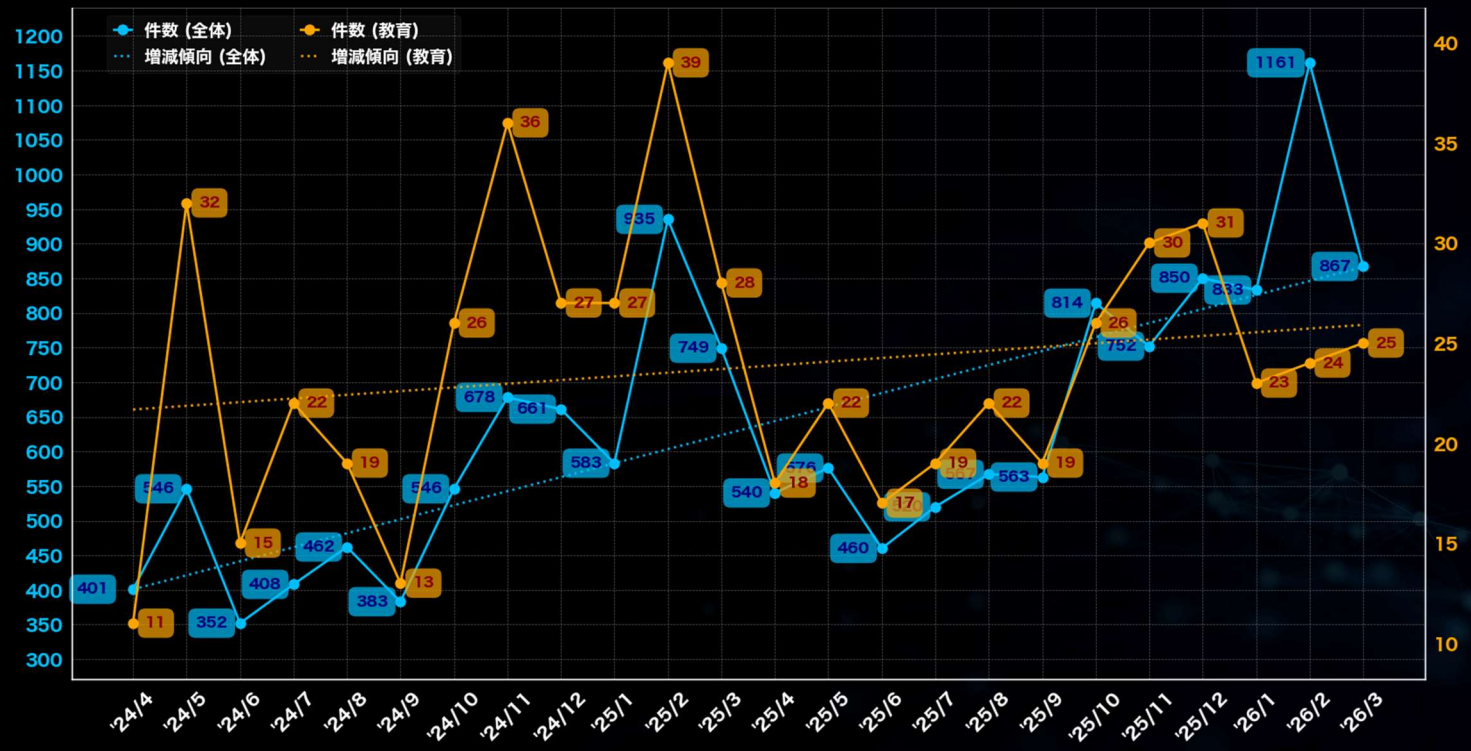
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて
国内被害組織からの公表や報道から判明した数も含んでいる）

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

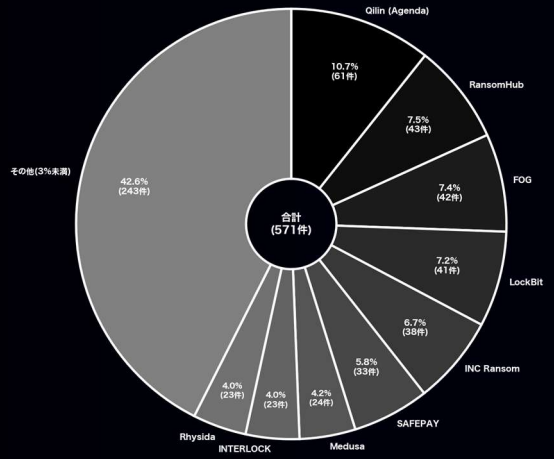
業種に関する分析（全世界）
（過去2年間／2024年4月～2026年3月）

教育

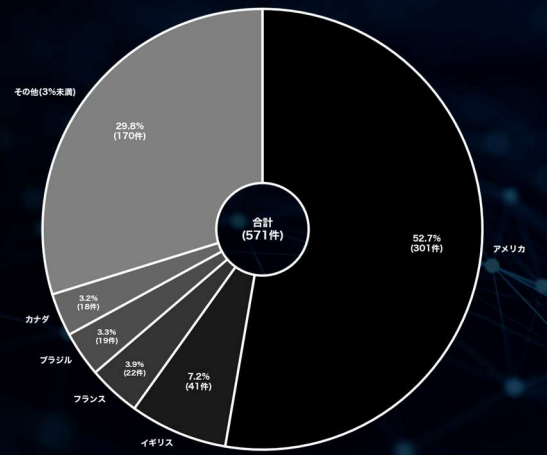
「教育」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、39件の掲載があった。一方、最も少なかった月は2024年4月で、11件であった。被害組織の所在国の割合では、アメリカが約53%と最も多く、次いでイギリスとフランスがそれぞれ約7%と約4%である。攻撃グループについては、少なくとも88のグループが関与しており、特に「Qilin (Agenda)」が61件のリークサイト掲載を実施している。次いで「RansomHub」と「FOG」がそれぞれ43件と42件の掲載を行っている。過去2年間の推移は緩やかな増加傾向となっている。



▼攻撃グループ別



▼国別



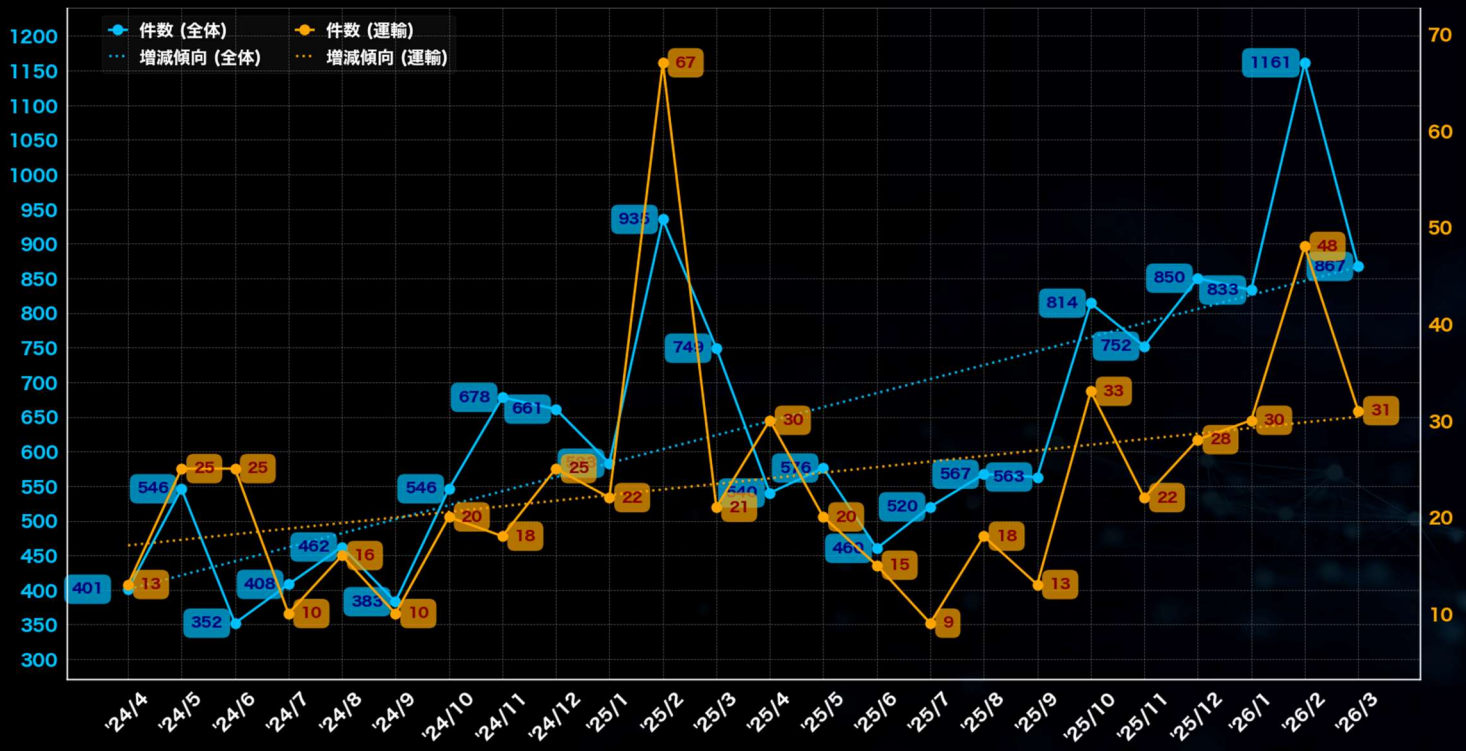
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

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

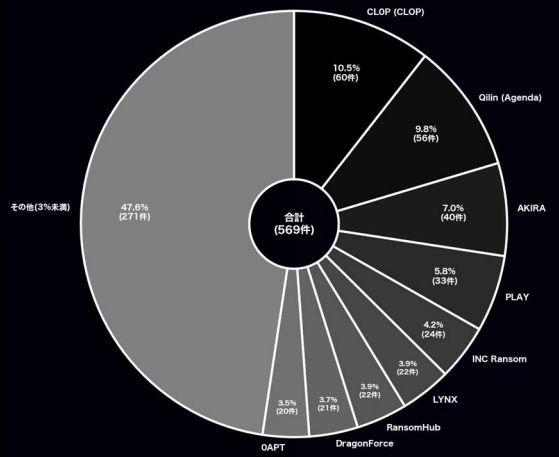
業種に関する分析（全世界）
（過去2年間／2024年4月～2026年3月）

運輸

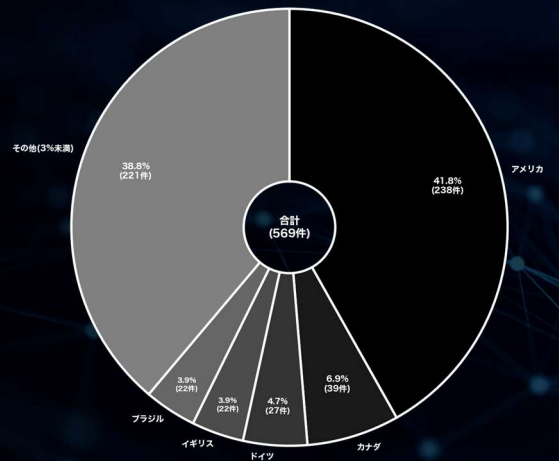
「運輸」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、67件の掲載があった。一方、最も少なかった月は2025年7月で、9件であった。被害組織の所在国の割合では、アメリカが約42%と最も多く、次いでカナダとドイツがそれぞれ約7%と約5%である。攻撃グループについては、少なくとも92のグループが関与しており、特に「CL0P (CLOP)」が60件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「AKIRA」がそれぞれ56件と40件の掲載を行っている。運輸関係は全体件数に対する割合こそ低く、過去2年間では著しく被害が減少するケースもある一方で、緩やかな増加傾向が続いている。



▼攻撃グループ別



▼国別



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

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

CIGのコンテンツ紹介

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

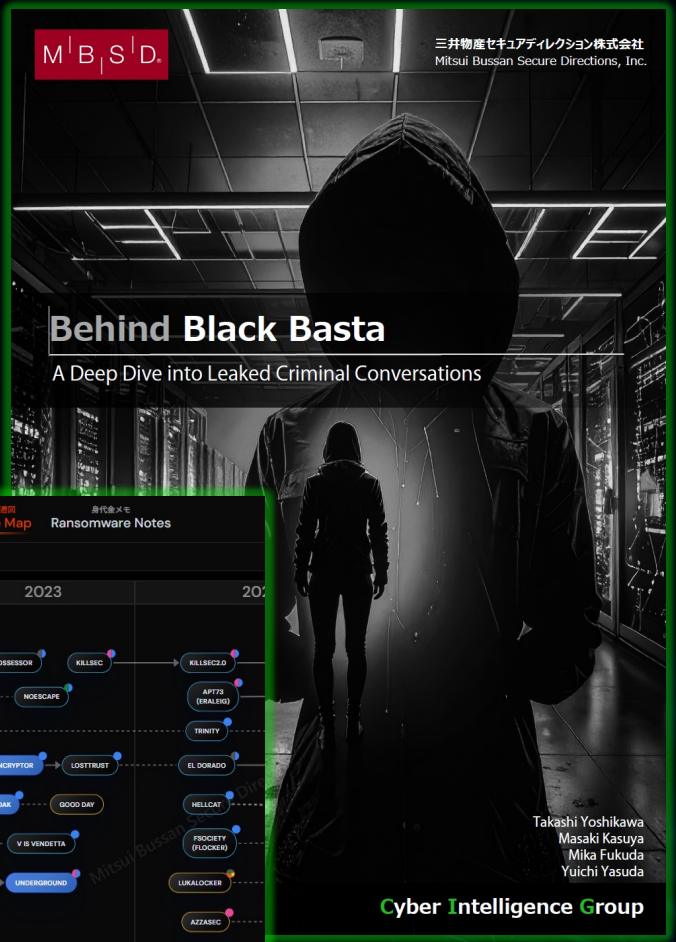
● CIG Ransomware Information Portal (WEBアプリケーション)：
https://www.mbsd.jp/cig-ransomware-portal/

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

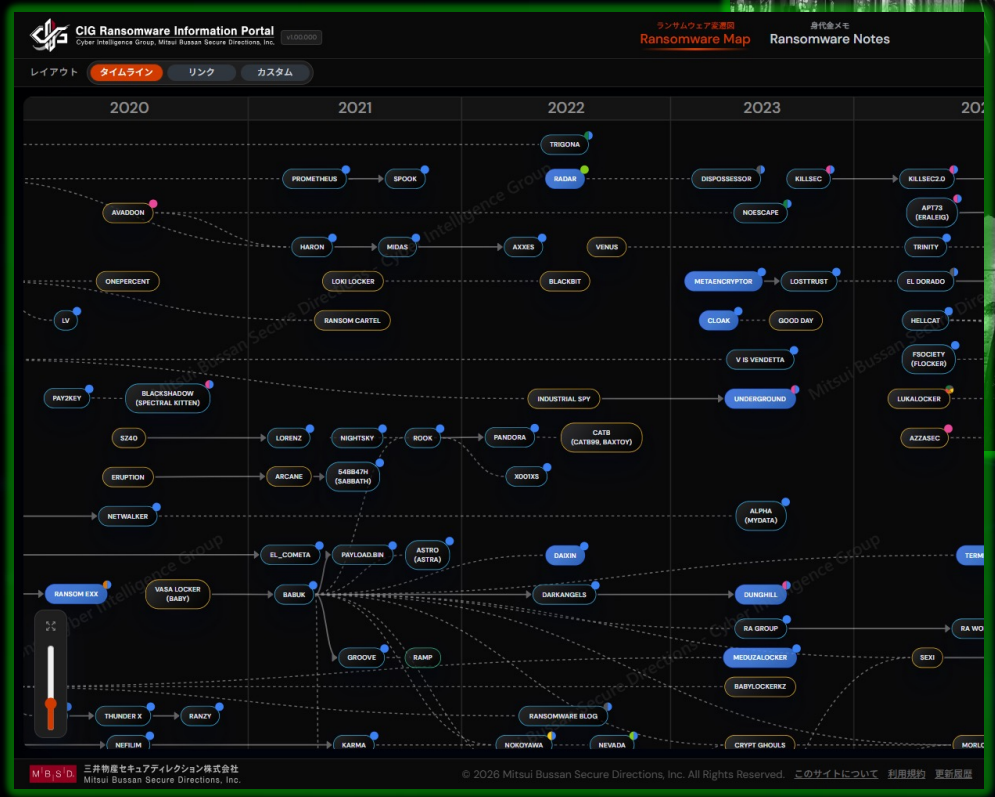
● 技術ブログ：
https://www.mbsd.jp/research/cig/
https://www.mbsd.jp/research/t.yoshikawa/

● 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