暴露型ランサムウェア攻撃統計
CIGマンスリーレポート

2025年10月号 Rev 1.00
(2025年9月分)

2025
9

Cyber Intelligence Group

目次

総括と監視対象（レポート① ~ ④）

グローバル統計（レポート⑤ ~ ⑯）

日本関連組織を対象とした統計（レポート⑰ ~ 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

2025

9

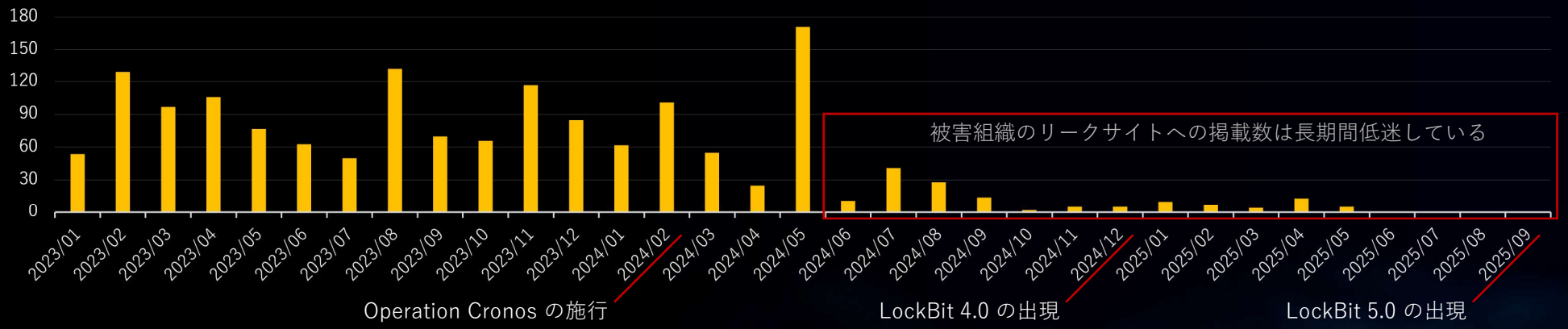
今月のハイライト

● LockBit 5.0 の出現と DragonForce および Qilinとの連合

LockBit の活動経緯

2025年9月上旬、LockBit 5.0 の出現を確認した。初代 LockBit (別名: ABCD) が登場した2019年9月3日から6年が経過しており、同グループは長期にわたり活動を続けるランサムウェア集団の一つである。2024年2月に国際的な法執行機関が連携して実施した「Operation Cronos」では、関係者の逮捕やリークサイトの差し押さえが行われ、2024年6月以降はリークサイトの掲載数が著しく低下している。2025年10月中旬時点においても目立った変化を確認していない状況である。

LockBit による被害を受けた企業のリークサイト掲載数



DragonForce および Qilin との連合 - LockBit が再度勢力を増す可能性

LockBit 5.0 の登場直後、DragonForce が LockBit および Qilin に対して協力関係を結ぶことを提案した。2025年9月中旬には、これら三者が協力している様子がハッカーフォーラム上で確認できた。

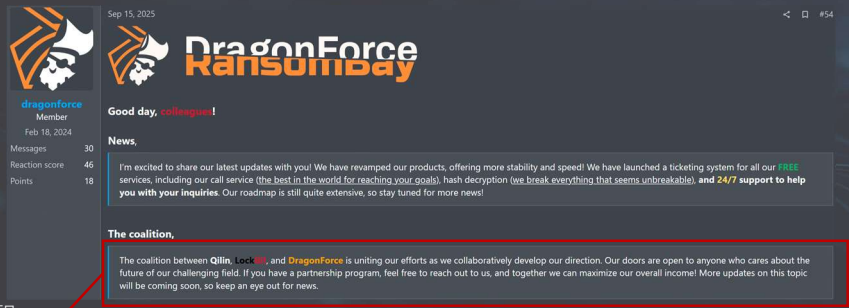
Operation Cronos 以降に弱体化した LockBit にとって、DragonForce および Qilin との連携は、勢力を拡大しつつあるグループと協力し、リソースやインフラを共有することで効率良く攻撃を行うことが見込まれる。

補足情報

- DragonForce: ランサムウェア攻撃用のインフラと管理システムを提供し、参加グループが独自名称のまま活動を継続できる基盤を2025年3月に発表。
- Qilin: 今年の 6～9 月はリークサイトの掲載数において一位。

勢力の低下が見られる LockBit ではあるが再び猛威を振るい、かつての勢いを取り戻す可能性もあるため、今後の動向を注視する必要がある。

DragonForceがハッカーフォーラムにて LockBit / Qilin との連合を宣言



日本語訳:

Qilin、LockBit、そして DragonForce の三者による連合が、私たちの取り組みを一つにまとめ、共に進むべき方向を形づくっています。私たちは、この困難な分野の未来を真剣に考えるすべての方々に対して、常に扉を開いています。もしあなたがパートナーシップ・プログラムをお持ちであれば、ぜひご連絡ください。協力することで、全体としての収益を最大化できるはずです。このテーマに関するさらなる情報も、まもなく公開予定です。今後のニュースをお見逃しなく！

※ 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: 2025年9月1日～2025年10月15日）

【ランサムウェア管理者が、Lockergoga、Nefilim、Megacortex、ランサムウェアを数百人の被害者に配布したとしてサイバー犯罪で起訴】（米国司法省：2025/09/09）
ウクライナ国籍のVolodymyr Tymoshchukが国際的ランサムウェア攻撃で起訴。2018～21年に世界中の企業や医療機関を標的とし、数千万ドルの損害。米国務省は最大1100万ドルの報奨金を提示。
https://www.justice.gov/usao-edny/pr/ransomware-administrator-charged-cybercrimes-deploying-lockergoga-nefilim-and

【Akiraランサムウェアグループ、初期アクセスにSonicWallデバイスを利用】（RAPID 7：2025/09/11）
SonicWall社がクラウドバックアップへの不正アクセスを公表。ファイアウォールの認証情報が漏洩した可能性がある。 Rapid7のIRチームは、SonicWallアプライアンスを標的とした侵入の増加を確認。
https://www.rapid7.com/blog/post/dr-akira-ransomware-group-utilizing-sonicwall-devices-for-initial-access/

【 LockBit復活：バージョン 5.0 の新機能とは】（VECTRA：2025/09/12）
ランサムウェア攻撃グループLockBitは2024年、法執行機関によって摘発されたが、LockBit 5.0として復活。より高速な暗号化と強力な回避機能を備え、アフィリエイトプログラムを刷新。
https://ja.vectra.ai/blog/lockbit-is-back-whats-new-in-version-5-0

【令和７年上半期における サイバー空間をめぐる脅威の情勢等について】（警察庁サイバー警察局：2025/09/18）
2025年上半期、サイバー空間の脅威はDDoS攻撃・AI悪用型攻撃・ランサムウェア（RaaS）・SNSやSMS経由の被害が増加。個人・企業被害多発、攻撃手法も高度化。
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

【CountLoader、マルチバージョンマルウェアローダーでロシアのランサムウェア活動を拡大】（The Hacker News：2025/09/18）
ランサムウェアグループが使用する新型マルウェアローダー「CountLoader」を発見。LockBitやBlack Bastaと関連し、ウクライナを標的にPDF偽装で拡散。.NET、PowerShell、JavaScriptの3バージョンが存在する。
https://thehackernews.com/2025/09/countloader-broadens-russian-ransomware.html

【EUサイバー機関、空港のソフトウェアが犯罪者に身代金目的で奪われたと発表】（BBC：2025/09/22）
ENISAは、犯罪者がランサムウェアを用いて欧州を含む空港の自動チェックイン・搭乗システムを混乱させたと発表。米Collins Aerospaceが標的となり、EUの空港で欠航や遅延が発生。
https://www.bbc.com/news/articles/cqjeej85452o

【EUは多様かつ収束的な脅威グループから常に標的にされている】（ENISA：2025/10/01）
ENISAは2025年版脅威レポートでランサムウェアをEU域内で最も影響力の大きい脅威と特定、供給網を介する波及リスクを強調した。
https://www.enisa.europa.eu/news/etl-2025-eu-consistently-targeted-by-diverse-yet-convergent-threat-groups
（レポート：https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025#contentList）

【LockBit、Qilin、DragonForceが提携し、ランサムウェアエコシステムを支配】（The Hacker News：2025/10/08）
LockBit、Qilin、DragonForceが戦略的カルテルを結成し、重要インフラ攻撃とRaaS拡張を目的に技術・資源を共有すると発表。
https://thehackernews.com/2025/10/lockbit-qilin-and-dragonforce-join.html

【CL0P関連のハッカーがOracleソフトウェアの欠陥を利用して数十の組織に侵入】（The Hacker News：2025/10/10）
Google Threat IntelligenceはOracle EBSのゼロデイCVE-2025-61882を悪用した攻撃を確認、数十組織が侵害され身代金要求を受けた。
https://thehackernews.com/2025/10/cl0p-linked-hackers-breach-dozens-of.html

【サイバー攻撃緊急時対応計画は文書化されるべきだと企業に勧告】（BBC：2025/10/14）
英国NCSCは、企業に“レジリエンスエンジニアリング”の導入を推奨。事業継続計画は紙やオフラインで保管し、メールなどが使用できない状況を想定したアナログな連絡手段などの回避策も含めるべきと提案。
https://www.bbc.com/news/articles/ced61xv967lo.amp

※ 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）：271（※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：59

※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）

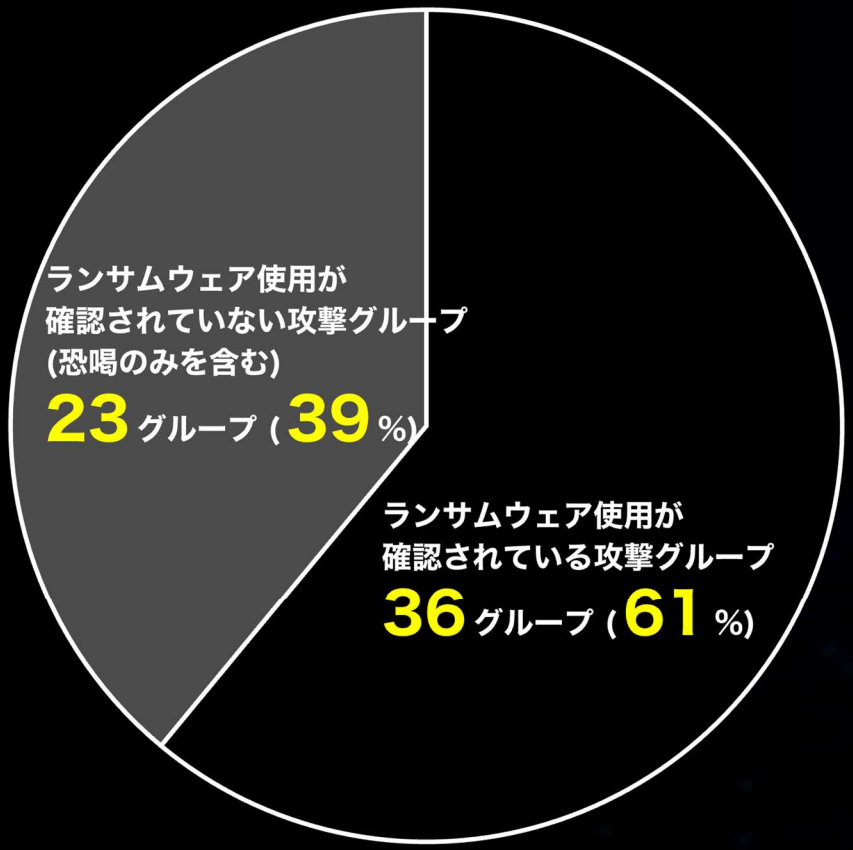
0mega (Omega)
8BASE
Abyss
AKIRA
AKO
Alpha (MYDATA)
AlphV (BlackCat)
Anubis
Apos Security
APT73 (Eraleig)
● ARACHNA
ARCUS MEDIA
Argonauts
Arkana
ArvinClub
Astro (Astra)
AtomSilo
Avaddon
AvosLocker
Axxes
AzzaSec
Babuk
Babuk (2025)
BASHE
BEAST
BERT
BianLian
BL0ODY (BLOODY)
Bl4ckt0r (BlackTor)
Black Basta
BlackByte
BlackDolphin
BlackLock
BlackMatter
Black Nevas
Blackout
● BLACKSHRANTAC
BlackSuit
BLUEBOX
BLUESKY
BQTLOCK
Brain Cipher
BULLY
Business Data Leaks
CACTUS
Cephalus
CHAOS (2025)
CHEERS
ChileLocker (Arcrypter)
CHORT
Cicada3301
CiphBit
CipherLocker
CL0P (CLOP)
Cloak
● COINBASE CARTEL
Conti
Cooming Project
Crazy Hunter Team
CROSSLOCK
CryptBB
CRYPTNET
CRYPTO24
CryptOn
Cuba
Cyclops
D4RK4RMY
DAGON
DAIXIN
dAn0n (danon)
Dark Angels
DARKBIT
DARKPOWER
DarkRace
DarkRypt
Darkside
Dark Vault
DataCarry
Desolator
DEVMAN
DEVMAN 2.0
Dire Wolf
Dispossessor[Databroker]
Donex
Donut Leaks
DoppelPaymer
dotAdmin
DragonForce
DragonRansomware
DUNGHILL
eCh0raix (eChoraix)
El_Cometa
EL DORADO
EMBARGO
Endurance
Entropy
Everest
FOG
Frag
FSOCIETY / FLOCKER
FSTeam
Funksec
GD LockerSec
GLOBAL
Grief
Groove
Gunra
HANDARA [Hacktivist]
Haron
HELLCAT
Helldown
HelloGookie
Hitler (AGL0BGVYCG)
Hive
HolyGhost
Hotarus
Hunters International
ICEFIRE
IMN Crew
INC Ransom
Insane
INTERLOCK
J GROUP
KAIROS
Karakurt
Karma
Kawa4096
KILLSEC
Knight
Kraken (HelloKitty)
LAMBDA
La Piovra
LAPSUS$
LeakedData (Silent Ransom Group)
LEAKNET
LILITH
Linkc
LockBit
Lorenz
LostTrust
● LunaLock
LV
LYNX
MADCAT
MAD LIBERATOR
MALAS
MalekTeam
Mallox
Mamona RIP
MBC
Medusa
MEOW
Metaencryptor
Midas
● MIGA
Mindware
Mogilevich [fraud]
MOISHA
Money Message
Monti
Morpheus
Mount Locker
N3tw0rm (NetWorm)
N4UGHTYSEC (NAUGHTYSEC)
Nefilim
Nevada
NightSky
NightSpire
NITROGEN
NoEscape
Nokoyawa
NONAME (VFOKX)
NONAME [2023年確認]
Nova
NULLBULGE
● Obscura
Onyx
Orca
Pandora
Pay2Key
Payload.bin
Payouts King
PEAR
PLAY
PLAYBOY
Prometheus
PRYX
PUTIN TEAM
Pysa / Mespinoza
Qilin (Agenda)
QIULONG
Quantum
RABBIT HOLE
● RADAR
● RADIANT
Ragnar Locker
Ragnarok
RA GROUP
RALord
Rancoz
RansomBay
Ransom Cartel
Ransom Corp
RANSOMCORTEX
Ransomed.vc
Ransom EXX
RansomHouse
RansomHub
Ransomware Blog
Ranzy
RA WORLD
Raznatovic
RedAlert (N13V)
Red Ransomware Group (Red CryptoApp)
Relic
Revil (Sodinokibi)
Rhysida
Risen
ROOK
Royal
Rransom
RunSomeWares
Sabbath (54bb47h)
SAFEPAY
SARCOMA
SATAN LOCK
SATANLOCK V2
Secp0
Securotrop
SenSayQ
shaoleaks
SIEGEDSEC
Silent
Sinobi
SKIRA TEAM
SLUG
Snatch
Solidbit
Space Bears
Sparta
Spook
STORMOUS
Sugar
Suncrypt
SynACK
TeamXXX
Termite
● The Gentlemen
ThreeAM (3AM)
TRIGONA
TRINITY
TRISEC
Underground
UnSafe
Valencia
VanHelsing
VanirGroup
Vice Society
V IS VENDETTA
VSOP
WALocker
Warlock
WEREWOLVES
Weyhro
WORLD LEAKS
x001xs
XING Team
Yanluowang
● Yurei
Zeon
Zero Tolerance

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

監視中のランサムウェア攻撃グループ情報
（ランサムウェア使用の割合）

●現在活動中の攻撃グループにおけるランサムウェア使用の割合（2025年9月）

（※当月にリークサイト掲載を確認した攻撃グループ全59グループ中）



暴露型攻撃グループの中にはSTORMOUSやKarakurtなど、ランサムウェアの使用が明確に確認されていない攻撃グループや、ランサムウェアを使用せず窃取データで恐喝のみを行う集団（恐喝グループ）も存在する。

一例として、BianLianやCLOPなどがデータを暗号化せずに恐喝を行う手法に移行しているとされる。

左の円グラフは、2025年9月に活動中である事が確認された全59グループにおけるランサムウェア使用の割合の内訳を示した図である。

※ 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

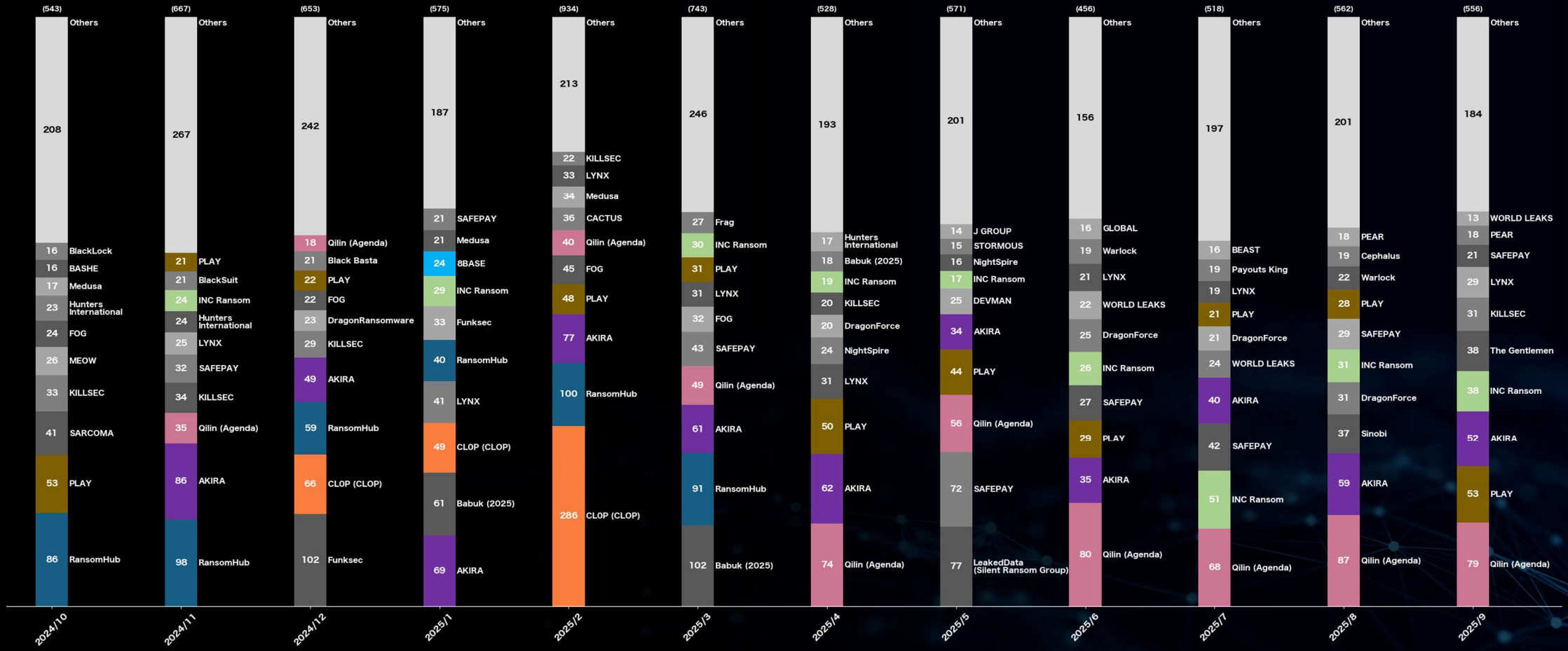
年間 統計
（全世界）

2025

9

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／2024年10月～2025年9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）

2025
9

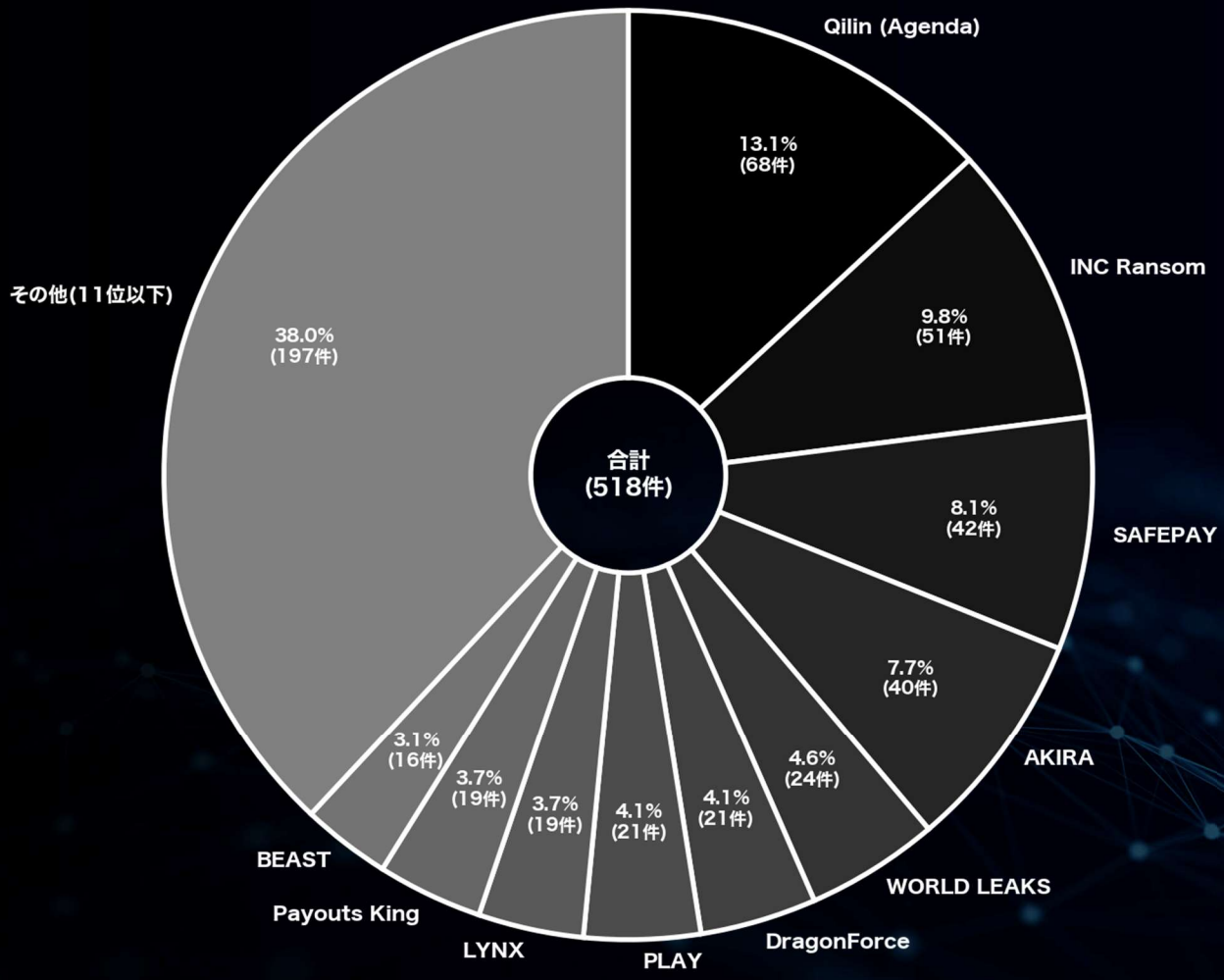
月別内訳 攻撃グループ TOP10（全世界）

（2025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)
Qilin (Agenda)	68	13.1	- 12
INC Ransom	51	9.8	+ 25
SAFEPAY	42	8.1	+ 15
AKIRA	40	7.7	+ 5
WORLD LEAKS	24	4.6	+ 2
DragonForce	21	4.1	- 4
PLAY	21	4.1	- 8
LYNX	19	3.7	- 2
Payouts King	19	3.7	+ 19
BEAST	16	3.1	+ 16

▼ランサムウェア攻撃グループの勢力割合
（リークサイトの掲載数による比較）



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

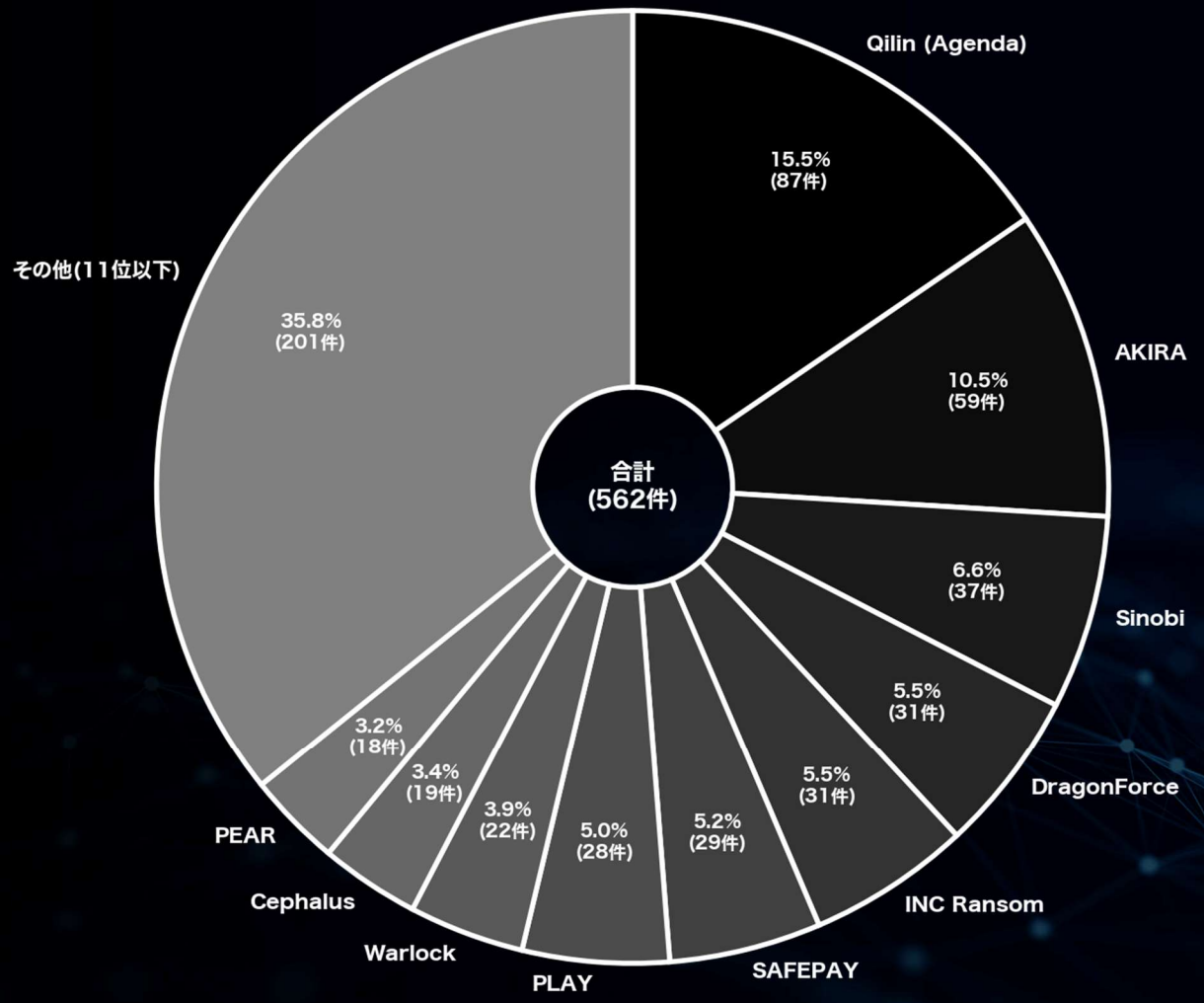
月別内訳 攻撃グループ TOP10（全世界）

（2025年 8 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)	87	15.5	+ 19
AKIRA	59	10.5	+ 19
Sinobi	37	6.6	+ 33
DragonForce	31	5.5	+ 10
INC Ransom	31	5.5	- 20
SAFEPAY	29	5.2	- 13
PLAY	28	5.0	+ 7
Warlock	22	3.9	+ 13
Cephalus	19	3.4	+ 19
PEAR	18	3.2	+ 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）



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

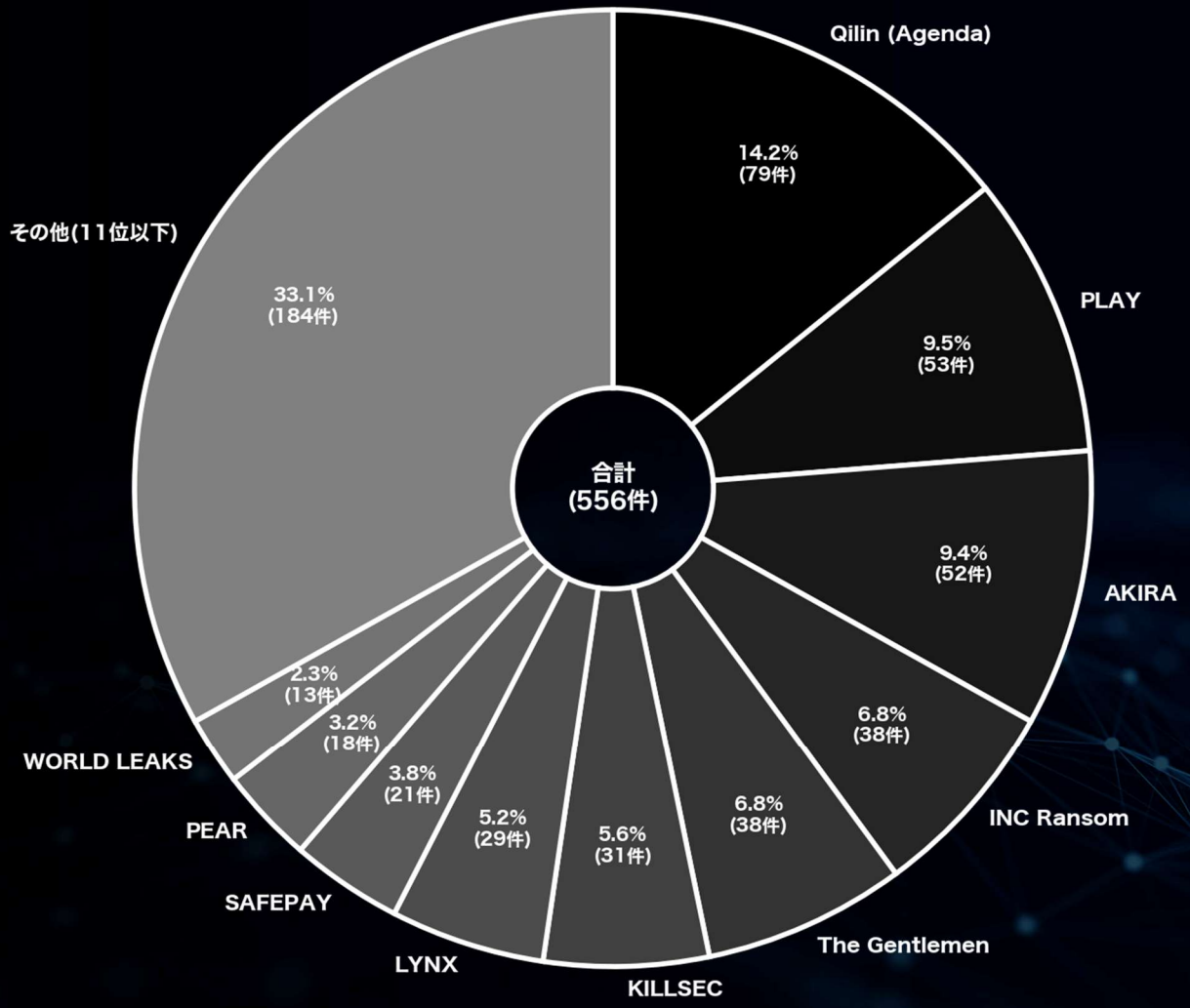
月別内訳 攻撃グループ TOP10（全世界）

（2025年 9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)	79	14.2	- 8
PLAY	53	9.5	+ 25
AKIRA	52	9.4	- 7
INC Ransom	38	6.8	+ 7
The Gentlemen	38	6.8	+ 38
KILLSEC	31	5.6	+ 29
LYNX	29	5.2	+ 15
SAFEPAY	21	3.8	- 8
PEAR	18	3.2	± 0
WORLD LEAKS	13	2.3	- 1

▼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）

2025

9

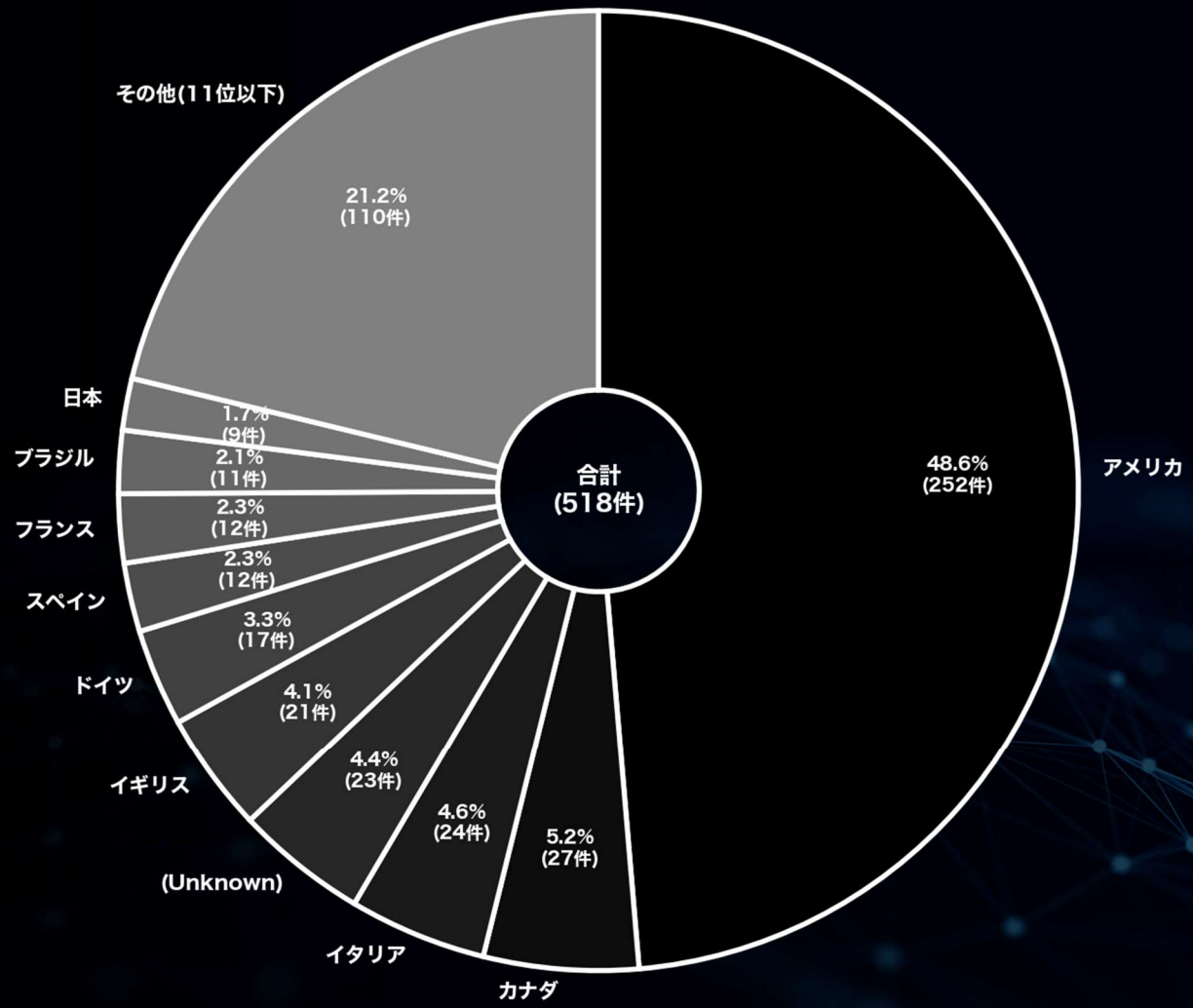
月別内訳 被害国TOP10（全世界）

（2025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	252	48.6	+ 15
カナダ	27	5.2	+ 8
イタリア	24	4.6	+ 13
(Unknown)	23	4.4	+ 11
イギリス	21	4.1	± 0
ドイツ	17	3.3	+ 2
スペイン	12	2.3	+ 1
フランス	12	2.3	+ 4
ブラジル	11	2.1	+ 3
日本	9	1.7	+ 8

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



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

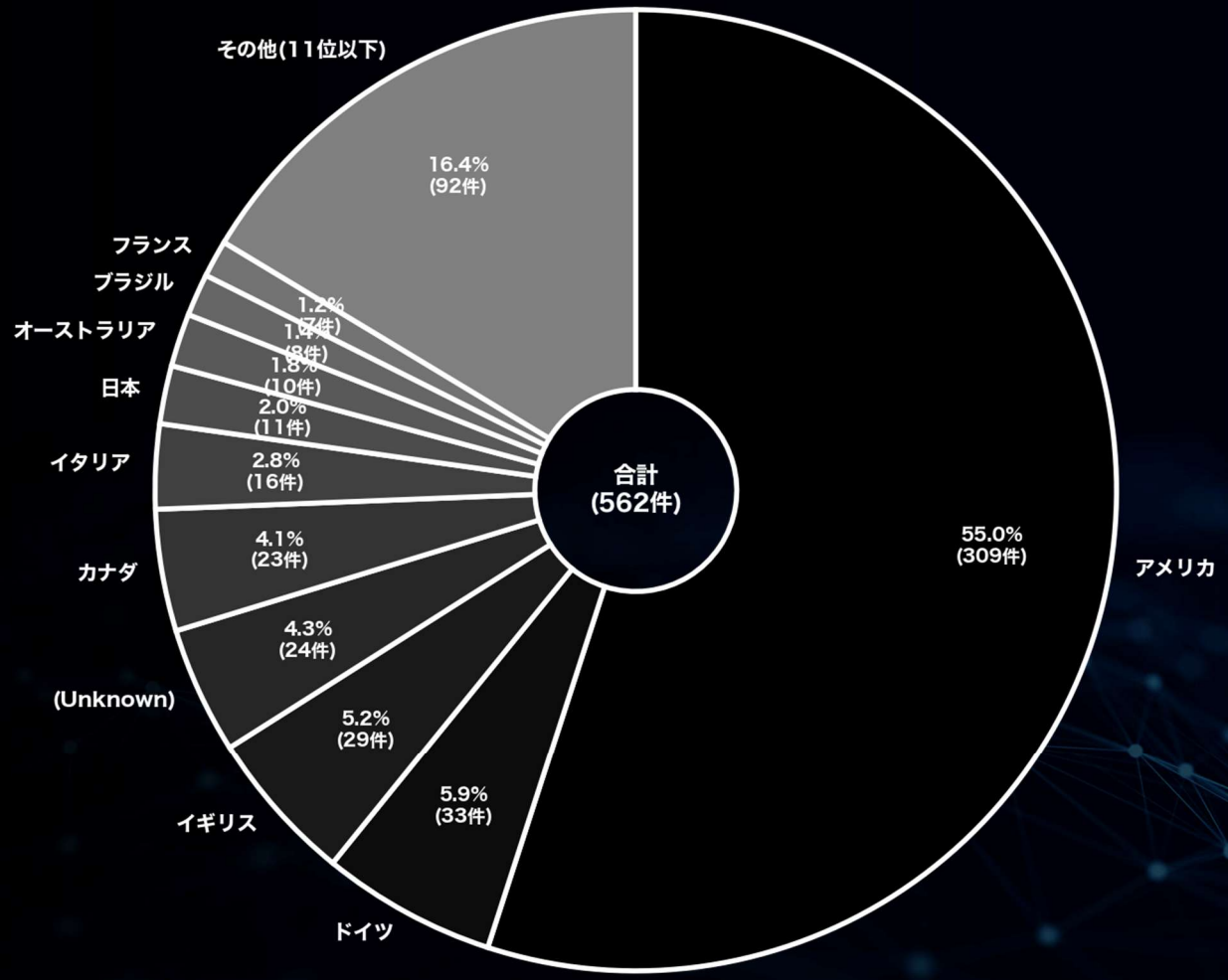
月別内訳 被害国TOP10（全世界）

（2025年 8 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	309	55.0	+ 57
ドイツ	33	5.9	+ 16
イギリス	29	5.2	+ 8
(Unknown)	24	4.3	+ 1
カナダ	23	4.1	- 4
イタリア	16	2.8	- 8
日本	11	2.0	+ 2
オーストラリア	10	1.8	+ 4
ブラジル	8	1.4	- 3
フランス	7	1.2	- 5

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



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

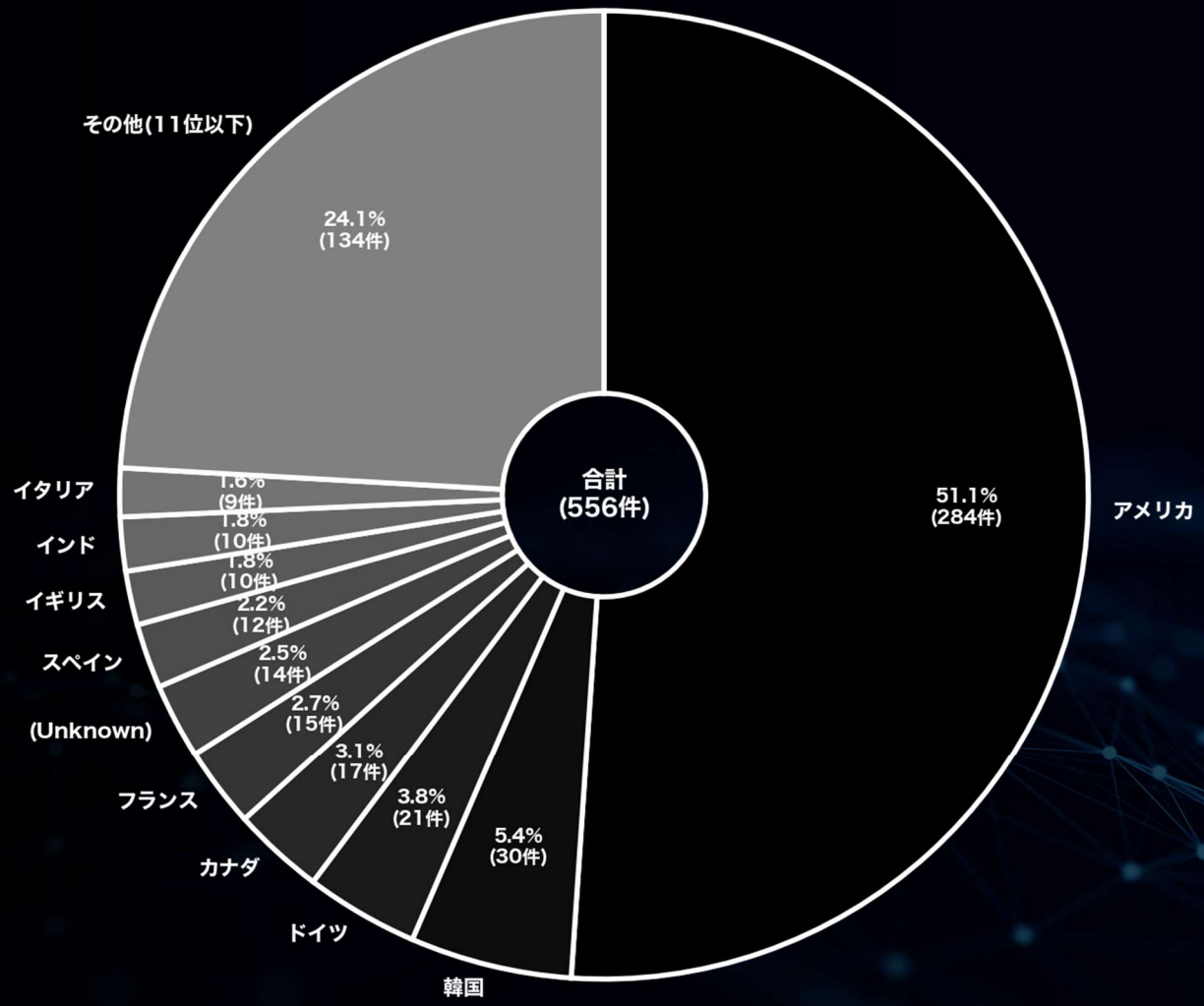
月別内訳 被害国TOP10（全世界）

（2025年 9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	284	51.1	- 25
韓国	30	5.4	+ 25
ドイツ	21	3.8	- 12
カナダ	17	3.1	- 6
フランス	15	2.7	+ 8
(Unknown)	14	2.5	- 10
スペイン	12	2.2	+ 6
イギリス	10	1.8	- 19
インド	10	1.8	+ 7
イタリア	9	1.6	- 7

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



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

被害国 月別統計
（アジア）　（過去3ヶ月分）

2025

9

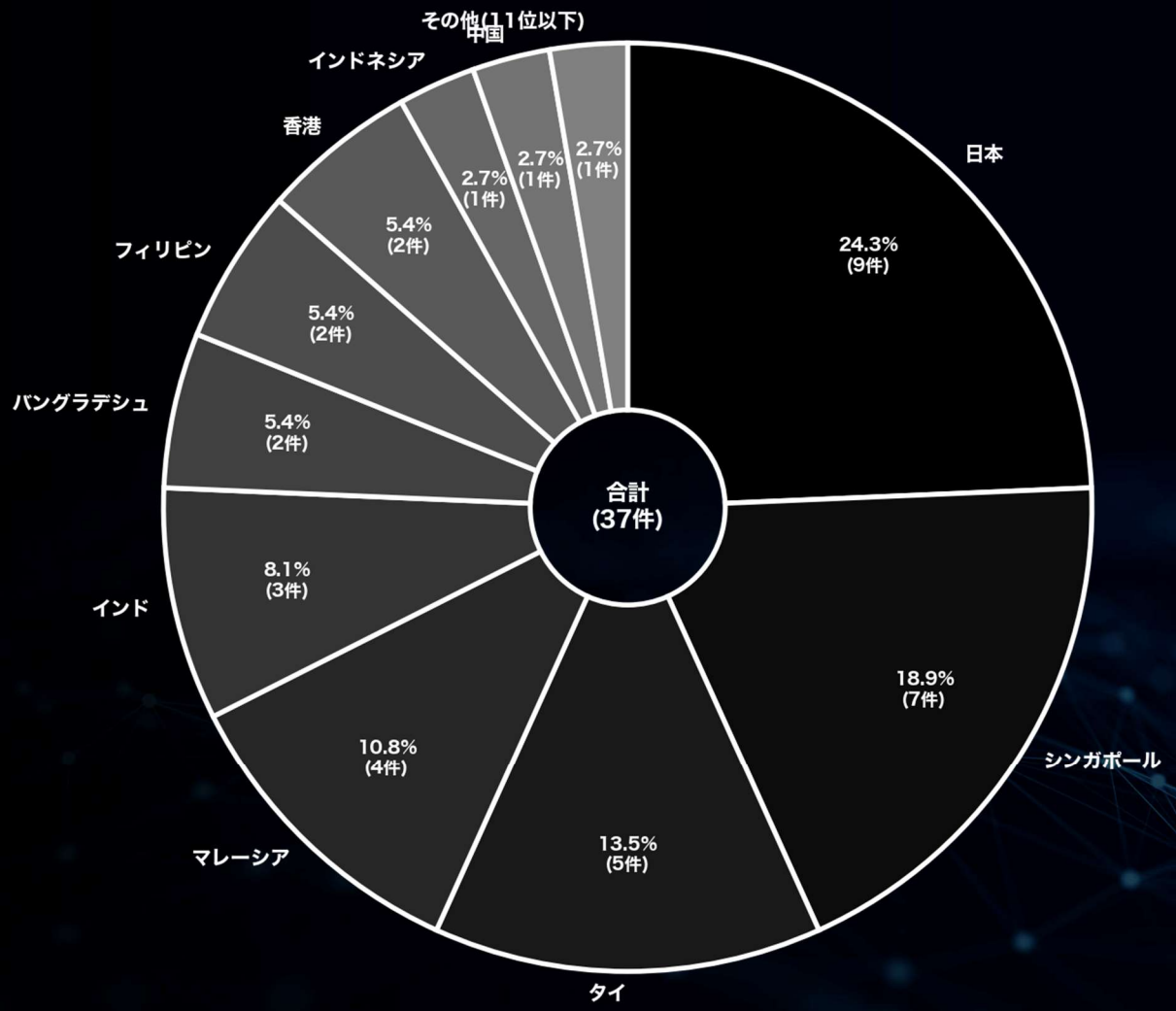
月別内訳 被害国TOP10（アジア）

（2025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)
日本	9	24.3	+ 8
シンガポール	7	18.9	+ 4
タイ	5	13.5	± 0
マレーシア	4	10.8	+ 4
インド	3	8.1	- 6
バングラデシュ	2	5.4	+ 1
フィリピン	2	5.4	+ 1
香港	2	5.4	+ 1
インドネシア	1	2.7	+ 1
中国	1	2.7	± 0

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



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

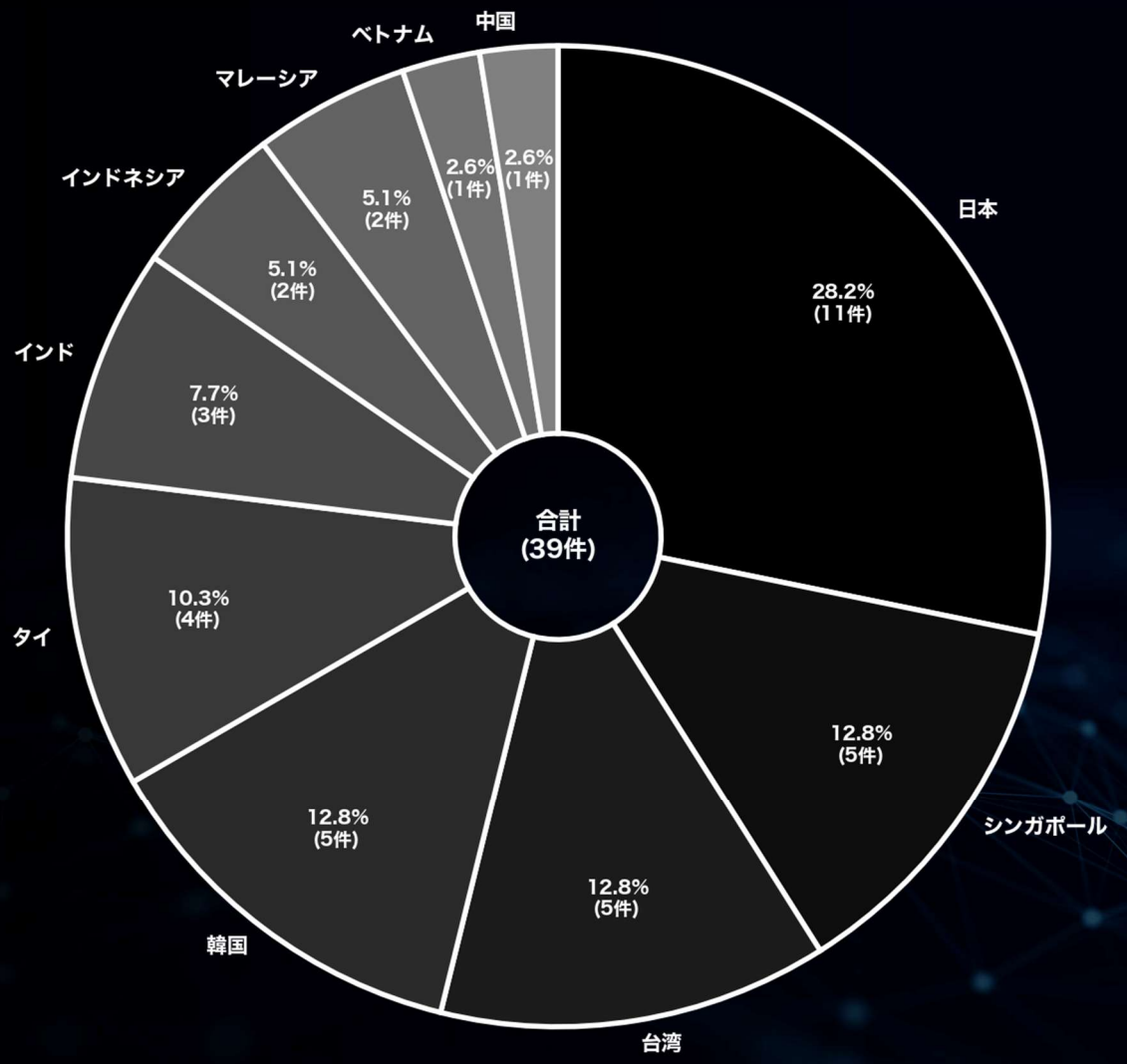
月別内訳 被害国TOP10（アジア）

（2025年 8 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	11	28.2	+ 2
シンガポール	5	12.8	- 2
台湾	5	12.8	+ 4
韓国	5	12.8	+ 5
タイ	4	10.3	- 1
インド	3	7.7	± 0
インドネシア	2	5.1	+ 1
マレーシア	2	5.1	- 2
ベトナム	1	2.6	+ 1
中国	1	2.6	± 0

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



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

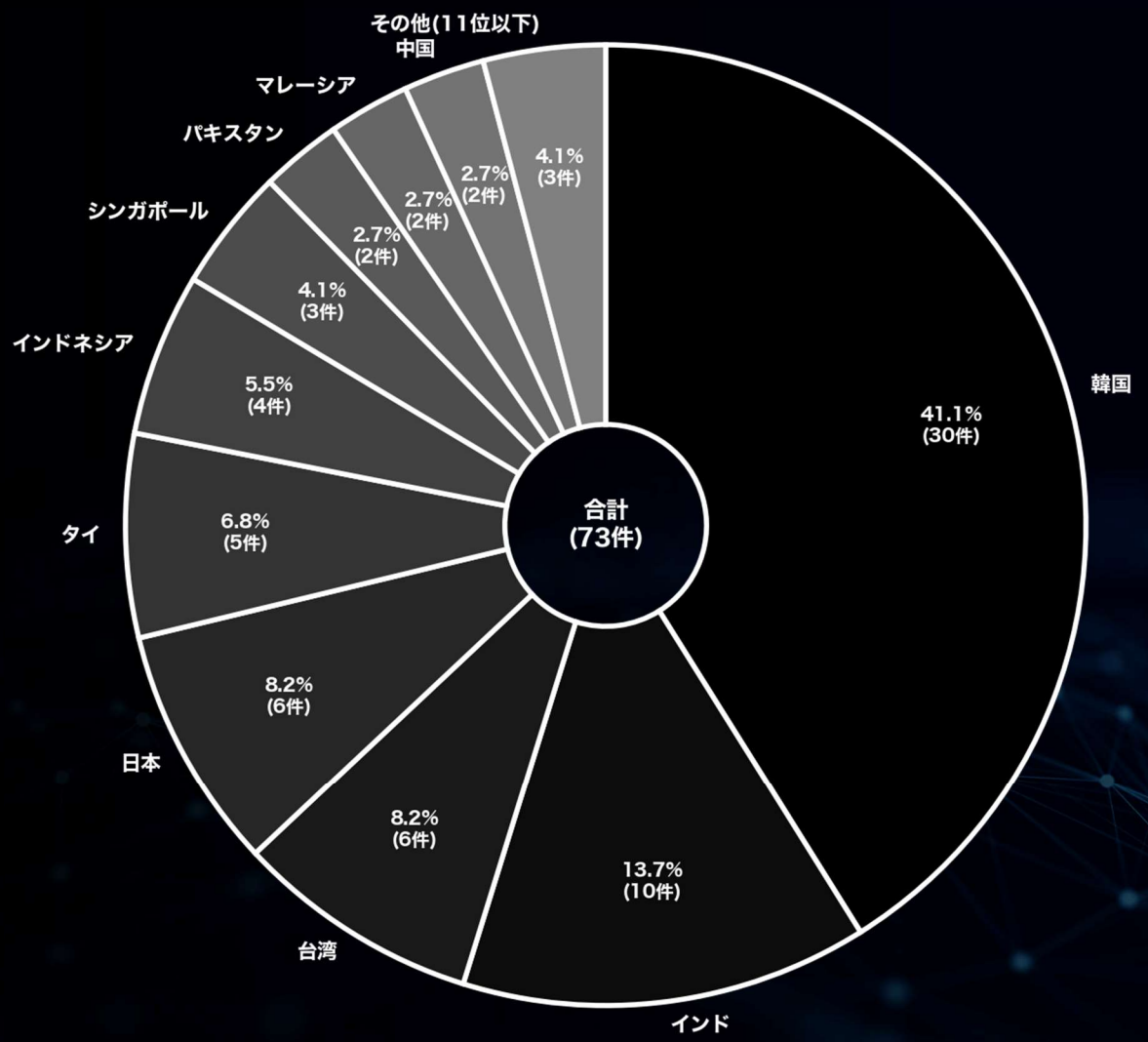
月別内訳 被害国TOP10（アジア）

（2025年 9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)
韓国	30	41.1	+ 25
インド	10	13.7	+ 7
台湾	6	8.2	+ 1
日本	6	8.2	- 5
タイ	5	6.8	+ 1
インドネシア	4	5.5	+ 2
シンガポール	3	4.1	- 2
パキスタン	2	2.7	+ 2
マレーシア	2	2.7	± 0
中国	2	2.7	+ 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

業種 月別統計
（全世界） （過去3ヶ月分）

2025

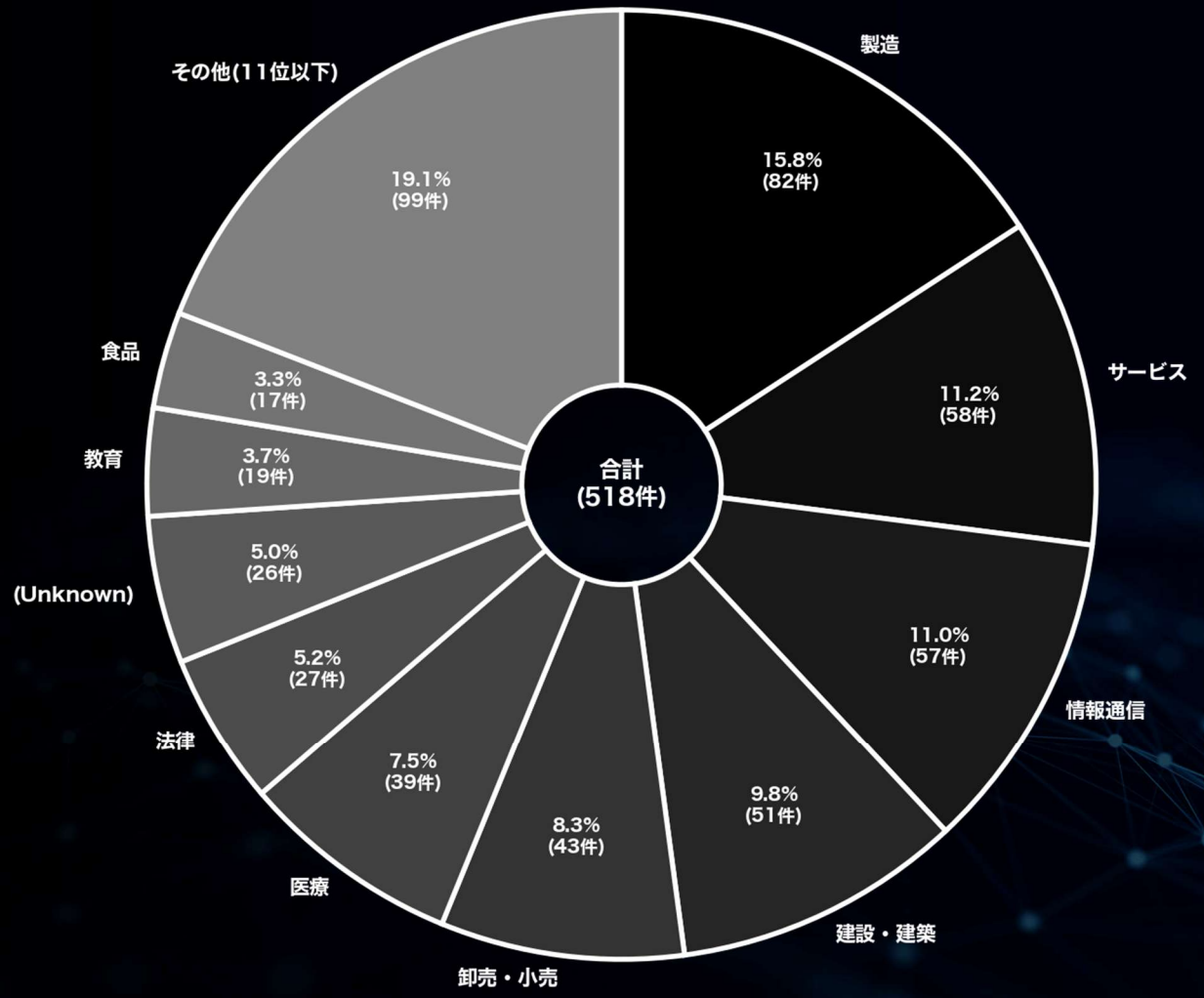
9

月別内訳 業種 TOP10（全世界）
（2025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	82	15.8	+ 18
サービス	58	11.2	- 13
情報通信	57	11.0	+ 15
建設・建築	51	9.8	+ 17
卸売・小売	43	8.3	+ 17
医療	39	7.5	- 7
法律	27	5.2	+ 7
(Unknown)	26	5.0	+ 13
教育	19	3.7	+ 2
食品	17	3.3	+ 10

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



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

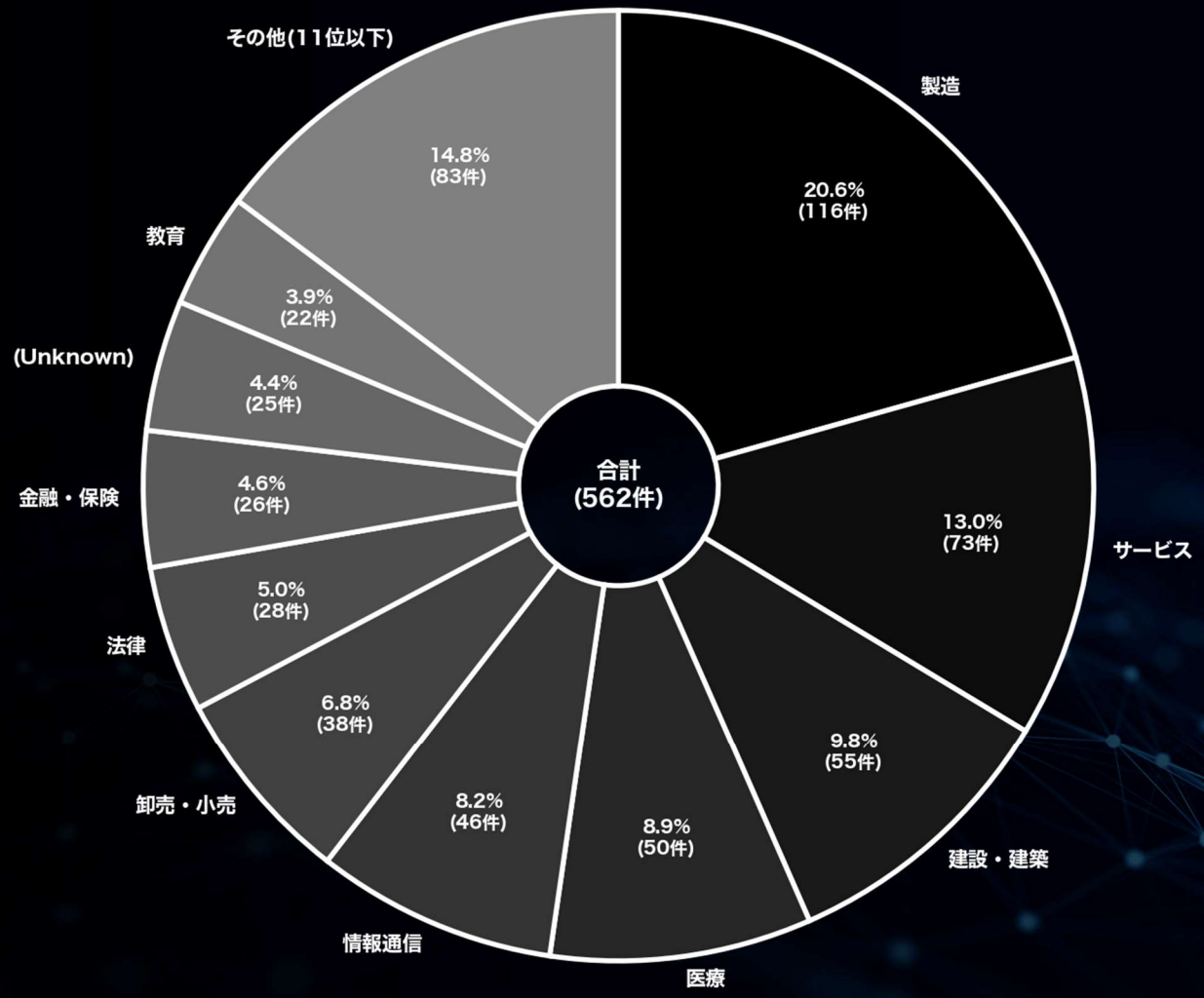
月別内訳 業種 TOP10（全世界）

（2025年 8 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	20.6	+ 34
サービス	73	13.0	+ 15
建設・建築	55	9.8	+ 4
医療	50	8.9	+ 11
情報通信	46	8.2	- 11
卸売・小売	38	6.8	- 5
法律	28	5.0	+ 1
金融・保険	26	4.6	+ 10
(Unknown)	25	4.4	- 1
教育	22	3.9	+ 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）



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

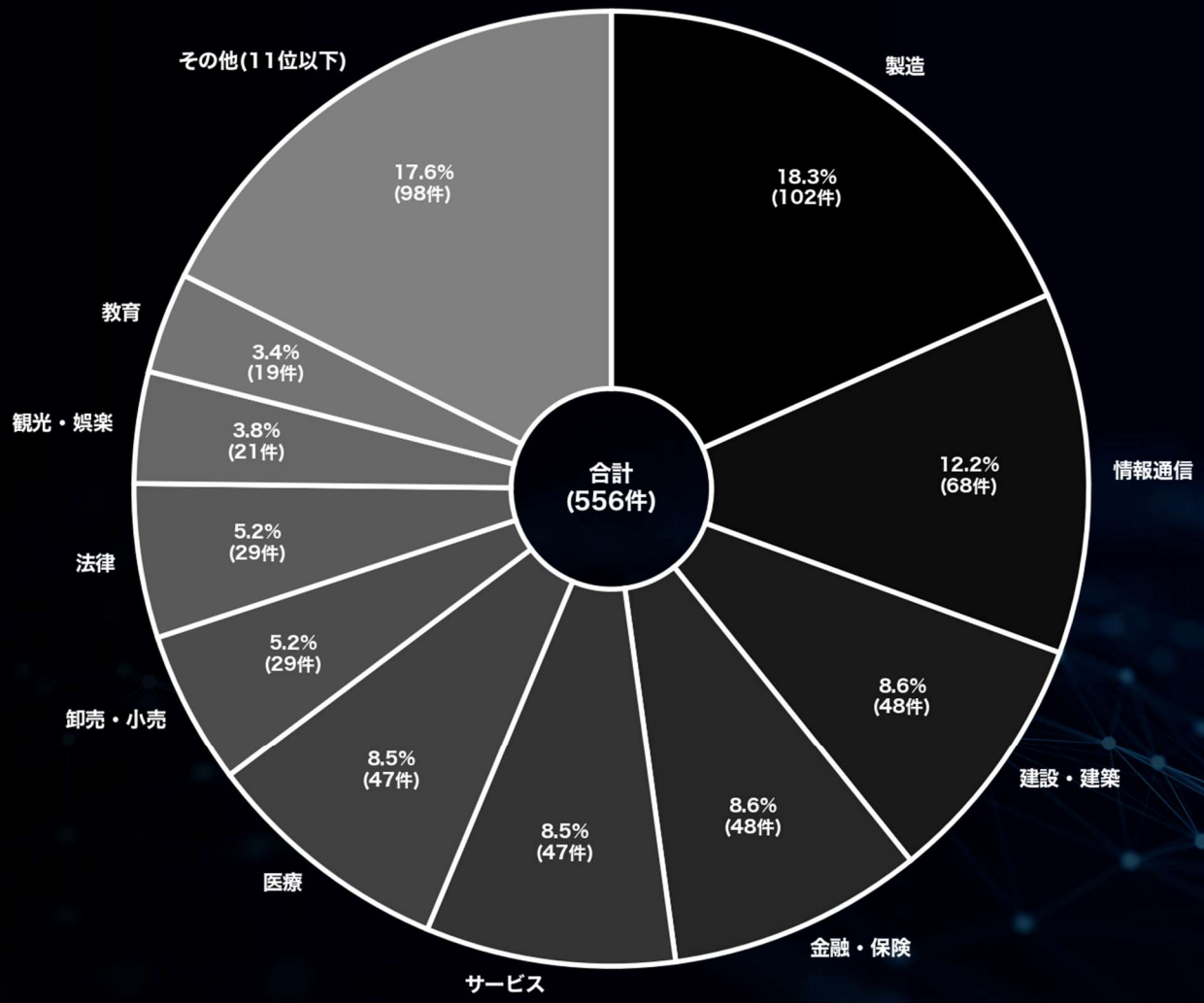
月別内訳 業種 TOP10（全世界）

（2025年 9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	102	18.3	- 14
情報通信	68	12.2	+ 22
建設・建築	48	8.6	- 7
金融・保険	48	8.6	+ 22
サービス	47	8.5	- 26
医療	47	8.5	- 3
卸売・小売	29	5.2	- 9
法律	29	5.2	+ 1
観光・娯楽	21	3.8	+ 6
教育	19	3.4	- 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）



※ 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）

2025

9

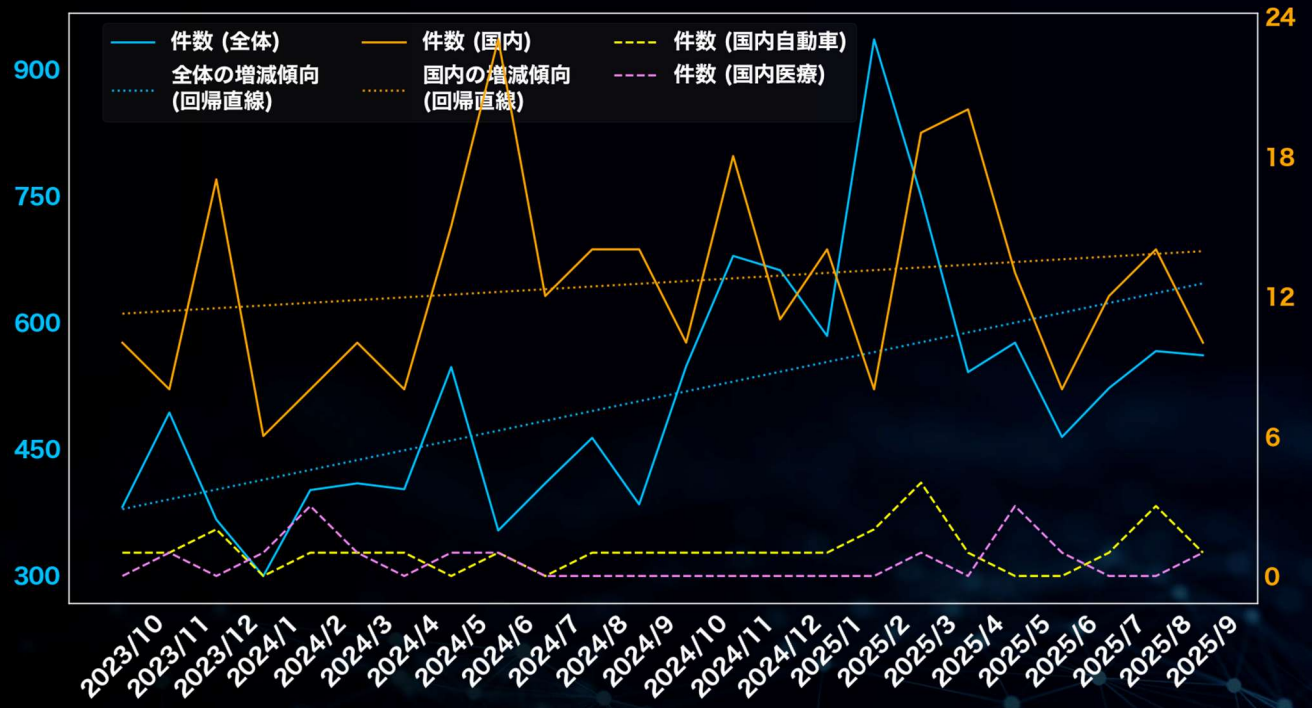
被害数の推移（全世界及び国内）
（過去2年間／2023年10月～2025年9月）

※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)
2023/10	380	10	1	0
2023/11	492	8	1	1
2023/12	365	17	2	0
2024/1	298	6	0	1
2024/2	400	8	1	3
2024/3	408	10	1	1
2024/4	401	8	1	0
2024/5	546	15	0	1
2024/6	352	23	1	1
2024/7	408	12	0	0
2024/8	462	14	1	0
2024/9	383	14	1	0
2024/10	547	10	1	0
2024/11	678	18	1	0
2024/12	661	11	1	0
2025/1	583	14	1	0
2025/2	935	8	2	0
2025/3	749	19	4	1
2025/4	540	20	1	0
2025/5	575	13	0	3
2025/6	463	8	0	1
2025/7	521	12	1	0
2025/8	565	14	3	0
2025/9	560	10	1	1
合計	12272	302	26	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

資本金別 月別統計
（国内）

2025

9

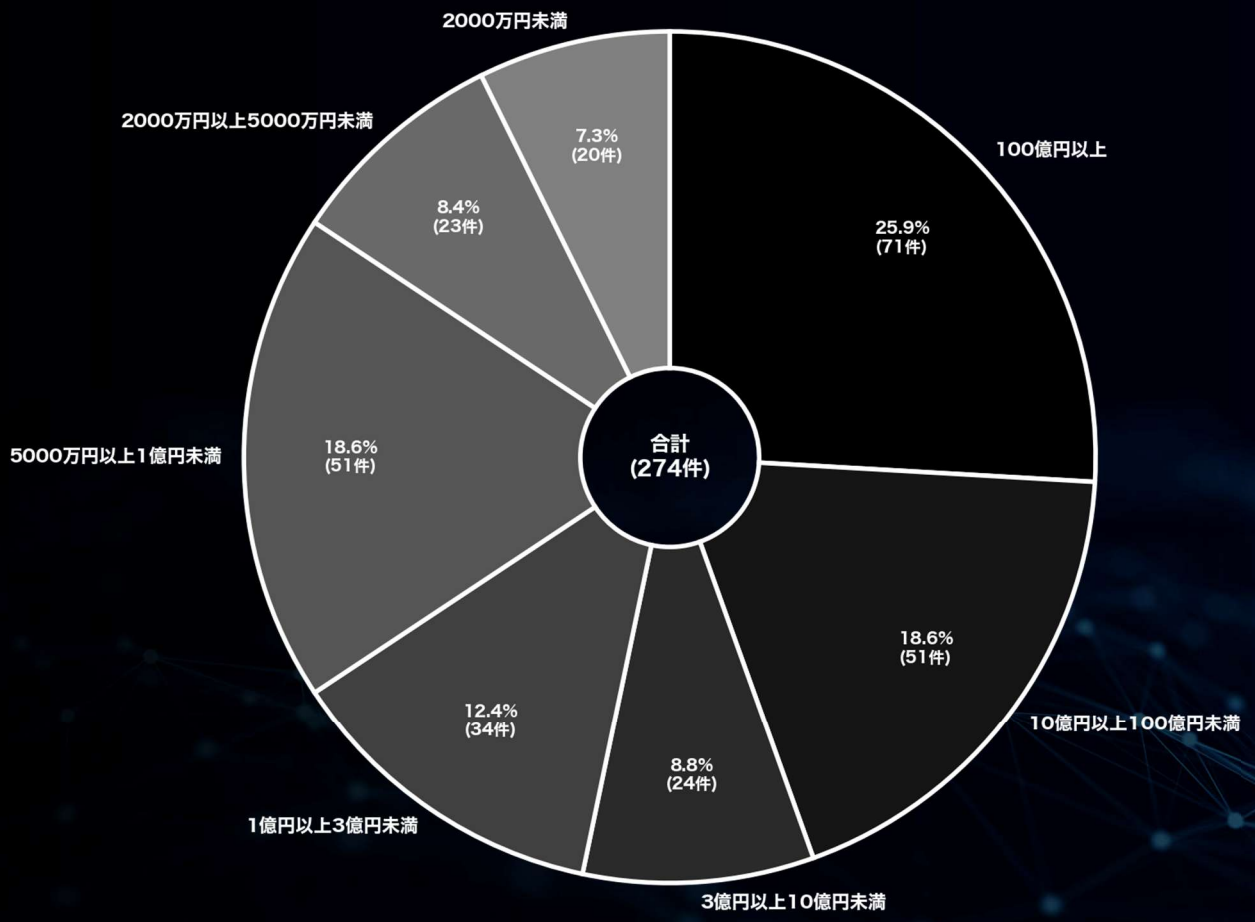
月別内訳 資本金別（国内）
（過去2年間／2023年10月～2025年9月）

※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	71	25.9
10億円以上100億円未満	51	18.6
3億円以上10億円未満	24	8.8
1億円以上3億円未満	34	12.4
5000万円以上1億円未満	51	18.6
2000万円以上5000万円未満	23	8.4
2000万円未満	20	7.3

中小企業に関する詳細な分析は
本レポート「中小企業における被害分析」を参照

▼ランサムウェア攻撃を受けた日本関連組織の規模（資本金）



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

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

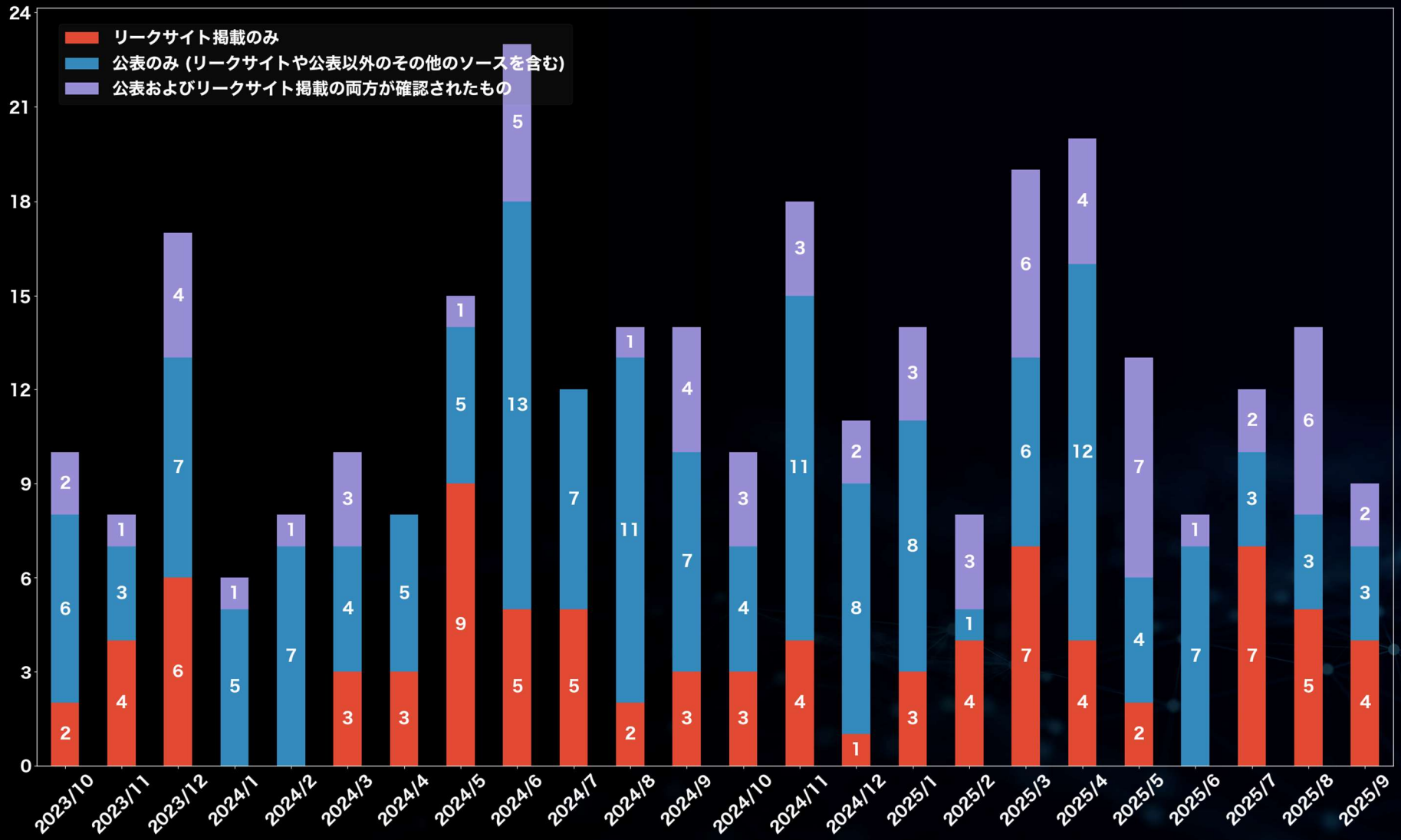
公表と暴露に関する統計
（国内）

2025

9

公表割合 月別内訳（国内）
（過去2年間／2023年10月～2025年9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

2025

9

公となった国内被害組織概要一覧（国内）
（過去1年間／2024年10月～2025年9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
2024/10	Qilin (Agenda)	空調機器メーカー(海外拠点)
2024/10	Underground	大手電機メーカー
2024/10	(Unknown)	公益財団法人
2024/10	SARCOMA	総合物流事業者
2024/10	MEOW	工具メーカー
2024/10	RansomHub	大手飲食サービス会社
2024/10	RansomHub	自動車部品メーカー
2024/10	(Unknown)	専門学校
2024/10	(Unknown)	総合商社
2024/10	(Unknown)	不動産会社
2024/11	KILLSEC	総合ゴム製品メーカー(海外拠点)
2024/11	(Unknown)	ソフトウエアメーカー
2024/11	(Unknown)	専門商社
2024/11	BianLian	大手スポーツ用品メーカー(海外拠点)
2024/11	BlackSuit	電子部品メーカー(海外拠点)
2024/11	(Unknown)	一般社団法人
2024/11	MEOW	電子部品メーカー(海外拠点)
2024/11	(Unknown)	家具メーカー
2024/11	(Unknown)	保険代理店
2024/11	SAFEPAY	建設会社
2024/11	(Unknown)	食品メーカー
2024/11	Argonauts	化学品メーカー
2024/11	(Unknown)	総合電機メーカー(海外拠点)
2024/11	(Unknown)	工作機械メーカー(海外拠点)
2024/11	(Unknown)	イベント企画制作会社
2024/11	(Unknown)	イベント企画制作会社

被害月	攻撃グループ	業種概要
2024/11	BlackSuit	自動車部品メーカー(海外拠点)
2024/11	(Unknown)	水処理システムメーカー(海外拠点)
2024/12	(Unknown)	公益財団法人
2024/12	8BASE	農業機械メーカー
2024/12	PLAY	大手食品メーカー(海外拠点)
2024/12	(Unknown)	タンカー運送会社
2024/12	(Unknown)	鉄鋼加工メーカー
2024/12	(Unknown)	情報通信サービス会社
2024/12	(Unknown)	工業機械メーカー
2024/12	(Unknown)	教育委員会
2024/12	CL0P (CLOP)	大手食品メーカー(海外拠点)
2024/12	(Unknown)	印刷サービス会社
2024/12	(Unknown)	産業・建設機械メーカー
2025/1	(Unknown)	乳製品メーカー
2025/1	Hunters International	化学触媒メーカー
2025/1	(Unknown)	ソフトウエアメーカー
2025/1	Space Bears	不織布メーカー
2025/1	AKIRA	工業用繊維製品メーカー(海外拠点)
2025/1	Hunters International	大手香料メーカー(海外拠点)
2025/1	LYNX	輸入品卸売業(海外拠点)
2025/1	(Unknown)	総合美容商社
2025/1	(Unknown)	テーマパーク運営
2025/1	(Unknown)	保険代理店
2025/1	(Unknown)	報道関連会社
2025/1	(Unknown)	外航海運事業者
2025/1	(Unknown)	フッ素ポリマー製品製造

被害月	攻撃グループ	業種概要
2025/1	Qilin (Agenda)	自動車部品メーカー
2025/2	Qilin (Agenda)	自動車部品メーカー
2025/2	Hunters International	住宅・施設建設
2025/2	FOG	ITサービス会社
2025/2	(Unknown)	保険代理店
2025/2	LYNX	ITサービス会社
2025/2	Cicada3301	システムインテグレーター
2025/2	Hunters International	緑化・造園業者
2025/2	CL0P (CLOP)	自動車部品メーカー
2025/3	(Unknown)	粘着テープ製造(海外拠点)
2025/3	Qilin (Agenda)	医療機関
2025/3	RansomHub	リビルド品製造
2025/3	(Unknown)	不動産仲介
2025/3	Night Spire	塗料メーカー
2025/3	Qilin (Agenda)	産業用機器メーカー(海外拠点)
2025/3	Night Spire	ボンディングワイヤメーカー(海外拠点)
2025/3	Qilin (Agenda)	自動制御機器製品メーカー(海外拠点)
2025/3	CACTUS	自動車部品メーカー(海外拠点)
2025/3	(Unknown)	流体制御機器（バルブ）製造
2025/3	(Unknown)	ソフトウェア開発
2025/3	Blackout	機器部品メーカー
2025/3	Cicada3301	精密部品メーカー
2025/3	RansomHub	一般機械器具製造業
2025/3	Night Spire	特殊鋼部品メーカー(海外拠点)
2025/3	Night Spire	切削工具メーカー(海外拠点)
2025/3	(Unknown)	百貨店業

（※本ページの表の情報は、日本にフォーカスする関係上、リークサイトに掲載された情報に加えて国内被害組織からの公表や報道から判明した情報も含む）

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

公となった国内被害組織概要一覧（国内）
（過去1年間／2024年10月～2025年9月）

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

被害月	攻撃グループ	業種概要
2025/3	(Unknown)	鉄鋼製品メーカー(海外拠点)
2025/3	KILLSEC	事務機器メーカー(海外拠点)
2025/4	KILLSEC	情報機器メーカー(海外拠点)
2025/4	AKIRA	大手総合印刷・電子材料メーカー(海外拠点)
2025/4	SARCOMA	大手総合化学メーカー(海外拠点)
2025/4	AKIRA	自動化装置メーカ(海外拠点)
2025/4	(Unknown)	総合エンジニアリング企業
2025/4	(Unknown)	トラック・バス等販売
2025/4	Night Spire	センサ・電子部品メーカー
2025/4	(Unknown)	総合建設業
2025/4	(Unknown)	総合物流事業者
2025/4	Qilin (Agenda)	精密機械製造(海外拠点)
2025/4	(Unknown)	エネルギーコンサルティング
2025/4	(Unknown)	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

被害月	攻撃グループ	業種概要
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	Space Bears	ゴム製品メーカー(海外拠点)
2025/5	PLAY	通信機器メーカー(海外拠点)
2025/6	(Unknown)	錠前・セキュリティ製品の販売
2025/6	(Unknown)	産業機械メーカー
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)

被害月	攻撃グループ	業種概要
2025/7	DEVMAN 2.0	電子部品メーカー
2025/7	SAFEPAY	パレル用補助材料メーカー
2025/7	(Unknown)	知的財産情報提供
2025/8	(Unknown)	ソフトウェア開発
2025/8	Black Nevas	特許事務所
2025/8	D4RK4RMY	大手金融機関
2025/8	Qilin (Agenda)	プラスチック製品製造業
2025/8	Qilin (Agenda)	自動車部品メーカー(海外拠点)
2025/8	Qilin (Agenda)	業務用食品卸・加工業
2025/8	(Unknown)	農産物加工・流通
2025/8	Warlock	精密機器メーカー(海外拠点)
2025/8	RansomHouse	電池・電子部品メーカー(海外拠点)
2025/8	Qilin (Agenda)	自動車向けデザイン
2025/8	WORLD LEAKS	毛織物メーカー
2025/8	(Unknown)	業務用・産業用加湿器メーカー
2025/8	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)
2025/9	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	J GROUP	大手商社(海外拠点)

（※本ページの表の情報は、日本にフォーカスする関係上、リークサイトに掲載された情報に加えて国内被害組織からの公表や報道から判明した情報も含む）

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

公となった国内被害組織における拠点割合（国内）

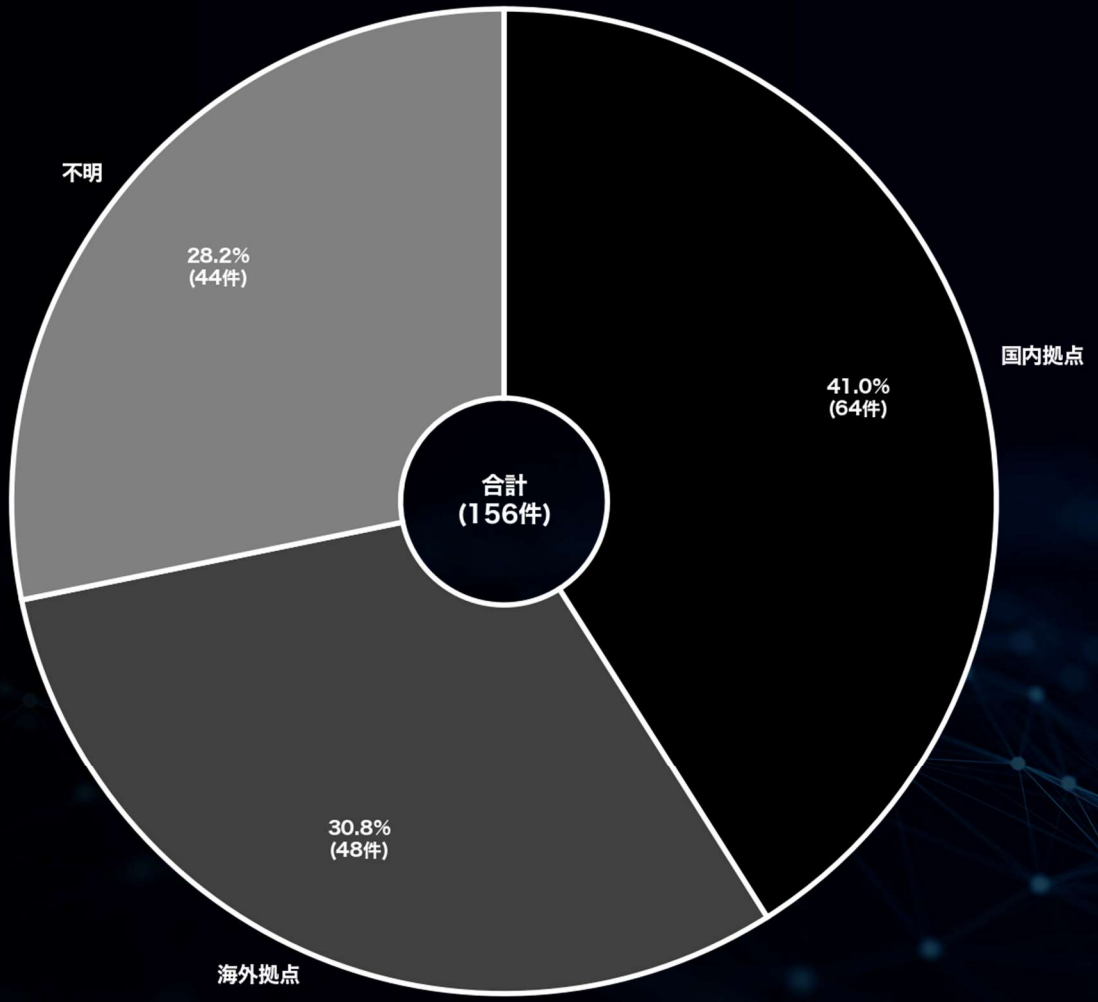
（過去1年間／2024年10月～2025年9月）

（※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	64	41.0
海外拠点	48	30.8
不明	44	28.2

▼ランサムウェア攻撃を受けた日本関連組織の拠点別割合



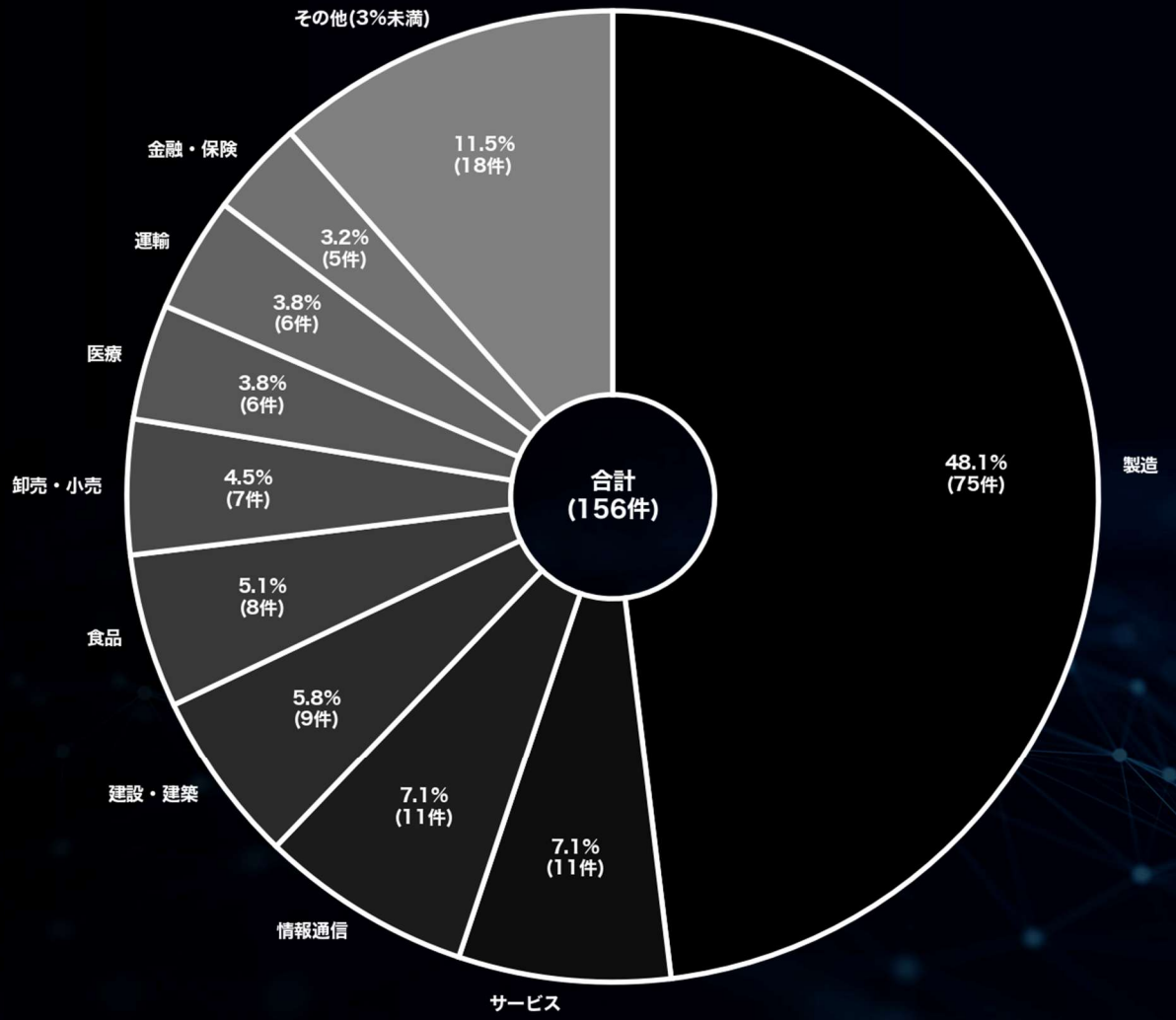
（※本ページの表／グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している）

※ 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／2024年10月～2025年9月）

業種	件数	割合(%)
製造	75	48.1
サービス	11	7.1
情報通信	11	7.1
建設・建築	9	5.8
食品	8	5.1
卸売・小売	7	4.5
医療	6	3.8
運輸	6	3.8
金融・保険	5	3.2
その他(3%未満)	18	11.5

▼ランサムウェア攻撃を受けた日本関連組織の業種別割合



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

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

中小企業における被害分析
（国内）

2025
9

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

月別内訳 資本金別（国内-中小企業）

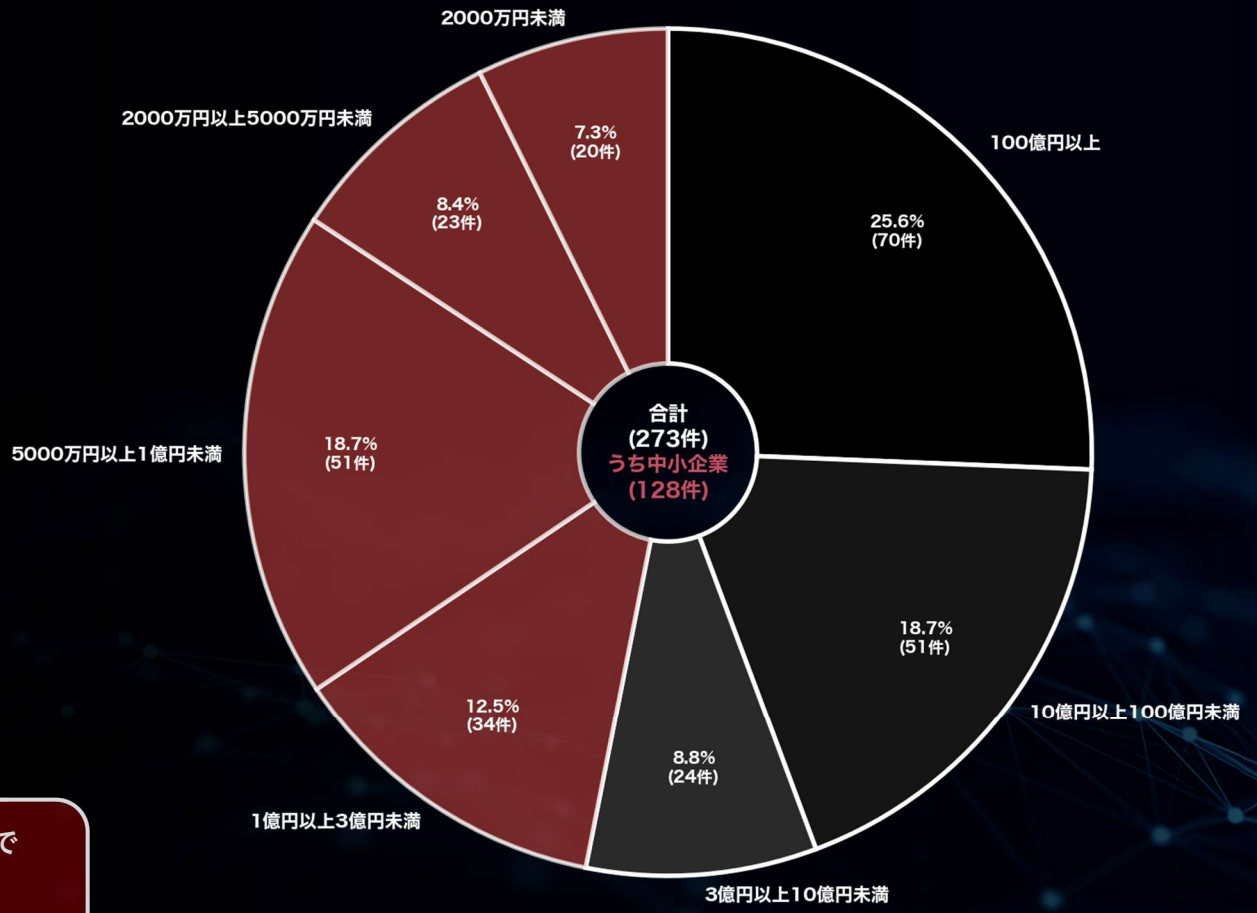
（過去2年間／2023年10月～2025年9月）

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	70	25.6
10億円以上100億円未満	51	18.7
3億円以上10億円未満	24	8.8
1億円以上3億円未満	34	12.5
5000万円以上1億円未満	51	18.7
2000万円以上5000万円未満	23	8.4
2000万円未満	20	7.3

▼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128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）

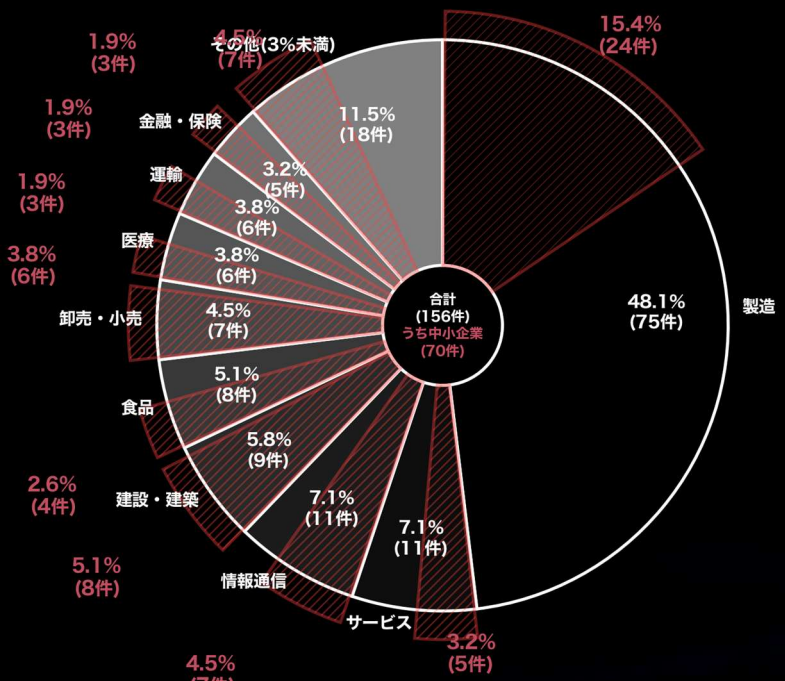
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

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／2024年10月～2025年9月）

赤色は中小企業を示す

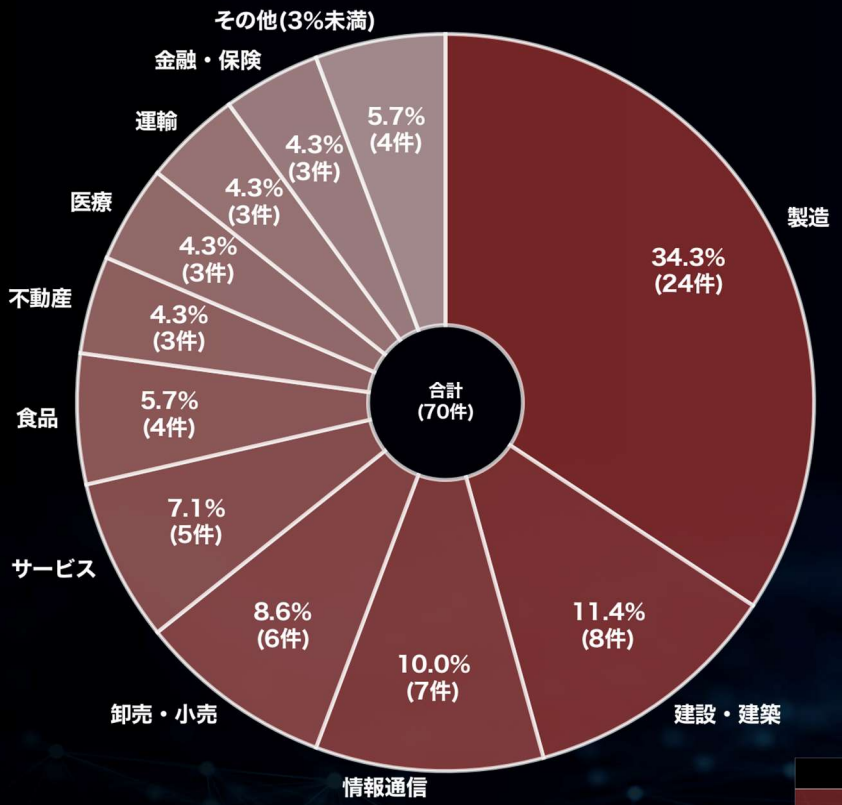
▼全体割合



※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	75 (24)	48.1 (15.4)
サービス	11 (5)	7.1 (3.2)
情報通信	11 (7)	7.1 (4.5)
建設・建築	9 (8)	5.8 (5.1)
食品	8 (4)	5.1 (2.6)
卸売・小売	7 (6)	4.5 (3.8)
医療	6 (3)	3.8 (1.9)
運輸	6 (3)	3.8 (1.9)
金融・保険	5 (3)	3.2 (1.9)
その他(3%未満)	18 (7)	11.5 (4.5)

▼中小企業のみの割合



業種	件数	割合(%)
製造	24	34.3
建設・建築	8	11.4
情報通信	7	10.0
卸売・小売	6	8.6
サービス	5	7.1
食品	4	5.7
不動産	3	4.3
医療	3	4.3
運輸	3	4.3
金融・保険	3	4.3
その他(3%未満)	4	5.7

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）

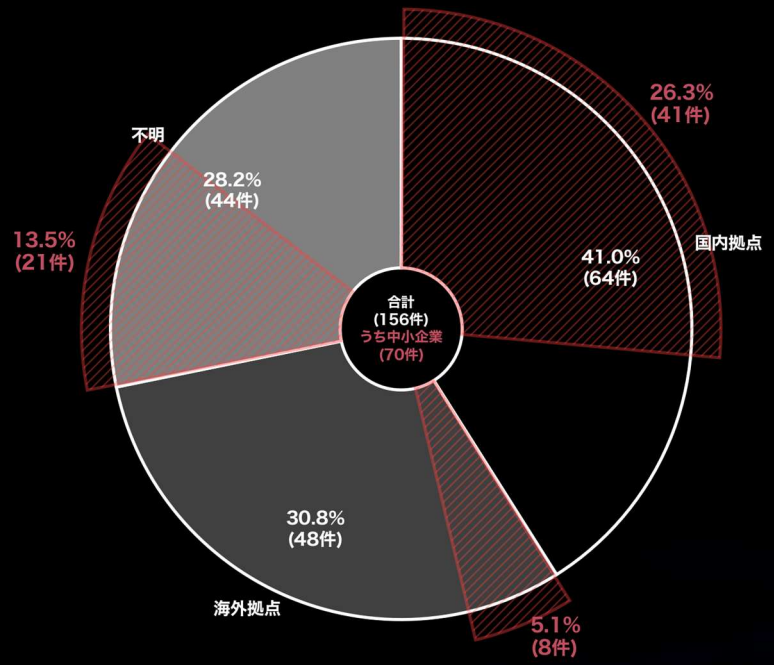
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

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）

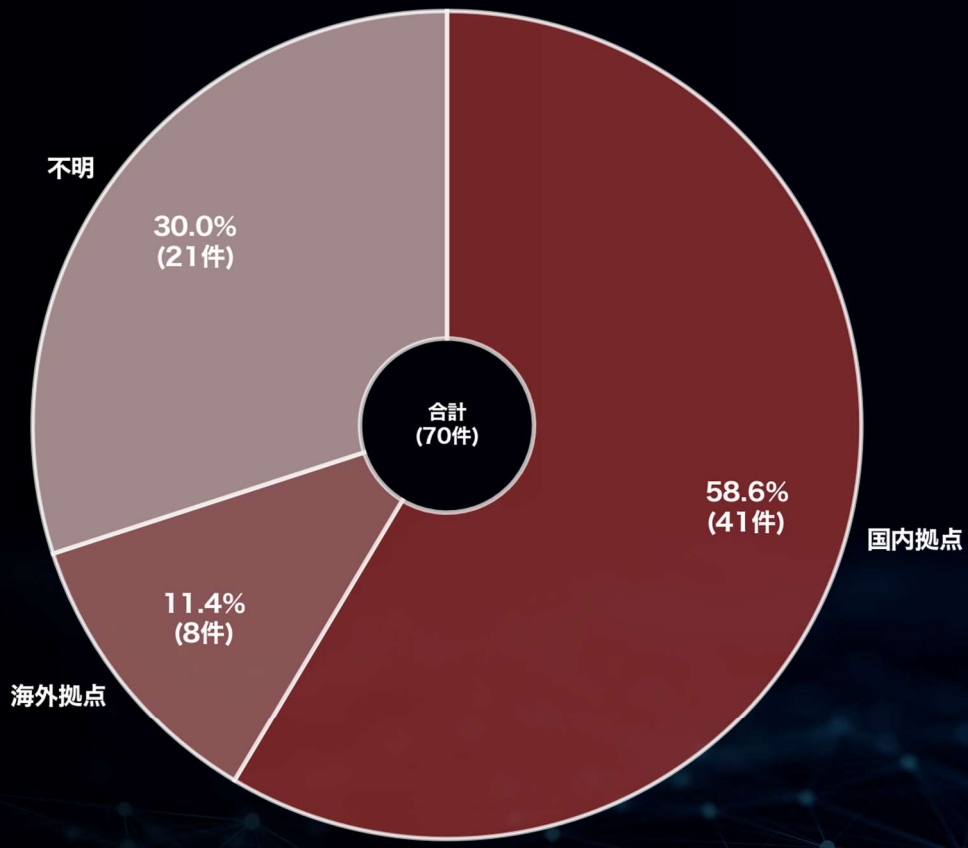
（過去1年間／2024年10月～2025年9月）

赤色は中小企業を示す

▼全体割合



▼中小企業のみの割合



※
「国内拠点」：公表等により、国内拠点における被害事案と判断されるケース数
「海外拠点」：公表等により、海外拠点（支社／関係会社）における被害事案と判断されるケース数
「不明」：上記以外、被害拠点の地域的情報が得られなかったケース数
※各数値の()内の数値は、資本金10億円未満の組織に対する集計結果を示す

拠点	件数 (中小企業)	割合(%)
国内拠点	64 (41)	41.0 (26.3)
海外拠点	48 (8)	30.8 (5.1)
不明	44 (21)	28.2 (13.5)
合計	156 (70)	100 (44.9)

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

※医療や教育、行政機関など資本金が不明な一部の組織については集計から除外

拠点	件数 (中小企業)	割合(%)
国内拠点	41	58.6
海外拠点	8	11.4
不明	21	30.0

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

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

公となった国内被害組織概要一覧（国内-中小企業）

（過去1年間／2024年10月～2025年9月）

赤色は中小企業を示す

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

被害月	攻撃グループ	業種概要
2024/10	Qilin (Agenda)	空調機器メーカー(海外拠点)
2024/10	Underground	大手電機メーカー
2024/10	(Unknown)	公益財団法人
2024/10	SARCOMA	総合物流事業者
2024/10	MEOW	工具メーカー
2024/10	RansomHub	大手飲食サービス会社
2024/10	RansomHub	自動車部品メーカー
2024/10	(Unknown)	専門学校
2024/10	(Unknown)	総合商社
2024/10	(Unknown)	不動産会社
2024/11	KILLSEC	総合ゴム製品メーカー(海外拠点)
2024/11	(Unknown)	ソフトウエアメーカー
2024/11	(Unknown)	専門商社
2024/11	BianLian	大手スポーツ用品メーカー(海外拠点)
2024/11	BlackSuit	電子部品メーカー(海外拠点)
2024/11	(Unknown)	一般社団法人
2024/11	MEOW	電子部品メーカー(海外拠点)
2024/11	(Unknown)	家具メーカー
2024/11	(Unknown)	保険代理店
2024/11	SAFEPAY	建設会社
2024/11	(Unknown)	食品メーカー
2024/11	Argonauts	化学品メーカー
2024/11	(Unknown)	総合電機メーカー(海外拠点)
2024/11	(Unknown)	工作機械メーカー(海外拠点)
2024/11	(Unknown)	イベント企画制作会社
2024/11	(Unknown)	イベント企画制作会社

被害月	攻撃グループ	業種概要
2024/11	BlackSuit	自動車部品メーカー(海外拠点)
2024/11	(Unknown)	水処理システムメーカー(海外拠点)
2024/12	(Unknown)	公益財団法人
2024/12	8BASE	農業機械メーカー
2024/12	PLAY	大手食品メーカー(海外拠点)
2024/12	(Unknown)	タンカー運送会社
2024/12	(Unknown)	鉄鋼加工メーカー
2024/12	(Unknown)	情報通信サービス会社
2024/12	(Unknown)	工業機械メーカー
2024/12	(Unknown)	教育委員会
2024/12	CL0P (CLOP)	大手食品メーカー(海外拠点)
2024/12	(Unknown)	印刷サービス会社
2024/12	(Unknown)	産業・建設機械メーカー
2025/1	(Unknown)	乳製品メーカー
2025/1	Hunters International	化学触媒メーカー
2025/1	(Unknown)	ソフトウエアメーカー
2025/1	Space Bears	不織布メーカー
2025/1	AKIRA	工業用繊維製品メーカー(海外拠点)
2025/1	Hunters International	大手香料メーカー(海外拠点)
2025/1	LYNX	輸入品卸売業(海外拠点)
2025/1	(Unknown)	総合美容商社
2025/1	(Unknown)	テーマパーク運営
2025/1	(Unknown)	保険代理店
2025/1	(Unknown)	報道関連会社
2025/1	(Unknown)	外航海運事業者
2025/1	(Unknown)	フッ素ポリマー製品製造

被害月	攻撃グループ	業種概要
2025/1	Qilin (Agenda)	自動車部品メーカー
2025/2	Qilin (Agenda)	自動車部品メーカー
2025/2	Hunters International	住宅・施設建設
2025/2	FOG	ITサービス会社
2025/2	(Unknown)	保険代理店
2025/2	LYNX	ITサービス会社
2025/2	Cicada3301	システムインテグレーター
2025/2	Hunters International	緑化・造園業者
2025/2	CL0P (CLOP)	自動車部品メーカー
2025/3	(Unknown)	粘着テープ製造(海外拠点)
2025/3	Qilin (Agenda)	医療機関
2025/3	RansomHub	リビルド品製造
2025/3	(Unknown)	不動産仲介
2025/3	Night Spire	塗料メーカー
2025/3	Qilin (Agenda)	産業用機器メーカー(海外拠点)
2025/3	Night Spire	ボンディングワイヤメーカー(海外拠点)
2025/3	Qilin (Agenda)	自動制御機器製品メーカー(海外拠点)
2025/3	CACTUS	自動車部品メーカー(海外拠点)
2025/3	(Unknown)	流体制御機器（バルブ）製造
2025/3	(Unknown)	ソフトウェア開発
2025/3	Blackout	機器部品メーカー
2025/3	Cicada3301	精密部品メーカー
2025/3	RansomHub	一般機械器具製造業
2025/3	Night Spire	特殊鋼部品メーカー(海外拠点)
2025/3	Night Spire	切削工具メーカー(海外拠点)
2025/3	(Unknown)	百貨店業

（※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／2024年10月～2025年9月）

赤色は中小企業を示す

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

被害月	攻撃グループ	業種概要
2025/3	(Unknown)	鉄鋼製品メーカー(海外拠点)
2025/3	KILLSEC	事務機器メーカー(海外拠点)
2025/4	KILLSEC	情報機器メーカー(海外拠点)
2025/4	AKIRA	大手総合印刷・電子材料メーカー(海外拠点)
2025/4	SARCOMA	大手総合化学メーカー(海外拠点)
2025/4	AKIRA	自動化装置メーカ(海外拠点)
2025/4	(Unknown)	総合エンジニアリング企業
2025/4	(Unknown)	トラック・バス等販売
2025/4	Night Spire	センサ・電子部品メーカー
2025/4	(Unknown)	総合建設業
2025/4	(Unknown)	総合物流事業者
2025/4	Qilin (Agenda)	精密機械製造(海外拠点)
2025/4	(Unknown)	エネルギーコンサルティング
2025/4	(Unknown)	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	Space Bears	ゴム製品メーカー(海外拠点)
2025/5	PLAY	通信機器メーカー(海外拠点)
2025/6	(Unknown)	錠前・セキュリティ製品の販売
2025/6	(Unknown)	産業機械メーカー
2025/6	Qilin (Agenda)	医療機器メーカー(海外拠点)
2025/6	(Unknown)	ポンプ製造業
2025/6	(Unknown)	大手紳士服チェーン
2025/6	(Unknown)	保険事故調査サービス業
2025/6	(Unknown)	設備工事業
2025/6	(Unknown)	建材・住宅・リフォーム・不動産事業
2025/7	Kawa4096	大手保険会社
2025/7	NightSpire	ゴム製品メーカー(海外拠点)
2025/7	Kawa4096	警備サービス業
2025/7	Dire Wolf	電子デバイス製造・販売(海外拠点)
2025/7	(Unknown)	障害福祉サービス業
2025/7	(Unknown)	衛生管理製品・サービス業
2025/7	INC Ransom	高電圧電気機器メーカー(海外拠点)
2025/7	INC Ransom	ファンデーション資材メーカー
2025/7	LYNX	大手食品メーカー(海外拠点)
2025/7	DEVMAN 2.0	電子部品メーカー
2025/7	SAFEPAY	パレル用補助材料メーカー
2025/7	(Unknown)	知的財産情報提供
2025/8	(Unknown)	ソフトウェア開発
2025/8	Black Nevas	特許事務所
2025/8	D4RK4RMY	大手金融機関
2025/8	Qilin (Agenda)	プラスチック製品製造業
2025/8	Qilin (Agenda)	自動車部品メーカー(海外拠点)
2025/8	Qilin (Agenda)	業務用食品卸・加工業
2025/8	(Unknown)	農産物加工・流通
2025/8	Warlock	精密機器メーカー(海外拠点)
2025/8	RansomHouse	電池・電子部品メーカー(海外拠点)
2025/8	Qilin (Agenda)	自動車向けデザイン
2025/8	WORLD LEAKS	毛織物メーカー
2025/8	(Unknown)	業務用・産業用加湿器メーカー
2025/8	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)
2025/9	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	J GROUP	大手商社(海外拠点)

過去1年間、中小企業でのランサムウェア被害が継続的に発生している状況が確認されている。特に近年の国内事例では、取引先企業にまで被害が広がるサプライチェーン攻撃が見受けられる。各企業の事業継続性を守ると同時に、サプライチェーン全体の安全性を高めるため、企業規模に関わらずセキュリティ対策を日々アップデートしていくことが望ましい。

※二次被害を受けた被害組織については本資料に記載していない

（※本ページの表の情報は、日本にフォーカスする関係上、リークサイトに掲載された情報に加えて国内被害組織からの公表や報道から判明した情報も含む）

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

多重被害に関する分析

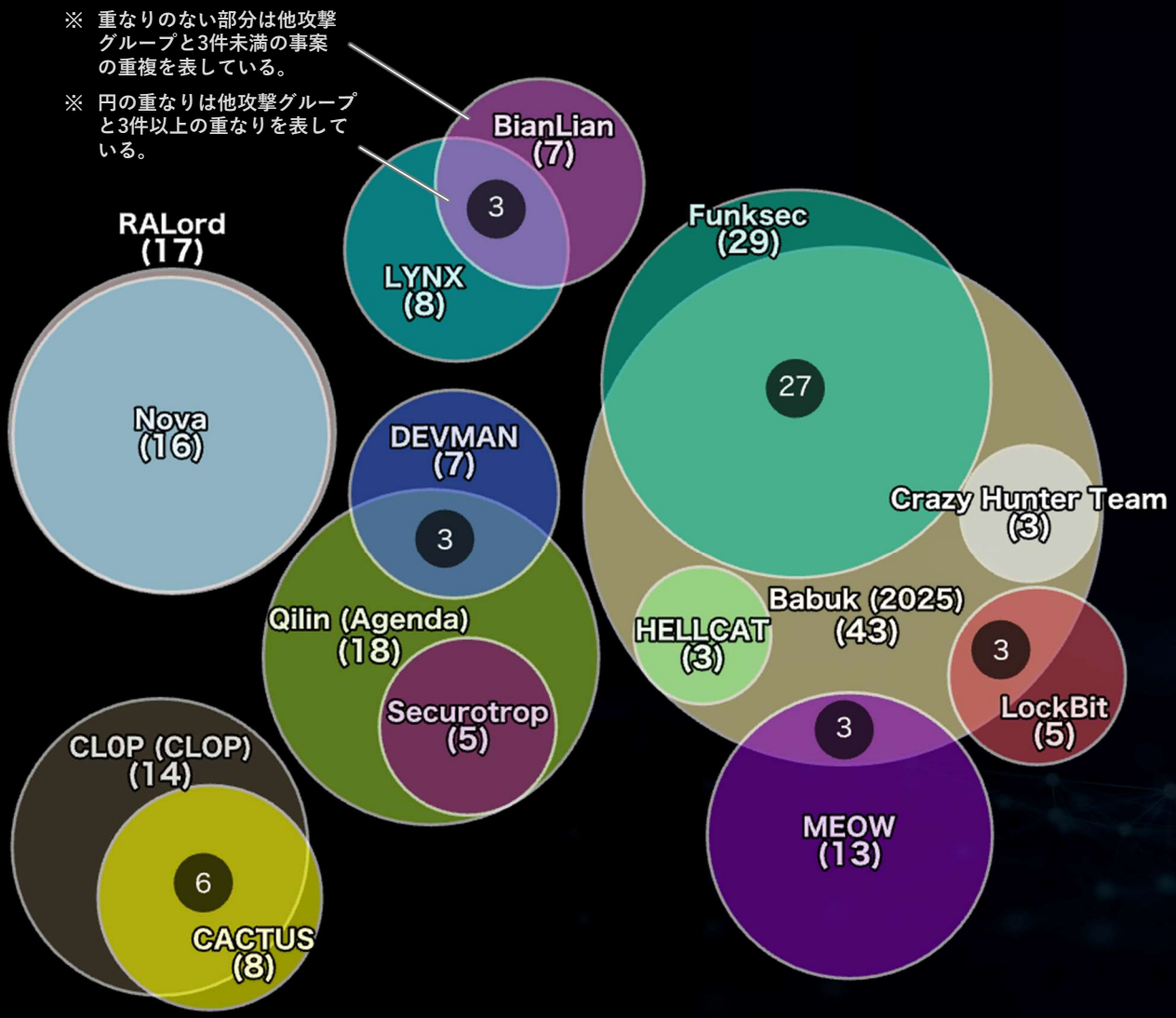
2025

9

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／2024年10月～2025年9月）（累計152件）

※多重被害に遭った組織数の累計



※異なる攻撃グループによるリークサイトへの掲載件数を元に算出

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

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

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

一度盗まれたデータの流用を完全に防ぐことは困難だが、複数回の侵入による多重被害は、インシデント発生時の適切な対応とその後の対策により、防御の可能性を大幅に高めることができる。
ランサムウェア被害発生を想定し、有事の際に冷静な対応ができるよう、対策のための情報の一つとして多重被害の実態を把握しておくことも重要である。

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

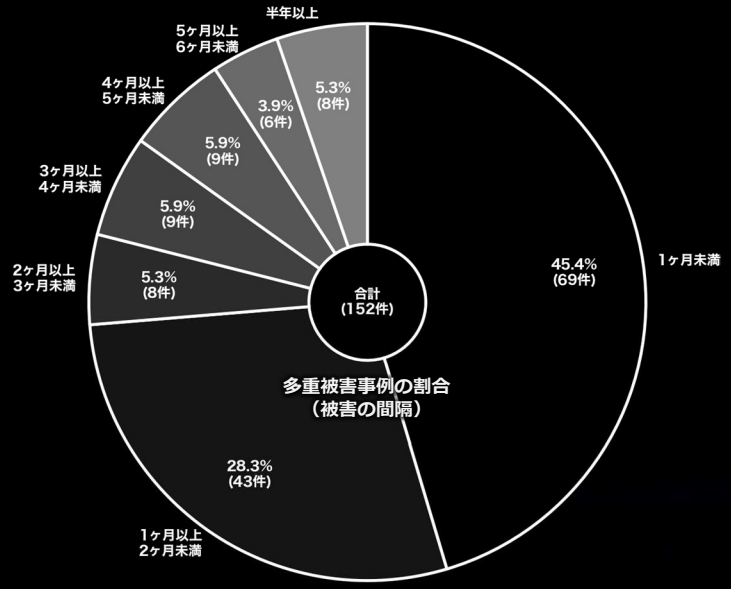
多重被害に遭った被害組織の傾向と分析（全世界）

（過去1年間／2024年10月～2025年9月）

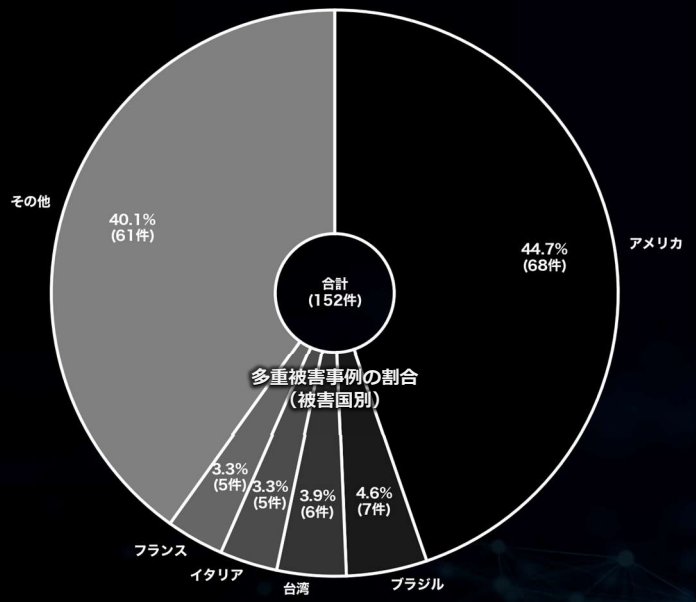
※多重被害：一度ランサムウェア攻撃の被害を受けた組織が異なる時期に異なる攻撃グループのリークサイトに再び掲載されるケース

▼被害の間隔

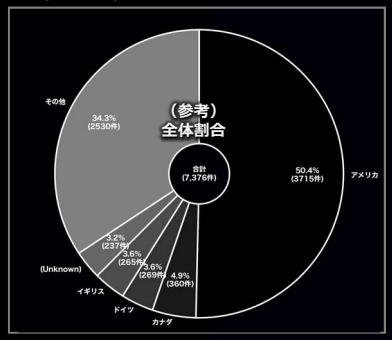
（一度目の被害から二度目の被害までの間隔）



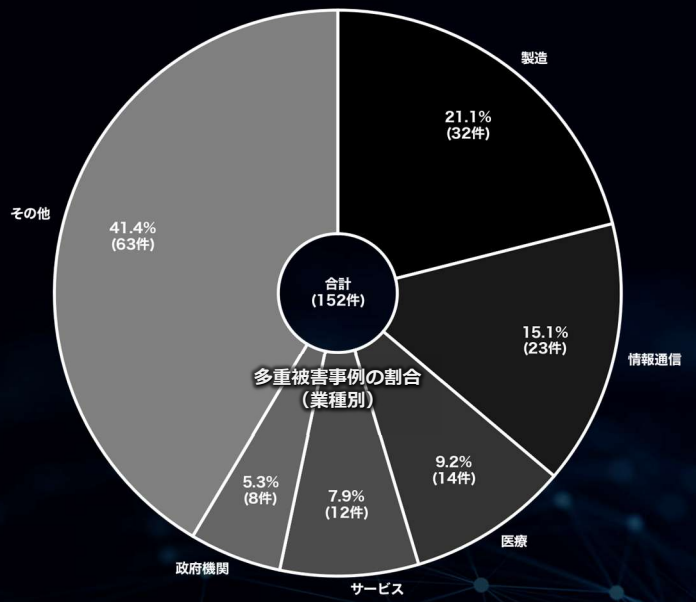
▼被害国別



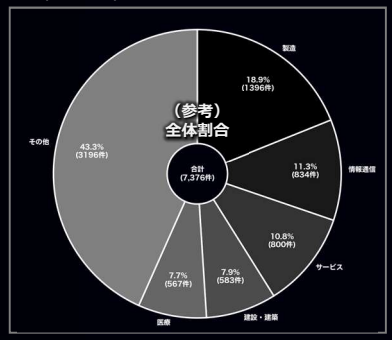
（参考比較）同期間の全データにおける割合



▼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：152件（全体7376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。

※ 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

2025

9

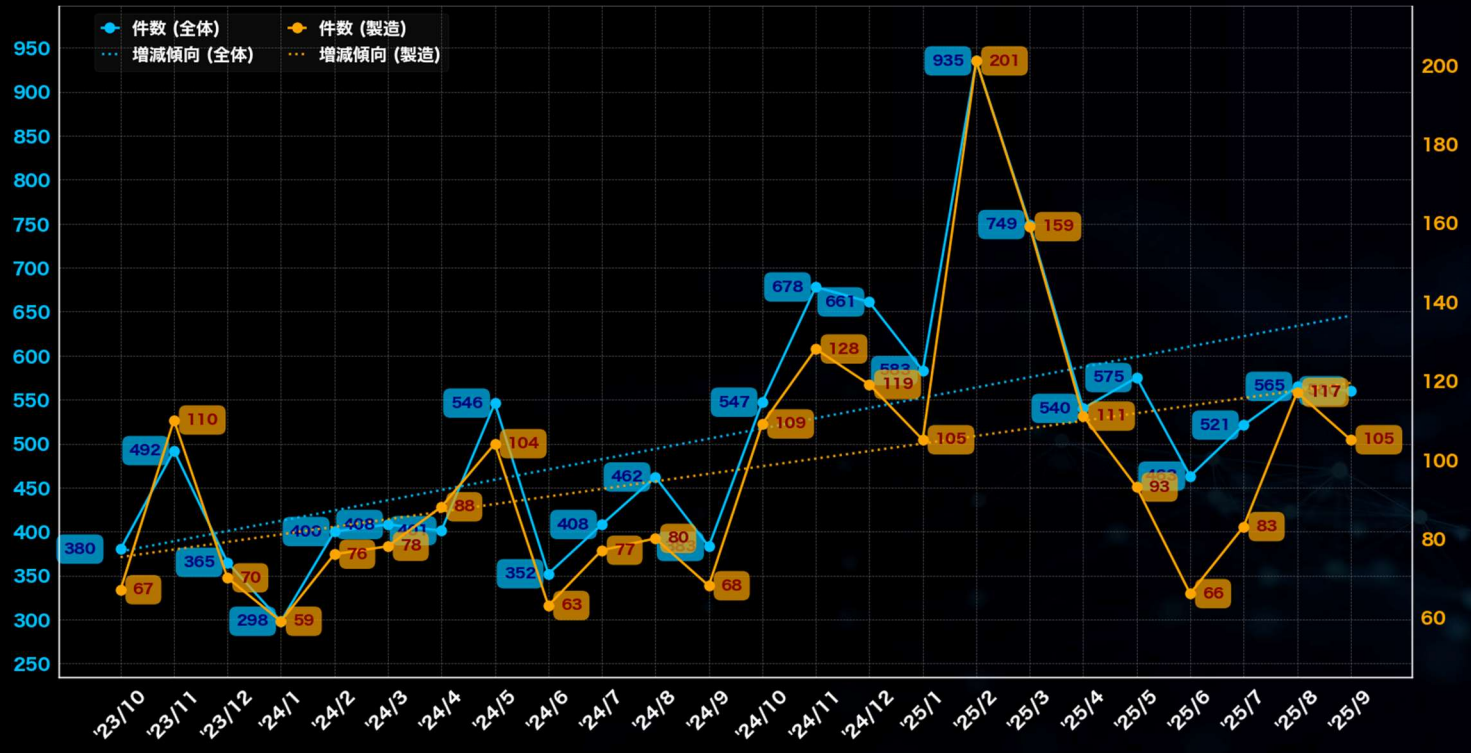
業種に関する分析

（過去2年間のリークサイト掲載上位10業種）

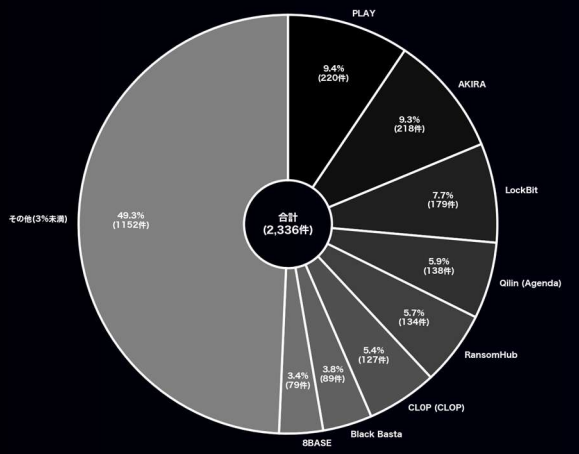
業種に関する分析（全世界）
（過去2年間／2023年10月～2025年9月）

製造

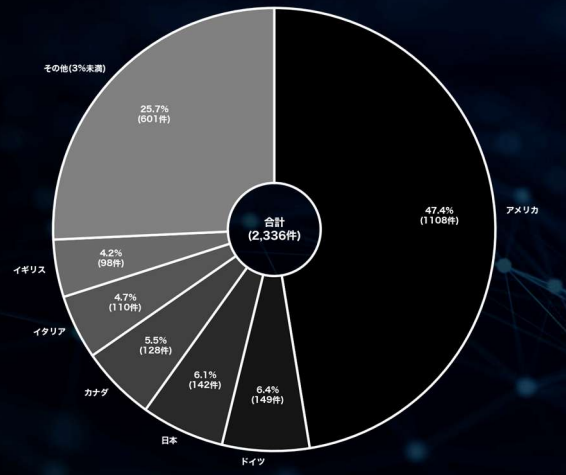
「製造」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、201件の掲載があった。一方、最も少なかった月は2024年1月で、59件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いでドイツと日本がそれぞれ約6%である。攻撃グループについては、少なくとも126のグループが関与しており、特に「PLAY」が220件のリークサイト掲載を実施している。次いで「AKIRA」と「LockBit」がそれぞれ218件と179件の掲載を行っている。製造関連の件数は全体件数に対して高い割合で推移しており、全体件数を引き上げている。全世界的に被害が多い業種であるが、日本関連組織においても多くの被害が出ている状況や、長期に渡り増加傾向にあることから、今後も国内外問わず被害が増加する可能性がある。



▼攻撃グループ別



▼国別



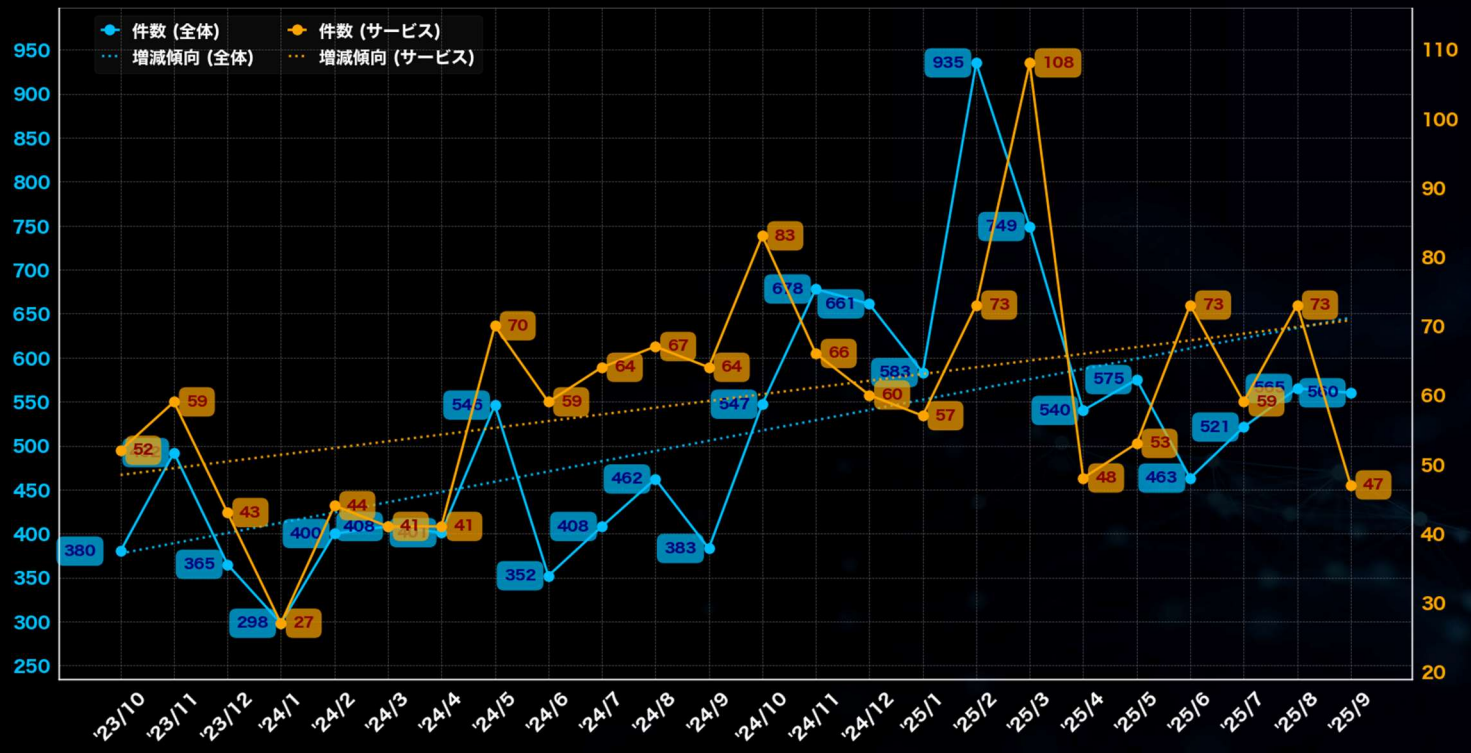
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

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

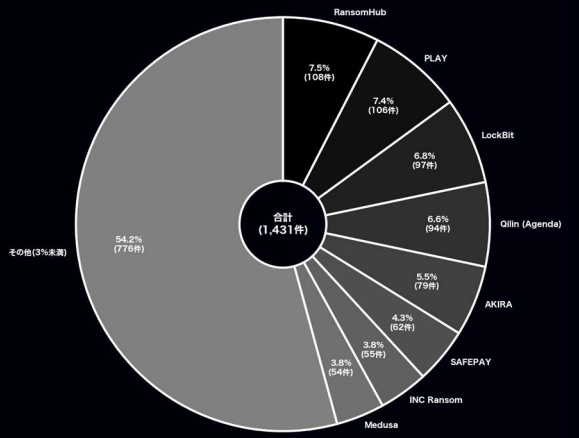
業種に関する分析（全世界）
（過去2年間／2023年10月～2025年9月）

サービス

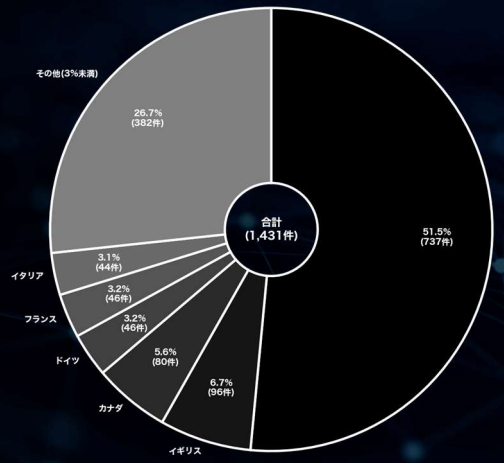
「サービス」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年3月で、108件の掲載があった。一方、最も少なかった月は2024年1月で、27件であった。被害組織の所在国の割合では、アメリカが約52%と最も多く、次いでイギリスとカナダがそれぞれ約7%と約6%である。攻撃グループについては、少なくとも119のグループが関与しており、特に「RansomHub」が108件のリークサイト掲載を実施している。次いで「PLAY」と「LockBit」がそれぞれ106件と97件の掲載を行っている。サービス関連の件数は製造関連と同じく全体件数に対し、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



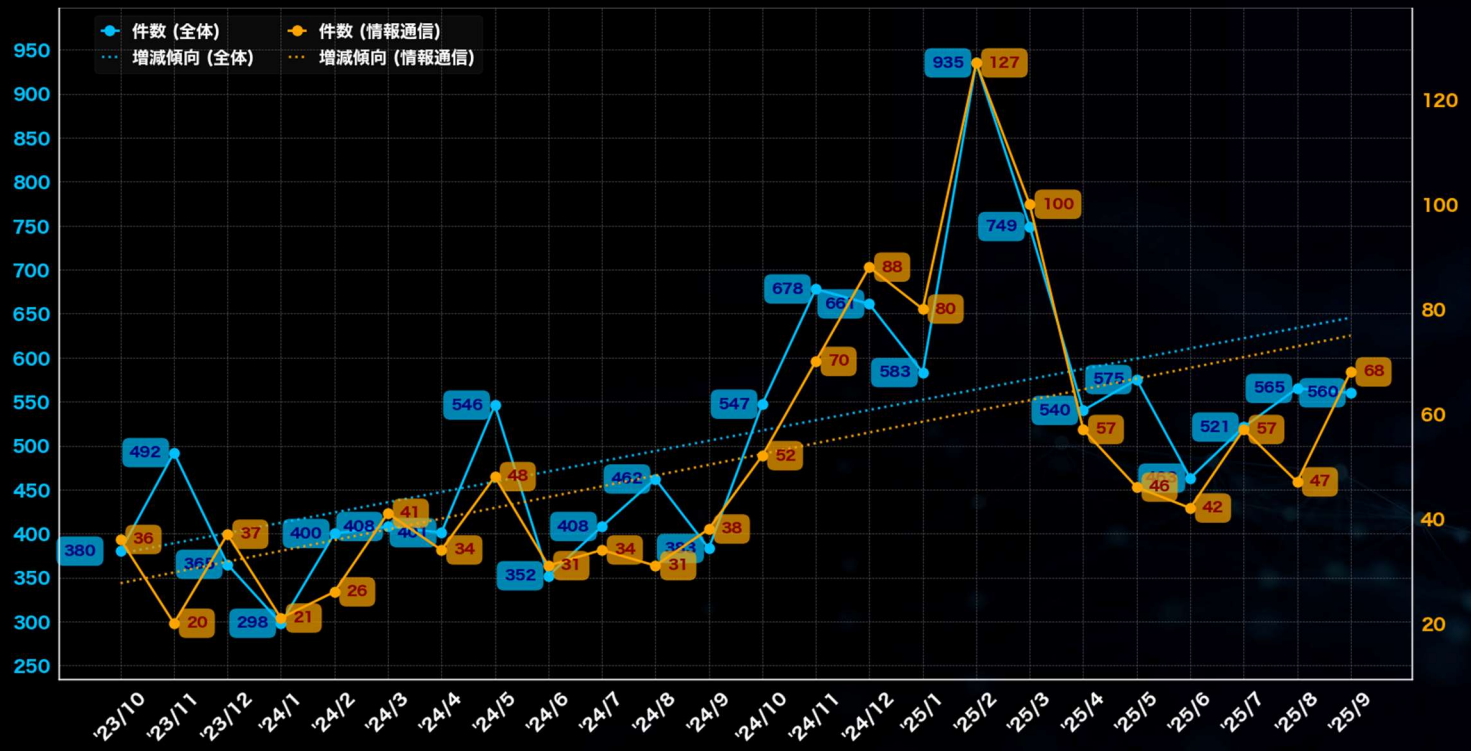
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

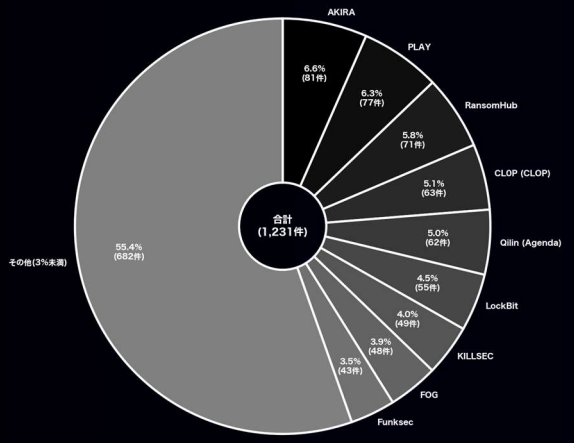
業種に関する分析（全世界）
（過去2年間／2023年10月～2025年9月）

情報通信

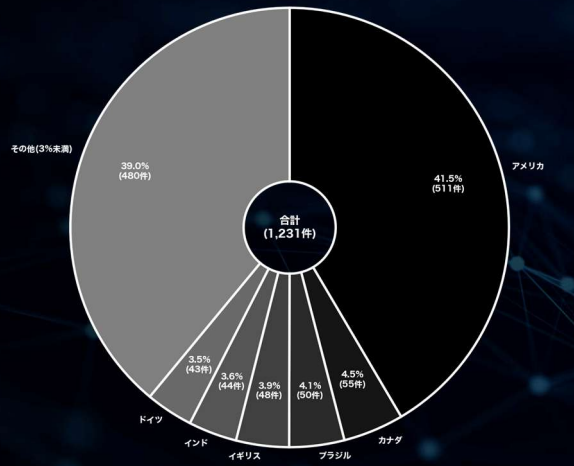
「情報通信」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、127件の掲載があった。一方、最も少なかった月は2023年11月で、20件であった。被害組織の所在国の割合では、アメリカが約42%と最も多く、次いでカナダとブラジルがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも121のグループが関与しており、特に「AKIRA」が81件のリークサイト掲載を実施している。次いで「PLAY」と「RansomHub」とがそれぞれ77件と71件の掲載を行っている。過去2年間におけるリークサイト掲載件数は明確な増加傾向にある。



▼攻撃グループ別



▼国別



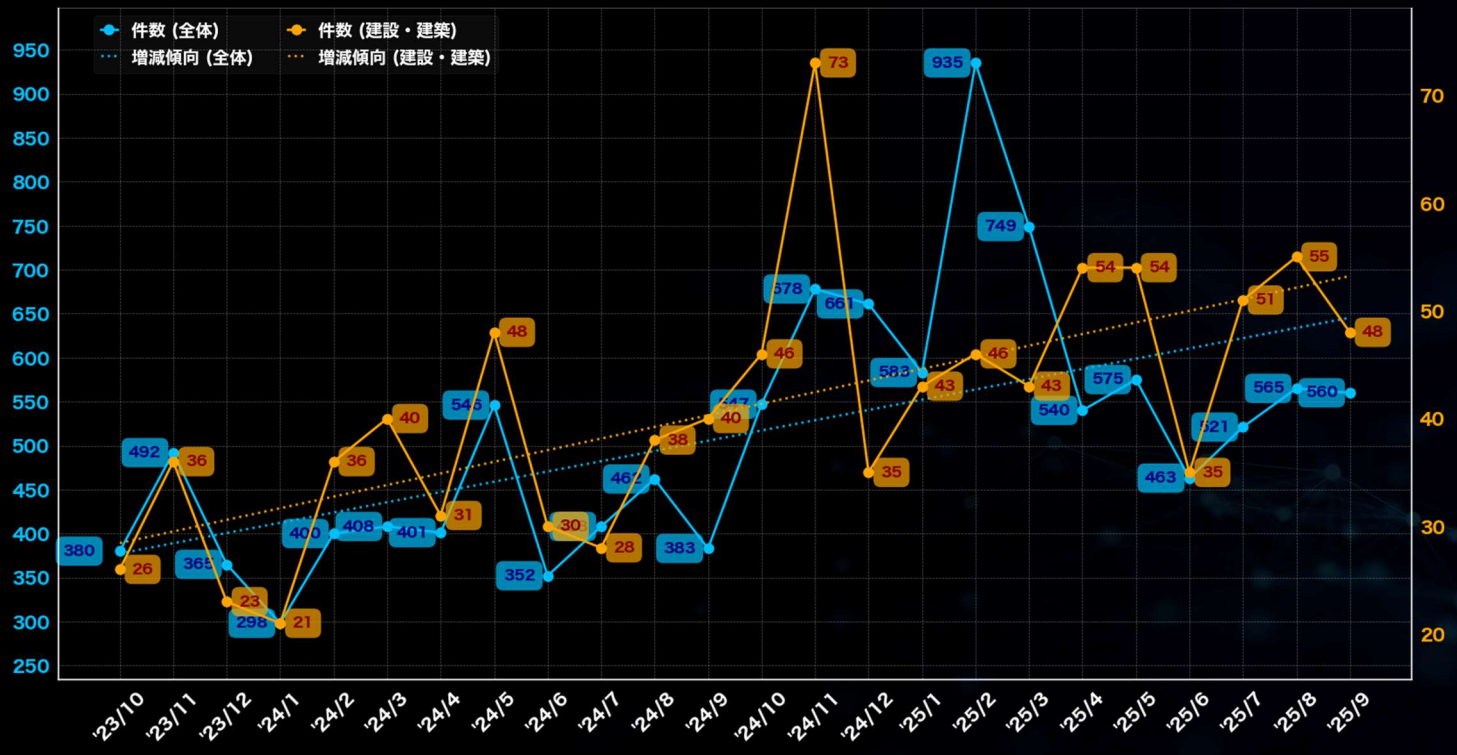
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

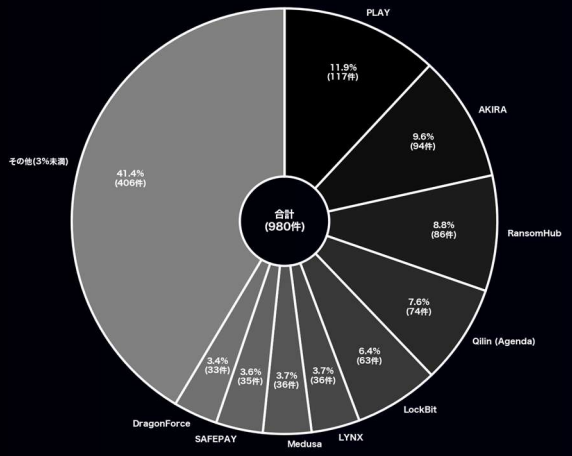
業種に関する分析（全世界）
（過去2年間／2023年10月～2025年9月）

建設・建築

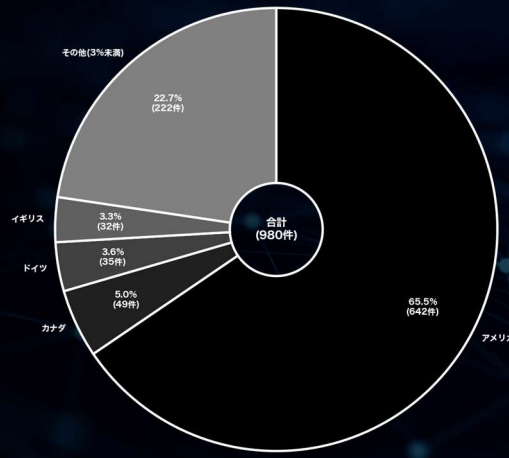
「建設・建築」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2024年11月で、73件の掲載があった。一方、最も少なかった月は2024年1月で、21件であった。被害組織の所在国の割合では、アメリカが約66%と最も多く、次いでカナダとドイツがそれぞれ約5%と約4%である。攻撃グループについては少なくとも93のグループが関与しており、特に「PLAY」が117件のリークサイト掲載を実施している。次いで「AKIRA」と「RansomHub」がそれぞれ94件と86件の掲載を行っている。製造関連などと比べると件数は少ないものの、明確な増加傾向にある。



▼攻撃グループ別



▼国別



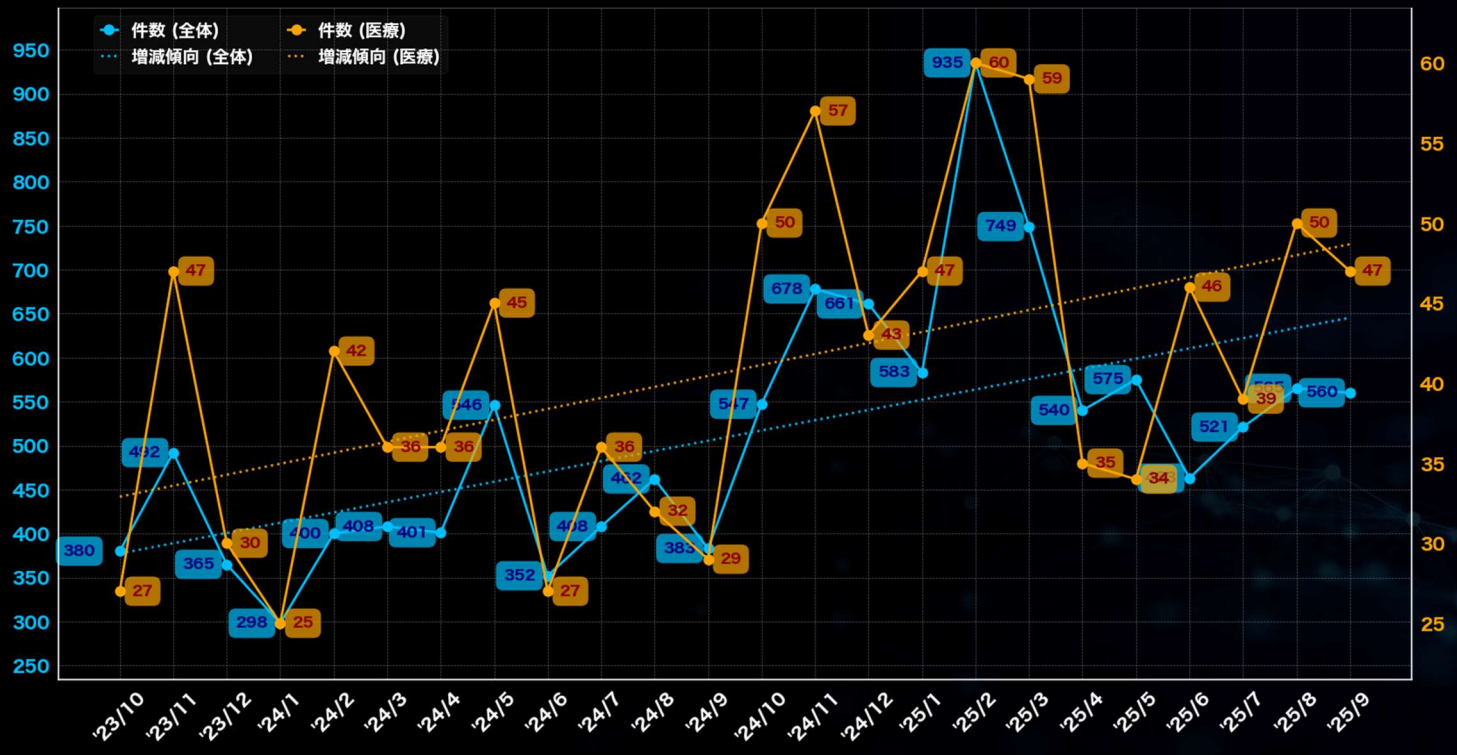
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

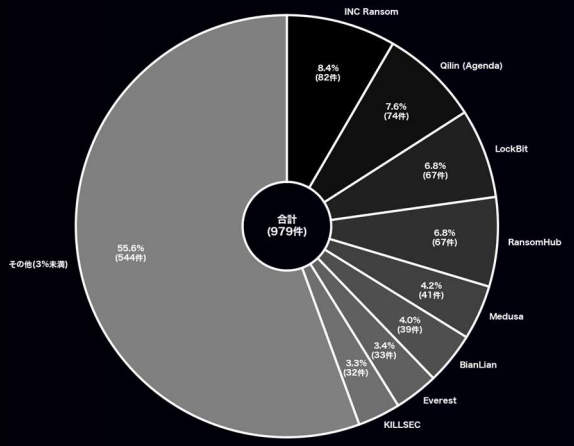
業種に関する分析（全世界）
（過去2年間／2023年10月～2025年9月）

医療

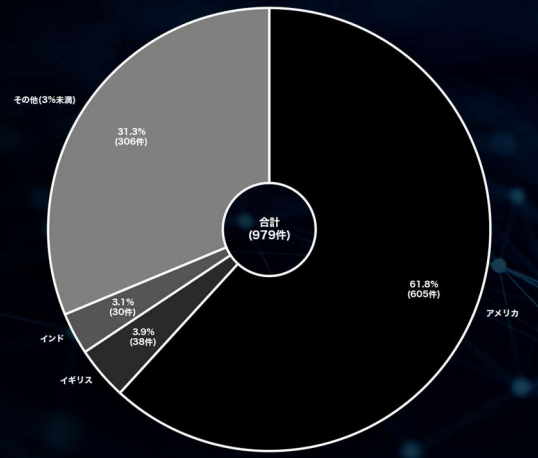
「医療」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、60件の掲載があった。一方、最も少なかった月は2024年1月で、25件であった。被害組織の所在国の割合では、アメリカが約62%と最も多く、次いでイギリス、インドがそれぞれ約4%と約3%である。攻撃グループについては、少なくとも106のグループが関与しており、特に「INC Ransom」が82件のリークサイト掲載を実施している。次いでと「Qilin（Agenda）」と「LockBit」がそれぞれ74件と67件の掲載を行っている。かつては低水準だった医療関連の被害数は2023年3月頃に増加し、その後も高水準を維持している。この変化の背景には、攻撃グループが生存競争の中で業種を問わない攻撃へと方針を転換していった可能性も否定できない。また、国別に見る傾向としてアメリカにおける被害が非常に高い割合を占めている点が顕著である。



▼攻撃グループ別



▼国別



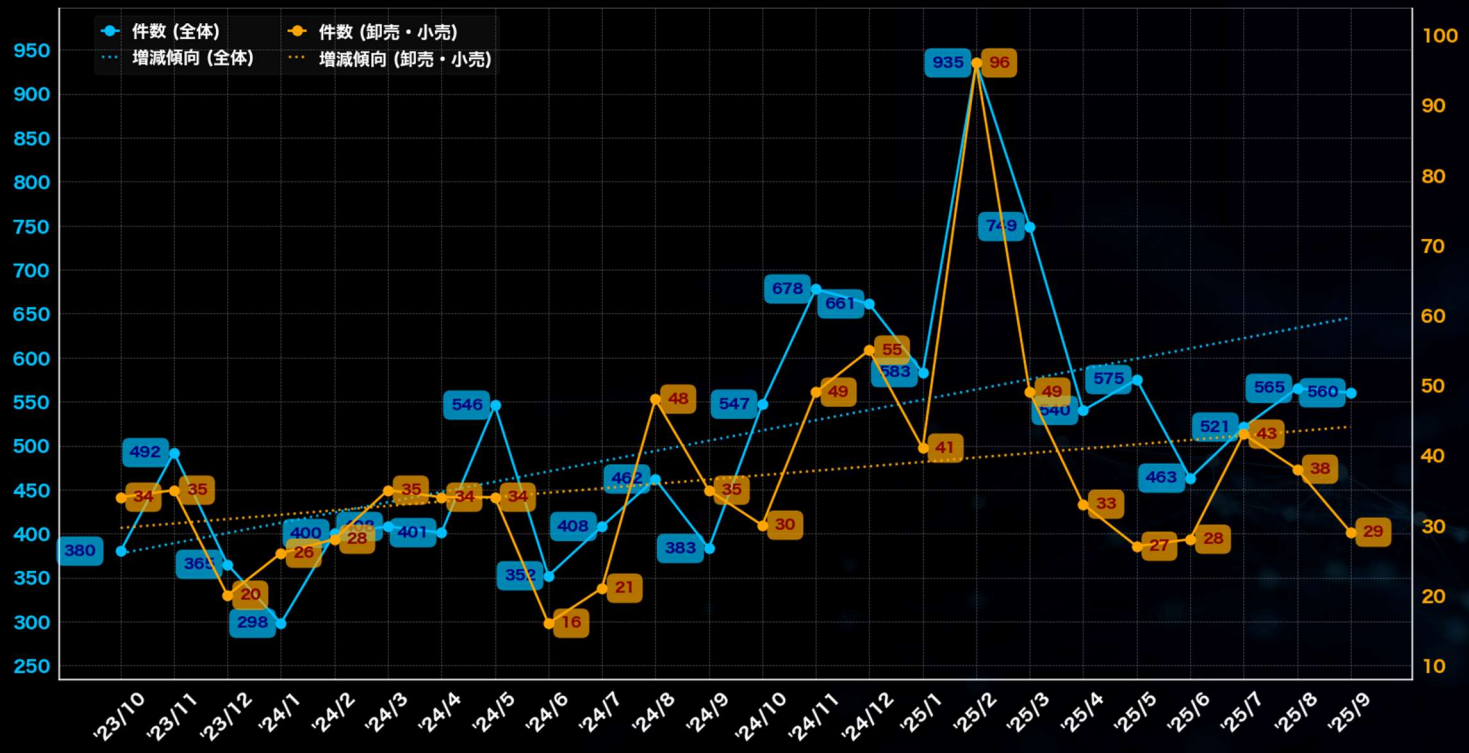
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて
国内被害組織からの公表や報道から判明した数も含んでいる）

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

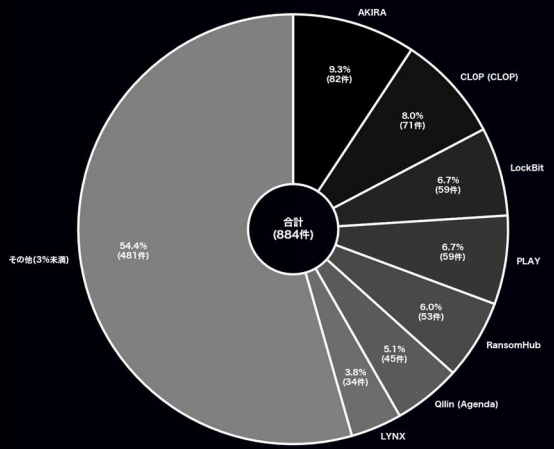
業種に関する分析（全世界）
（過去2年間／2023年10月～2025年9月）

卸売・小売

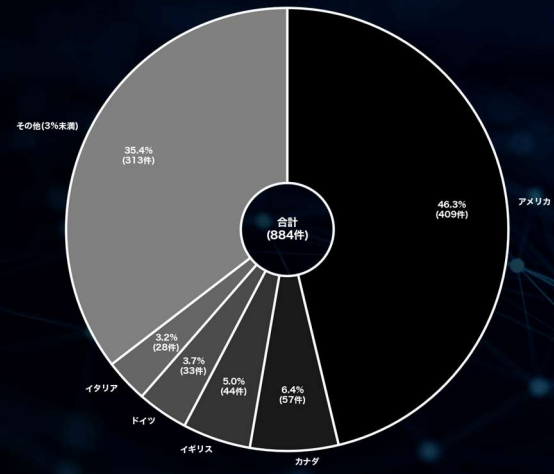
「卸売・小売」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、96件の掲載があった。一方、最も少なかった月は2024年6月で、16件であった。被害組織の所在国の割合では、アメリカが約46%と最も多く、次いでカナダとイギリスがそれぞれ約6%と約5%である。攻撃グループについては、少なくとも93のグループが関与しており、特に「AKIRA」が82件のリークサイト掲載を実施している。次いで「CL0P (CLOP)」と「LockBit」が71件と59件の掲載を行っている。卸売・小売関連は大きな増減の波があるものの、過去2年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



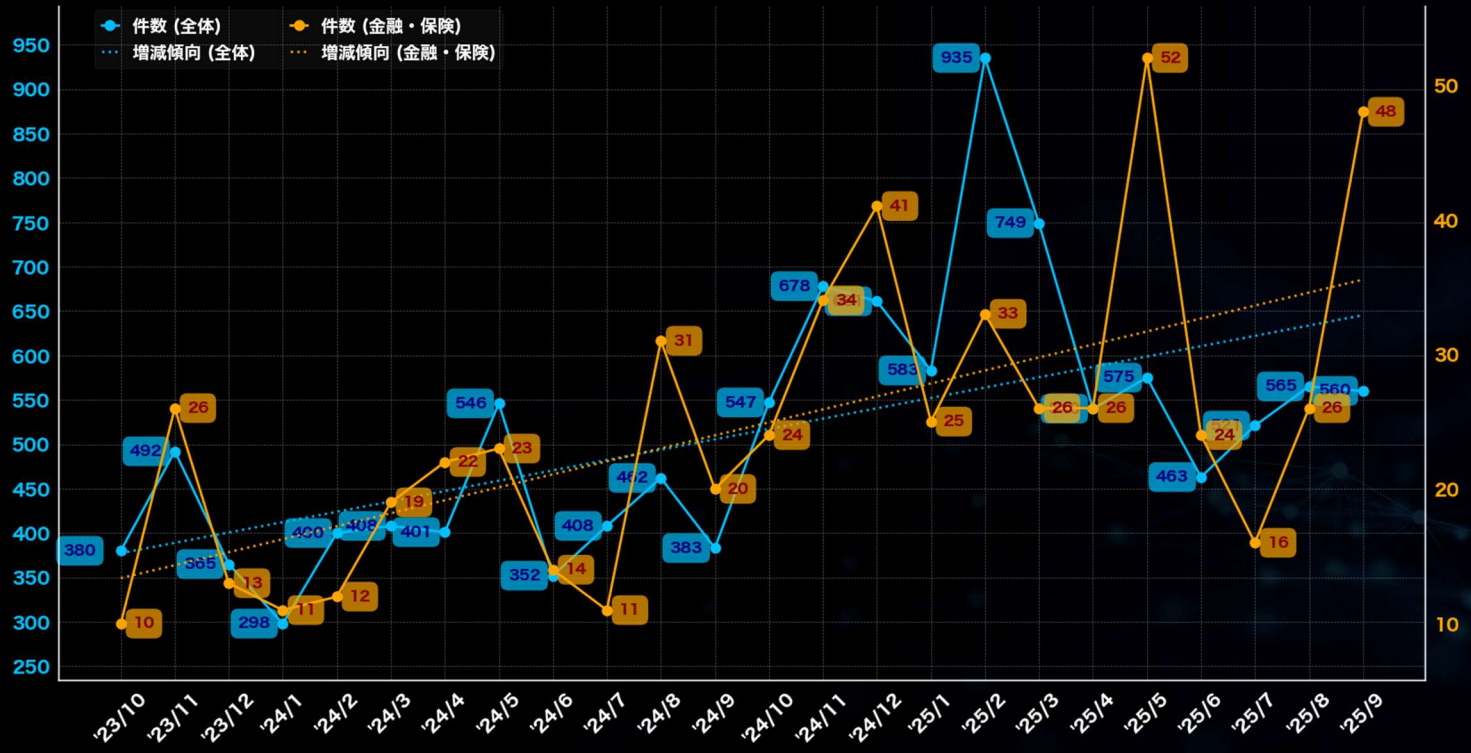
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

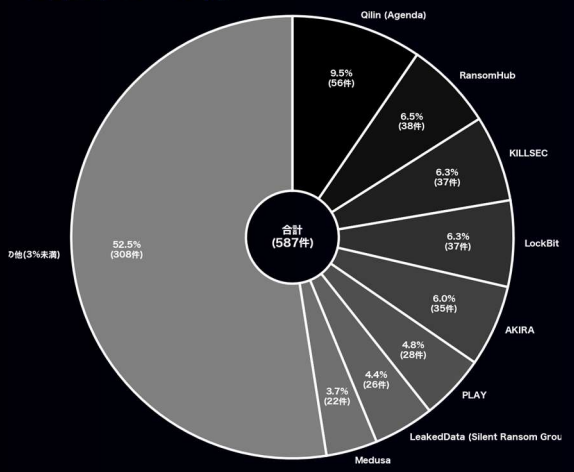
業種に関する分析（全世界）
（過去2年間／2023年10月～2025年9月）

金融・保険

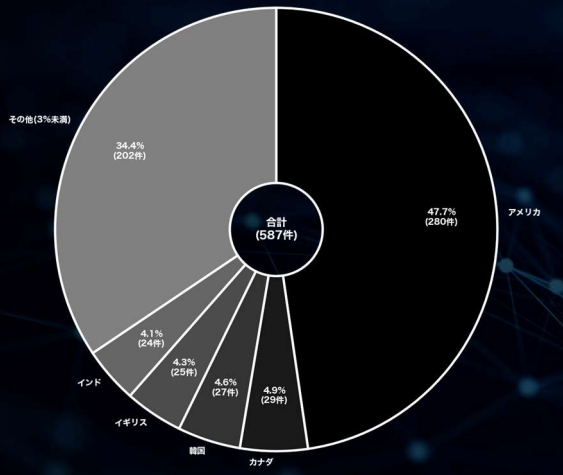
「金融・保険」業界に対するランサムウェア攻撃のリークサイト掲載件数は、最も多かった月が2025年5月で、52件の掲載があった。一方、最も少なかった月は2023年10月で、10件であった。被害組織の所在国の割合では、アメリカが約48%と最も多く、次いでカナダと韓国がそれぞれ約5%である。攻撃グループについては、少なくとも98のグループが関与しており、特に「Qilin (Agenda)」が56件のリークサイト掲載を実施している。次いで「RansomHub」と「KILLSEC」がそれぞれ38件と37件の掲載を行っている。金融・保険関連は全体件数に対する割合は低いものの明確な増加傾向にある。



▼攻撃グループ別



▼国別



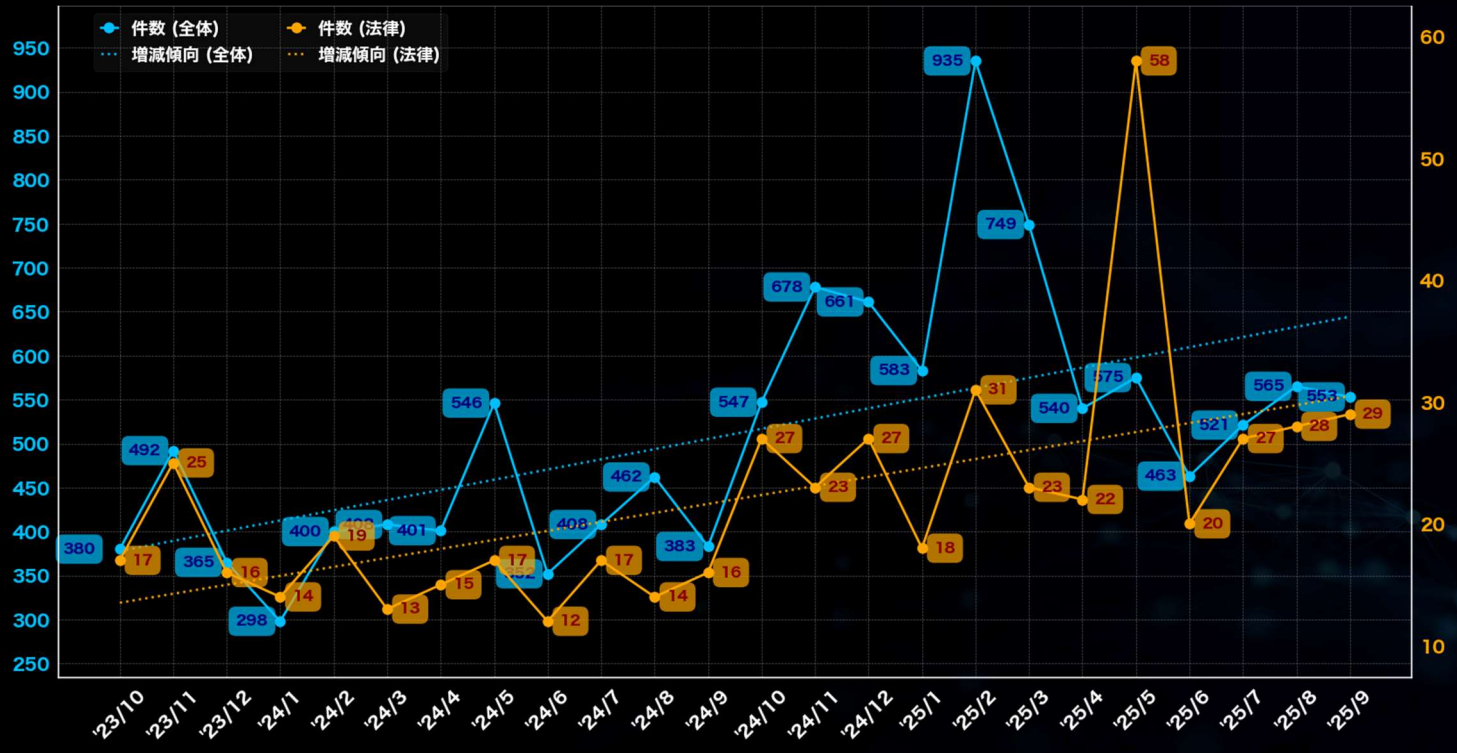
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

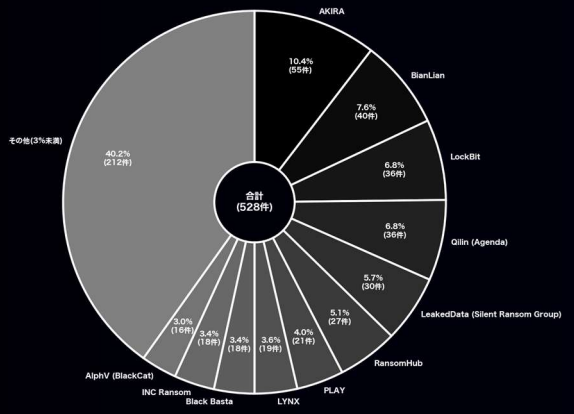
業種に関する分析（全世界）
（過去2年間／2023年10月～2025年9月）

法律

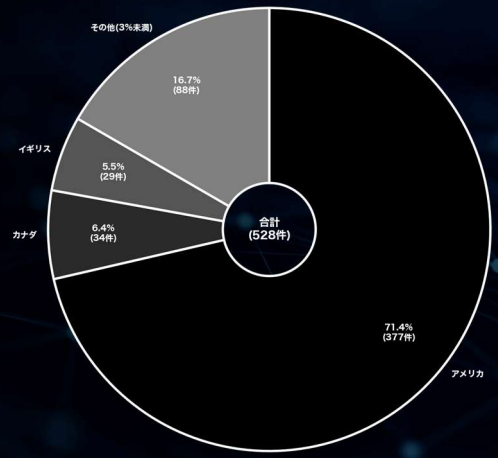
「法律」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年5月で、58件の掲載があった。一方、最も少なかった月は2024年6月で、12件であった。被害組織の所在国の割合では、アメリカが約71%と最も多く、次いでカナダとイギリスがそれぞれ約6%である。攻撃グループについては、少なくと76のグループが関与しており、特に「AKIRA」が55件のリークサイト掲載を実施している。次いで「BianLian」と「LockBit」がそれぞれ40件と36件の掲載を行っている。法律関連は2023年末以降、減少傾向が見られたが、2024年9月から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



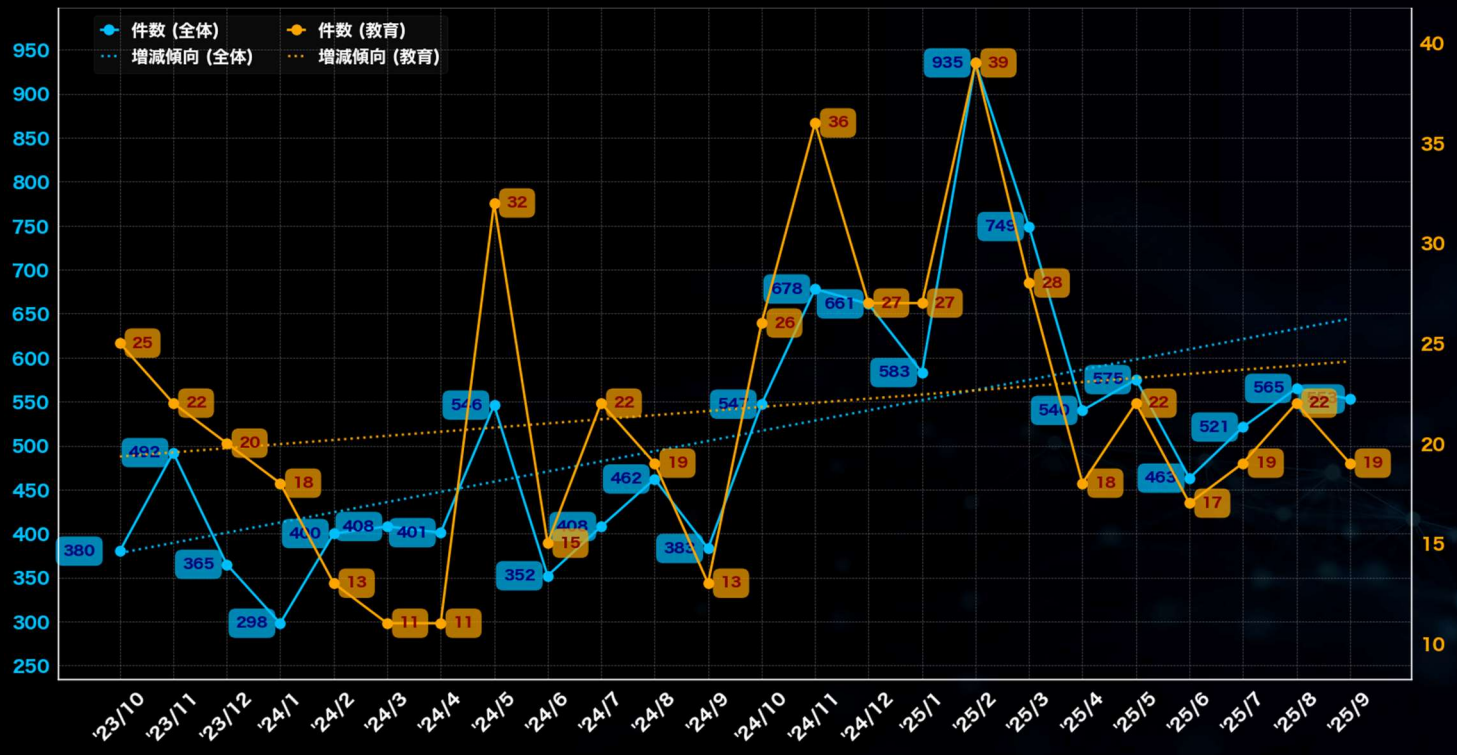
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

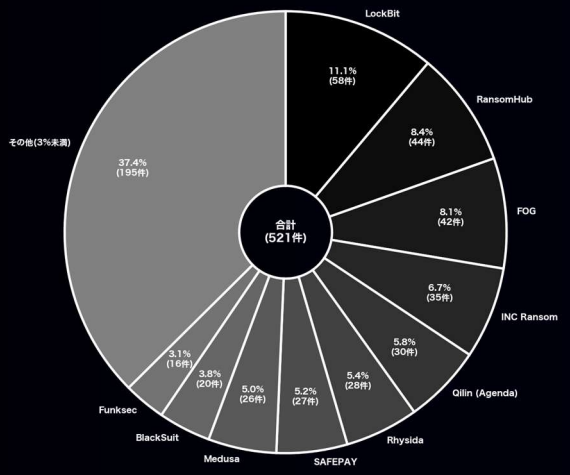
業種に関する分析（全世界）
（過去2年間／2023年10月～2025年9月）

教育

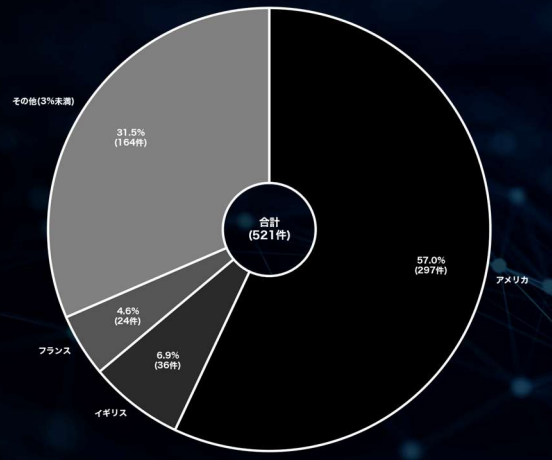
「教育」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、39件の掲載があった。一方、最も少なかった月は2024年3月と4月で、11件であった。被害組織の所在国の割合では、アメリカが約57%と最も多く、次いでイギリスとフランスがそれぞれ約7%と約4%である。攻撃グループについては、少なくとも82のグループが関与しており、特に「LockBit」が58件のリークサイト掲載を実施している。次いで「RansomHub」と「FOG」がそれぞれ44件と42件の掲載を行っている。教育業界は、攻撃グループ別で見ると、同業界を主な標的の一つとする「Rhysida」やFOGが上位に現れる点が特徴的である。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



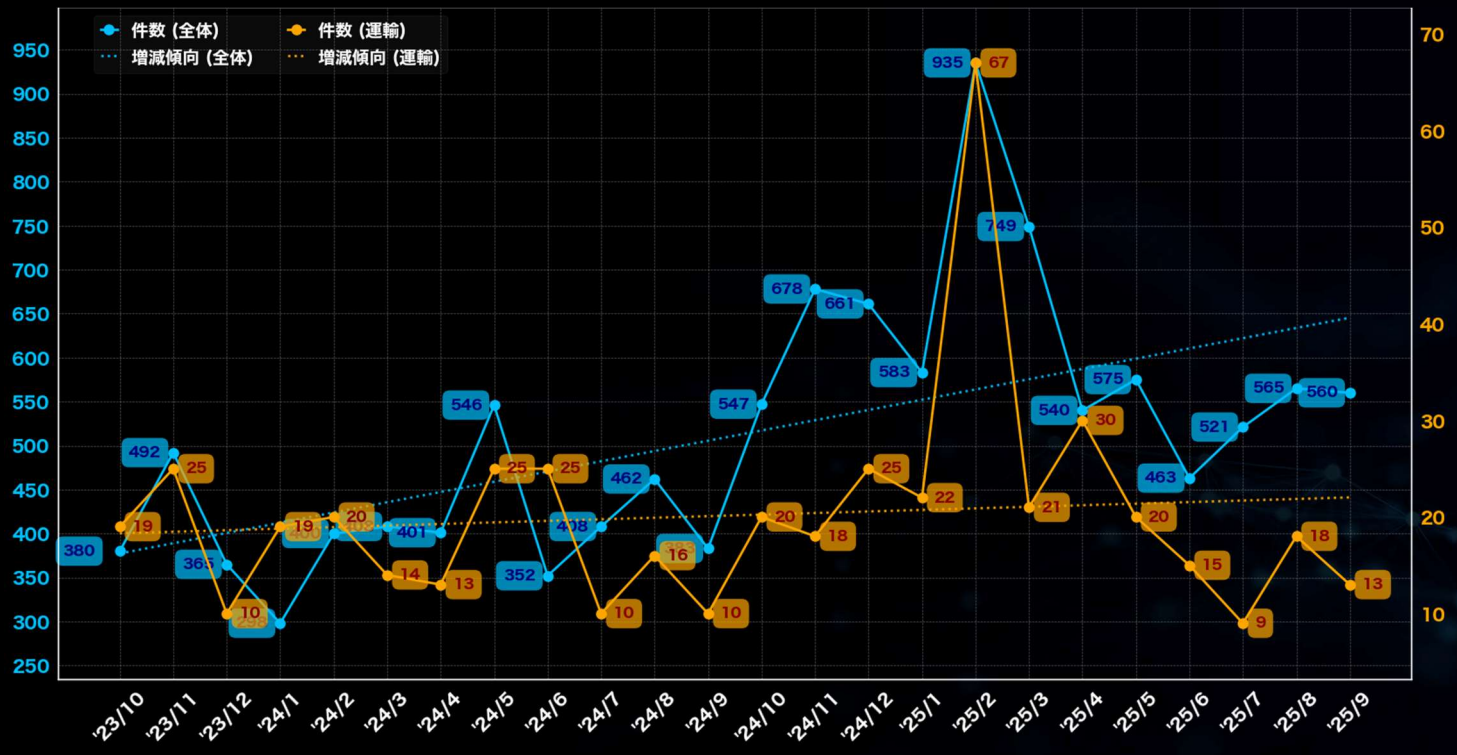
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

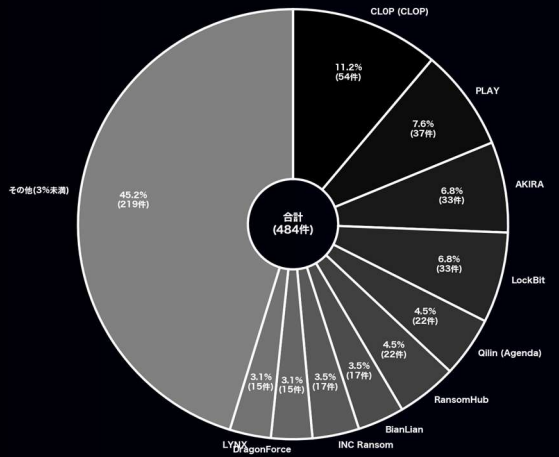
業種に関する分析（全世界）
（過去2年間／2023年10月～2025年9月）

運輸

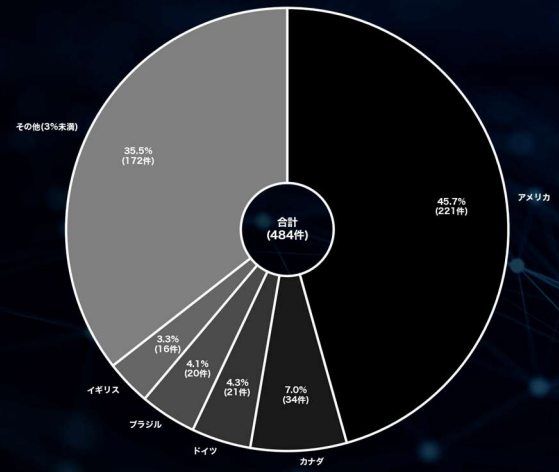
「運輸」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、67件の掲載があった。一方、最も少なかった月は2025年7月で9件であった。被害組織の所在国の割合では、アメリカが約46%と最も多く、次いでカナダとドイツがそれぞれ約7%と約4%である。攻撃グループについては、少なくとも85のグループが関与しており、特に「CL0P（CLOP）」が54件のリークサイト掲載を実施している。次いで「PLAY」と「LockBit」がそれぞれ37件と33件の掲載を行っている。運輸関係は全体件数に対する割合こそ低く、過去2年間では著しく被害が減少するケースもある一方で、緩やかな増加傾向が続いている。



▼攻撃グループ別



▼国別



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

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

CIGのコンテンツ紹介

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

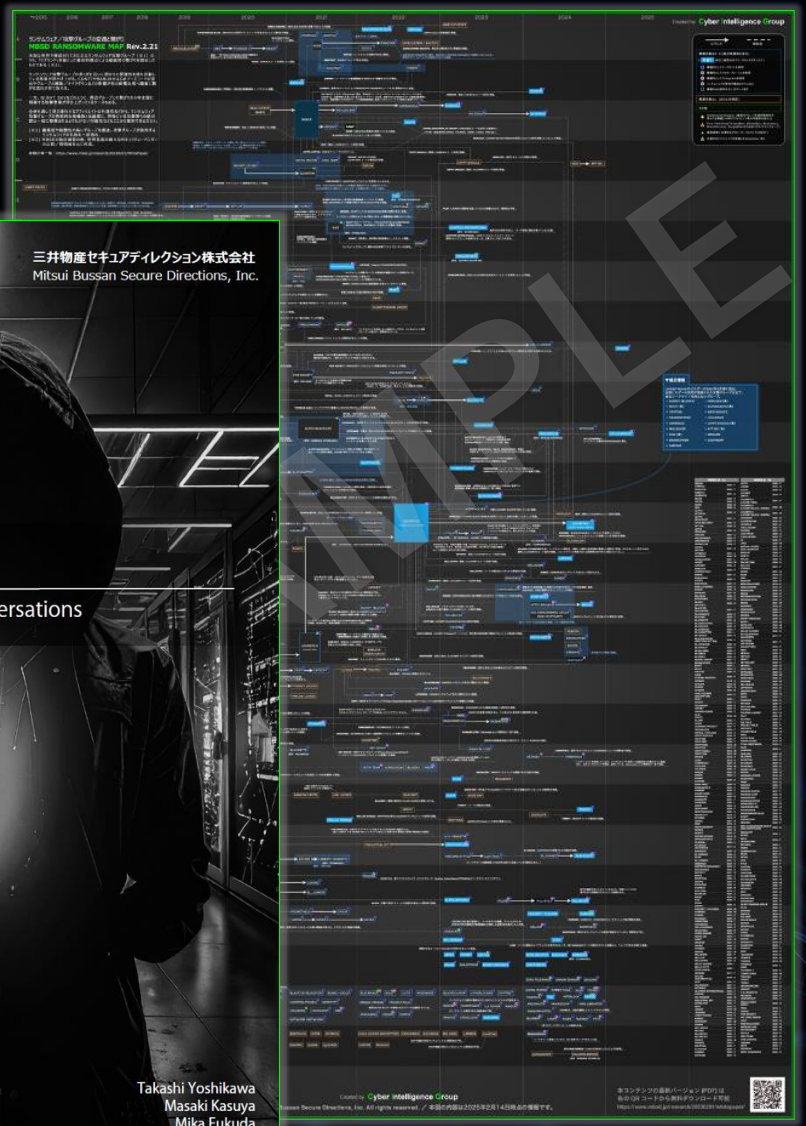
● ランサムウェア／攻撃グループの変遷と繋がり (MBSD RANSOMWARE MAP)：
https://www.mbsd.jp/research/20230201/whitepaper/

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

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

● 分析レポート：
https://www.mbsd.jp/report

MBSD RANSOMWARE MAP (Rev.2)



Black Basta 内部チャット分析レポート

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

本資料に関する留意事項及び二次利用について

留意事項

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

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

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

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

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

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

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

・ これらはあくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定されます。

・ 集計方法の変更や、時間が長期経過し公開／公表されるケースを再集計する場合もあるため、常に最新月のレポートを参照してください。

二次利用等に関して

本レポートはご自由に二次利用いただけます。様々な用途にぜひご活用ください。
ご利用・転載・引用の際には、出典として「MBSD Cyber Intelligence Group (CIG)」と明記くださいますようお願いいたします。
（※本レポートそのものの販売など直接的な営利目的でのご利用はご遠慮ください。有料セミナーや出版物、メディア記事など、利用者側の収益が発生する活動においても、参考情報として一部を引用・掲載いただくことに問題はありません。その際は大変お手数ですが、状況把握のため、ご利用前に下記連絡先まで簡単にご一報いただけますと幸いです）

お問い合わせ窓口：https://www.mbsd.jp/contact/

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

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

Cyber Intelligence Group