

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12月号 Rev 1.00 (2025年11月分)

2025

11

目次

総括と監視対象（レポート①～④）

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

グローバル統計（レポート⑤～⑬）

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

日本関連組織を対象とした統計（レポート⑬～⑲）

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

中小企業における被害分析（レポート⑲～⑳）

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

多重被害に関する分析（レポート㉑～㉒）

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

業種に関する分析（レポート㉓）

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

その他

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

総括と監視対象

2025

11

今月のハイライト

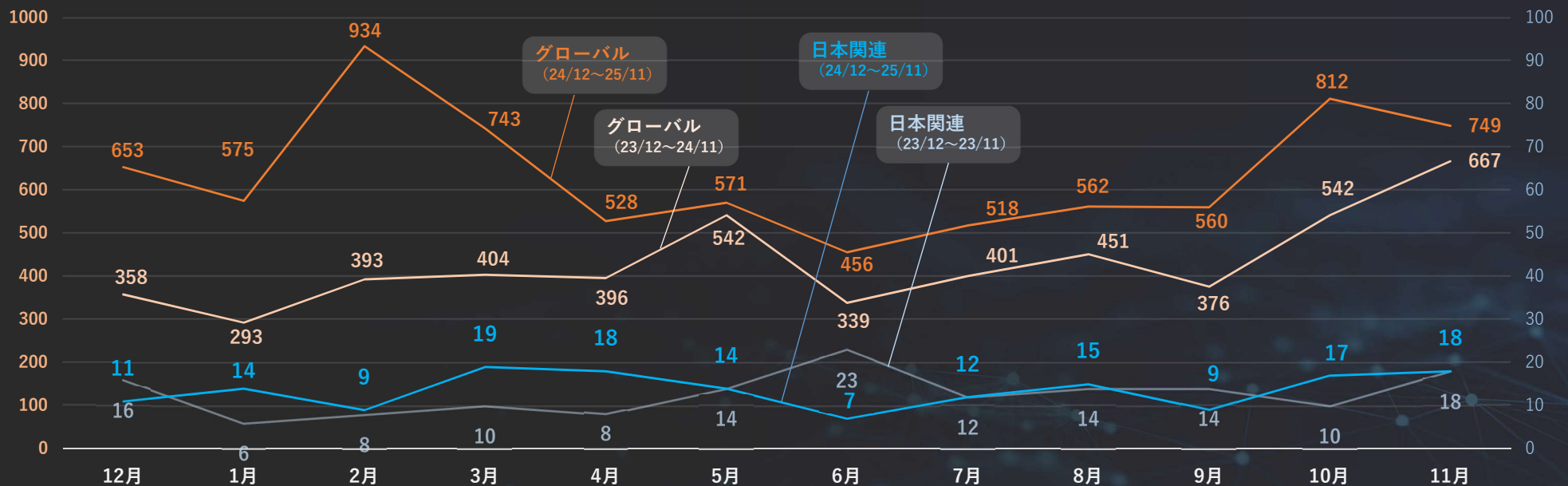
● 過去1年間でランサムウェアグループの掲載が大きく増加

過去1年間で、ランサムウェア攻撃グループのリークサイトに掲載される被害組織数は、世界的に明確な増加傾向を示している。とりわけ2025年2月には900を超える組織が新たに掲載され、この急増の背景には「CL0P（CLOP）」によるファイル転送サービスのゼロデイ脆弱性悪用を契機とした大規模な攻撃キャンペーンがある。ただし、CL0Pの攻撃を含まない月も前年同月を上回る水準で推移しており、ランサムウェア被害の増加が一過性ではないことが読み取れる。一方、日本関連組織に着目すると、グローバルほど顕著な増加は見られないものの、1年間を通じて一定の水準で被害が発生し続けている。前年と比較すると総件数はやや増加しており、日本の組織も常に攻撃のリスクに晒されていることがうかがえる。

リークサイト掲載数の年間比較

グローバル：過去1年を前年同時期と比較すると、全ての月で前年同月を上回る水準

日本関連：過去1年を前年同時期と比較すると、急激な増加は見られないものの、一定水準で被害が継続



国内では大企業の被害が目立ちがちだが、実際の集計結果では、日本関連の被害組織の約半数を中小企業が占めている。規模を問わず、あらゆる組織が標的となり得る状況である点にあらためて留意が必要である。

ランサムウェア関連記事 | 今月のピックアップ (期間: 2025年11月10日～2025年12月10日)

【Yanluowang初期アクセスブローカーがランサムウェア攻撃で有罪を認める】(Bleeping Computer : 2025/11/10)

ロシア人ハッカーが、初期アクセスブローカーとして複数の米企業に侵入し、そのアクセス権をYanluowangランサムウェア集団に販売したとして有罪を認めた。

<https://www.bleepingcomputer.com/news/security/yanluowang-initial-access-broker-pleaded-guilty-to-ransomware-attacks/>

【CISAとパートナーがAkiraランサムウェアに関するアドバイザリーアップデートを発表】(米国 CISA : 2025/11/13)

米CISAはAkiraランサムウェアに関する最新の共同勧告を公開した。VPNやバックアップ機器の脆弱性を悪用した侵入や被害拡大の手口を整理し、幅広い業種に対策強化を呼びかけている。

<https://www.cisa.gov/news-events/alerts/2025/11/13/cisa-and-partners-release-advisory-update-akira-ransomware>

【オペレーション・エンドゲーム、世界規模でRhadamanthys Stealer、Venom RAT、Elysium Botnetを解体】(The Hacker News : 2025/11/13)

欧州警察機構と欧州司法機構が主導する国際的な法執行作戦「Operation Endgame」により、Rhadamanthys Stealer、Venom RAT、Elysium Botnet といった主要なマルウェア基盤が解体された。

<https://thehackernews.com/2025/11/operation-endgame-dismantles.html>

【米・豪・英がロシア拠点のランサムウェア支援基盤に共同制裁措置を発表】(米国 財務省 : 2025/11/19)

米国・豪州・英国は、ランサムウェア攻撃などのサイバー攻撃を支援するロシア拠点の防弾ホスティング事業者に制裁を発動し、サイバー犯罪基盤への圧力を強化した。

<https://home.treasury.gov/news/press-releases/sb0319>

(PDF: https://www.ncsc.govt.nz/assets/guidance/Documents/Bulletproof-Defense-Mitigating-Risks-from-Bulletproof-Hosting-Providers_508c.pdf)

【サイバーアップデート：州司法長官事務所がランサムウェアグループによる大規模なデータ侵害を確認】(Cyber News Center : 2025/11/19)

米ペンシルベニア州司法長官事務所がInc RansomというRaaSグループによるランサムウェア被害が発生し、個人情報を含む大規模なデータ漏えいが確認された。公的機関の脆弱性管理が問われている。

<https://www.cybernewscentre.com/19th-november-2025-cyber-update-state-ag-office-confirms-major-data-breach-by-ransomware-group/>

【ナビムンバイのサイバー警察が偽コールセンター詐欺を摘発。1億2千万ルピーの株式詐欺と米国民へのランサムウェア攻撃で20人を逮捕】(Free Press Journal : 2025/11/20)

インドのナビムンバイで、株式投資詐欺と米国民を狙ったランサムウェア／マルウェア攻撃を行っていた偽コールセンター拠点が摘発され、ナビムンバイ・サイバー警察と犯罪捜査部が関与者20人を逮捕した。

<https://www.freepressjournal.in/mumbai/navi-mumbai-cyber-police-bust-fake-call-centre-racket-20-arrested-for-12-crore-stock-scam-and-ransomware-attacks-on-us-citizens/>

【FinCEN、ランサムウェアに関する金融動向を発表。被害額21億ドル超・2023年に過去最高を記録しつつ法執行により減少傾向】(米国 財務省 : 2025/12/04)

米財務省の金融犯罪取締ネットワーク (FinCEN) は、2022～2024年のBSAデータを基にランサムウェアの金融動向を分析した。被害総額は21億ドル超に達し、2023年には件数・支払額とも過去最多を記録した。

<https://www.fincen.gov/news/news-releases/fincen-issues-financial-trend-analysis-ransomware/>

【政府へのサイバー攻撃：10以上の事例、傾向、予防のヒント】(SecureFrame : 2025/12/04)

サイバー攻撃が、AIやサプライチェーンの脆弱性により急増。英米組織のセキュリティ責任者88%が懸念。ランサムウェアやディープフェイクなど攻撃手法が高度化し、政府機関や契約業者が対応に苦慮。

<https://secureframe.com/blog/government-cyber-attacks/>

【侵入型ランサムウェア攻撃を受けたら読むFAQ】(JPCERT : 2025/12/05)

JPCERT/CCは、情報窃取や暗号化を行う侵入型ランサムウェア攻撃を受けた際の初動対応や判断ポイントをまとめたFAQを公開。

<https://www.jpcert.or.jp/magazine/security/ransom-faq.html>

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：282 ^(※1) ^(※2)

→ 当月リークサイト掲載の活動を確認した攻撃グループ数：55

● 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)

※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

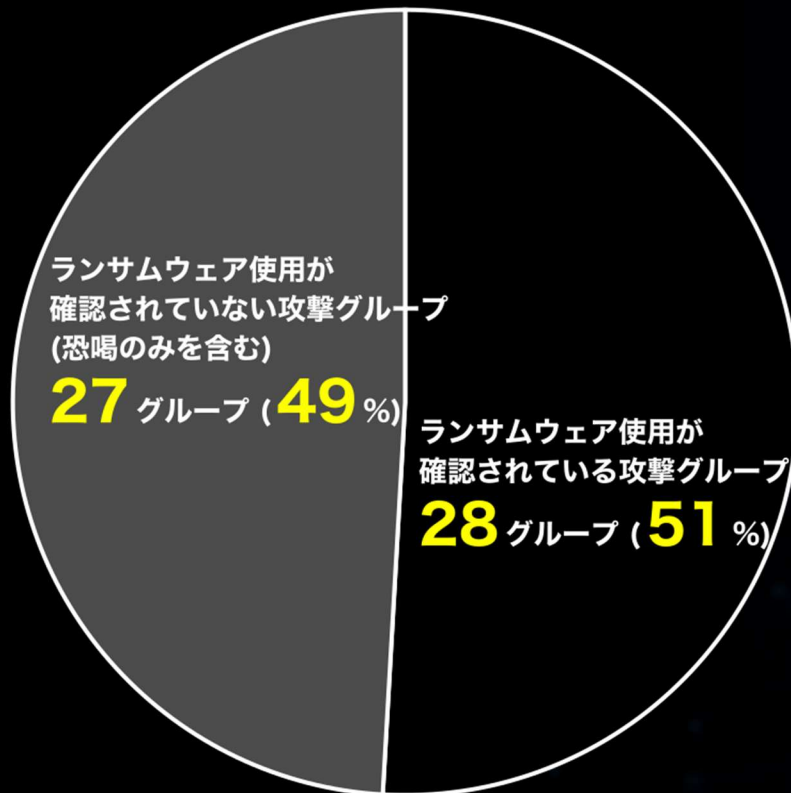
※2) 活動停止した攻撃グループを含む

Alpha (MYDATA)	CACTUS	DoppelPaymer	KAIROS	Morpheus	Rancoz	Space Bears
AlphV (BlackCat)	Cephalus	dotAdmin	Karakurt	Mount Locker	RansomBay	Sparta
Anubis	CHAOS (2025)	DragonForce	Karma	N3tw0rm (NetWorm)	Ransom Cartel	Spook
Apos Security	CHEERS	DragonRansomware	Kawa4096	N4UGHTYSEC (NAUGHTYSEC)	Ransom Corp	STORMOUS
APT73 (Eralig)	ChileLocker (Arcrypter)	DUNGHILL	● Kazu	NASIR SECUTRIY	RANSOMCORTEX	Sugar
ARACHNA	CHORT	eCh0raix (eChoraix)	KILLSEC	Nefilim	Ransomed.vc	Suncrypt
ARCUS MEDIA	Cicada3301	EL Cometa	Knight	Nevada	Ransom EXX	SynACK
Argonauts	CiphBit	EL DORADO	Kraken (HelloKitty)	NightSky	RansomHouse	TeamXXX
Arkana	CipherLocker	EMBARGO	Kryptos	NightSpire	RansomHub	TENGU
ArvinClub	CLOP (CLOP)	Endurance	Kyber	NITROGEN	Ransomware Blog	Termite
Astro (Astra)	Cloak	Entropy	LAMBDA	NoEscape	Ranzy	The Gentlemen
AtomSilo	COINBASE CARTEL	Everest	La Piovra	Nokoyawa	RA WORLD	ThreeAM (3AM)
Avaddon	Conti	FOG	LAPSUS\$	NONAME (VFOXX)	Raznatovic	● TridentLocker
AvosLocker	Cooming Project	Frag	LeakedData (Silent Ransom Group)	NONAME [2023年確認]	RedAlert (N13V)	TRIGONA
Axxes	Crazy Hunter Team	FSOCIETY / FLOCKER	LEAKNET	Nova	Red Ransomware Group (Red CryptoApp)	TRINITY
AzzaSec	CROSSLOCK	FSTeam	LILITH	NULLBULGE	Relic	TRISEC
Babuk	CryptBB	FulcrumSec	Linkc	Obscura	Revil (Sodinokibi)	Underground
Babuk (2025)	CRYPTNET	Funksec	LockBit	Onyx	Rhysida	Unsafe
BASHE	CRYPTO24	GD LockerSec	Lorenz	Orca	Risen	Valencia
BEAST	CryptOn	Genesis	LostTrust	Pandora	ROOK	VanHelsing
● Benzona	Cuba	GLOBAL	LunaLock	Pay2Key	Royal	VanirGroup
BERT	Cyclops	Grief	LV	Payload.bin	Ransom	Vice Society
BianLian	D4RK4RMY	Groove	LYNX	Payouts King	RunSomeWares	V IS VENDETTA
BLOODY (BLOODY)	DAGON	Gunra	MADCAT	PEAR	Sabbath (54bb47h)	VSOP
Bl4ckt0r (BlackTor)	DAIXIN	HANDARA [Hacktivist]	MAD LIBERATOR	PLAY	SAFEPAY	WALocker
Black Basta	dAn0n (danon)	Haron	MALAS	PLAYBOY	SARCOMA	Warlock
BlackByte	Dark Angels	HELLCAT	MalekTeam	Prometheus	SATAN LOCK	WEREWOLVES
BlackDolphin	DARKBIT	Helldown	Mallox	PRYX	SATANLOCK V2	Weyhro
BlackLock	DARKPOWER	HelloGookie	Mamona RIP	PUTIN TEAM	Scattered LAPSUS\$ Hunters	WORLD LEAKS
BlackMatter	DarkRace	Hitler (AGLOBGVYCG)	MBC	Pysa / Mespinoza	Secp0	x001xs
Black Nevas	DarkRypt	Hive	Medusa	Qilin (Agenda)	Securotop	XING Team

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 **11**月)

(※当月にリークサイト掲載を確認した攻撃グループ全**55**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11月に活動中である事が確認された全55グループにおけるランサムウェア使用の割合の内訳を示した図である。

年間統計

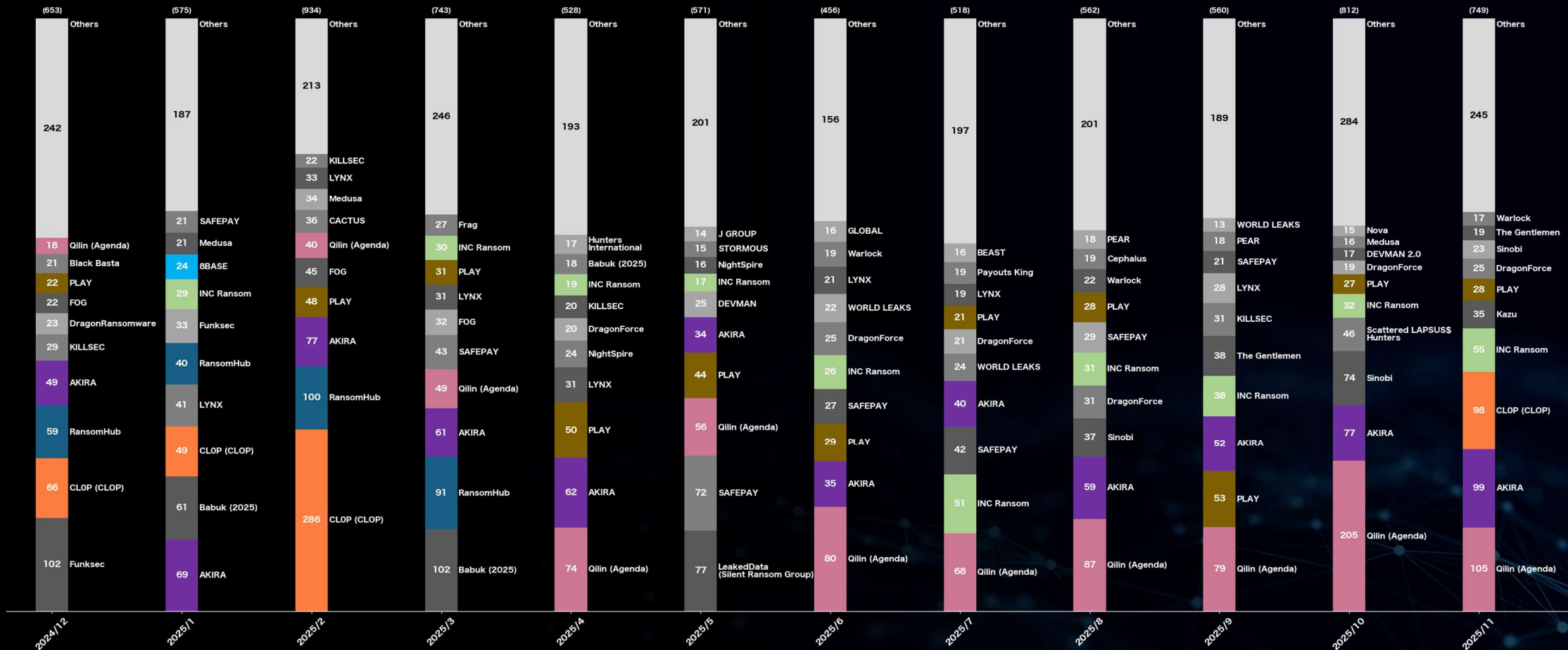
(全世界)

2025

11

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12月～2025年11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

11

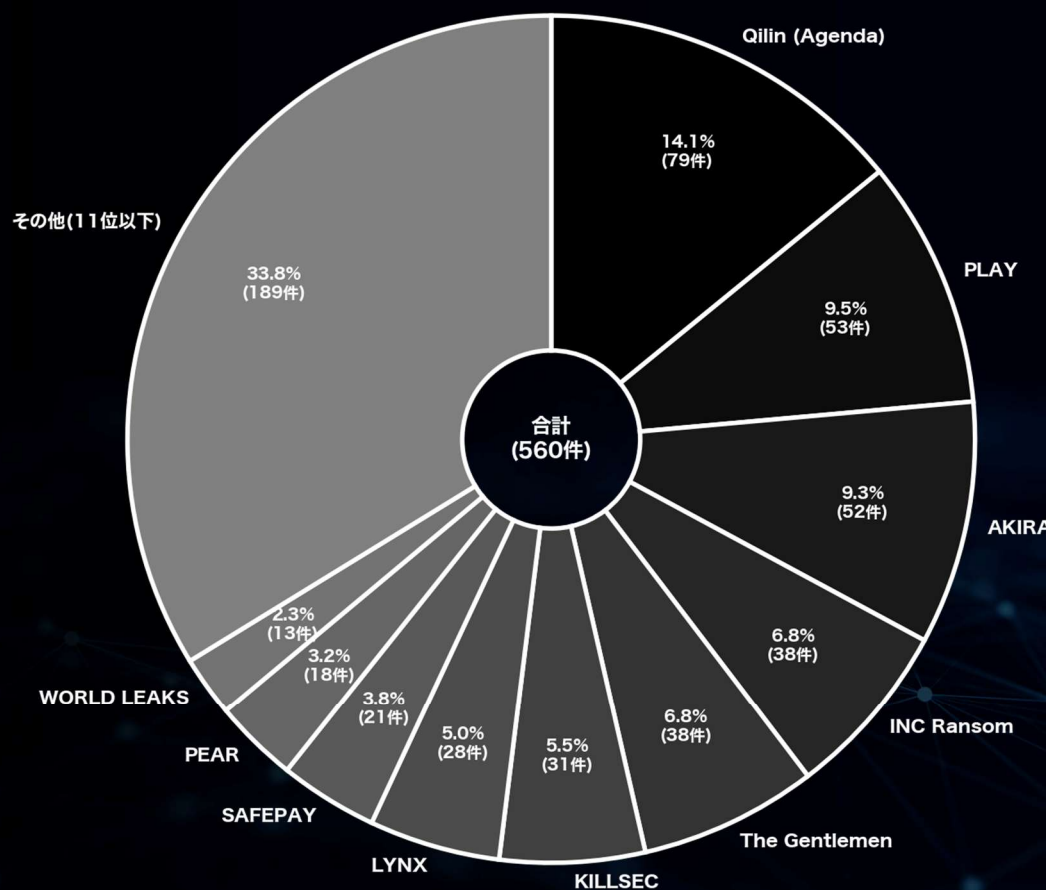
月別内訳 攻撃グループ TOP10 (全世界)

(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	14.1	- 8
PLAY	53	9.5	+ 25
AKIRA	52	9.3	- 7
INC Ransom	38	6.8	+ 7
The Gentlemen	38	6.8	+ 38
KILLSEC	31	5.5	+ 29
LYNX	28	5.0	+ 14
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)



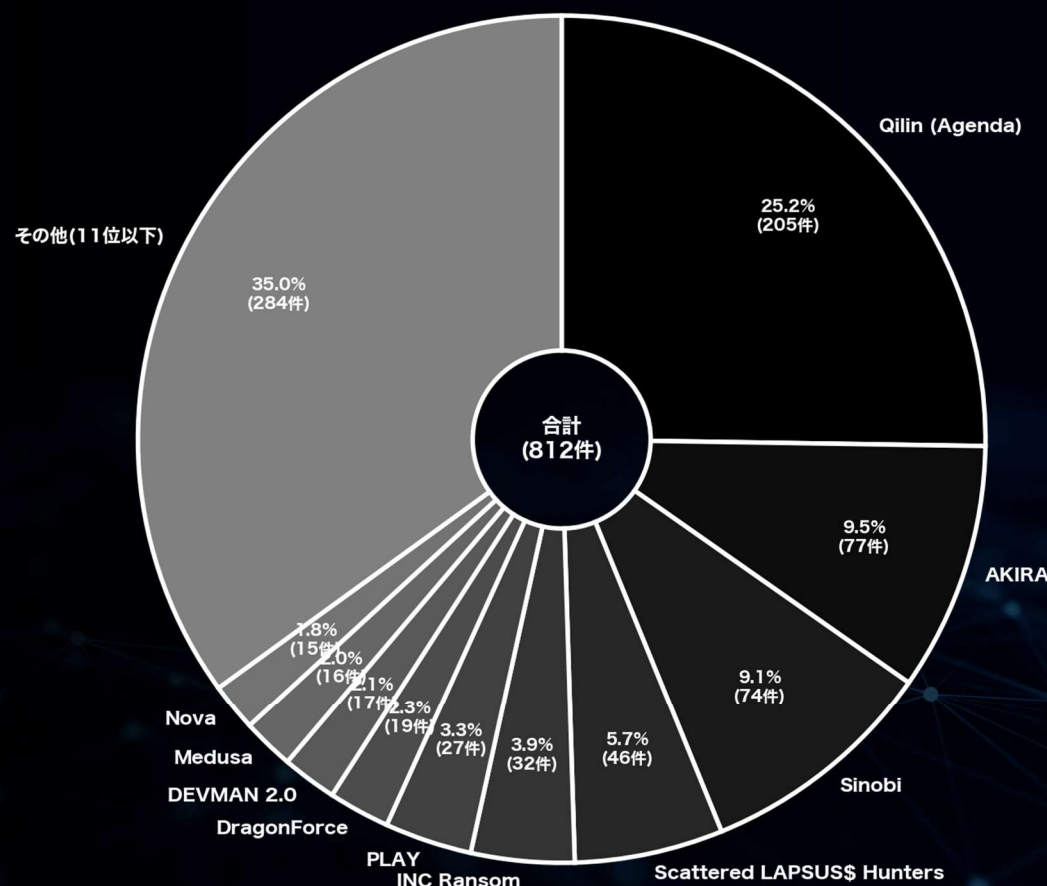
月別内訳 攻撃グループ TOP10 (全世界)

(2025年 10 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)	205	25.2	+ 126
AKIRA	77	9.5	+ 25
Sinobi	74	9.1	+ 71
Scattered LAPSUS\$...	46	5.7	+ 46
INC Ransom	32	3.9	- 6
PLAY	27	3.3	- 26
DragonForce	19	2.3	+ 11
DEVMAN 2.0	17	2.1	+ 5
Medusa	16	2.0	+ 7
Nova	15	1.8	+ 8

▼ランサムウェア攻撃グループの勢力割合 (リークサイトの掲載数による比較)



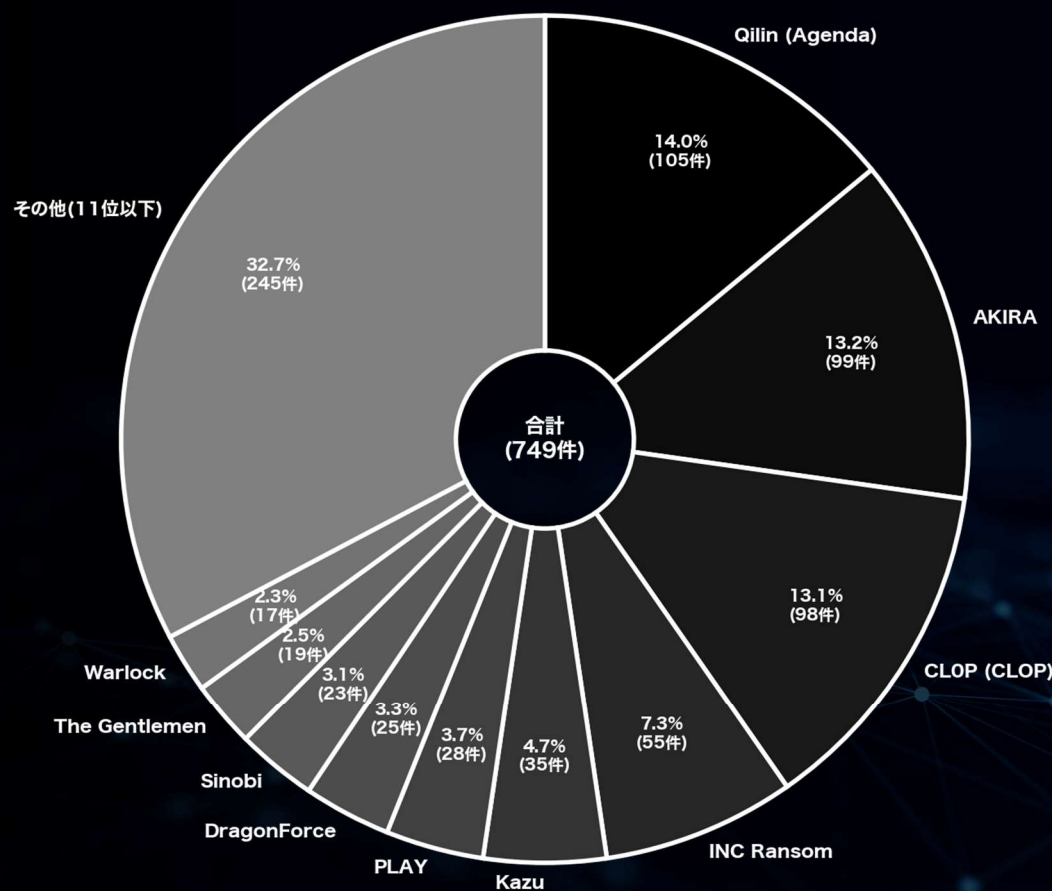
月別内訳 攻撃グループ TOP10 (全世界)

(2025年 **11** 月)

※件数順に降順／同件数のものが含まれる場合は名前順でTOP10までを記載

攻撃グループ名	件数	割合(%)	前月比(件数)
Qilin (Agenda)	105	14.0	- 100
AKIRA	99	13.2	+ 22
CLOP (CLOP)	98	13.1	+ 85
INC Ransom	55	7.3	+ 23
Kazu	35	4.7	+ 35
PLAY	28	3.7	+ 1
DragonForce	25	3.3	+ 6
Sinobi	23	3.1	- 51
The Gentlemen	19	2.5	+ 8
Warlock	17	2.3	+ 17

▼ランサムウェア攻撃グループの勢力割合
(リークサイトの掲載数による比較)



被害国 月別統計

(全世界) (過去3ヶ月分)

2025

11

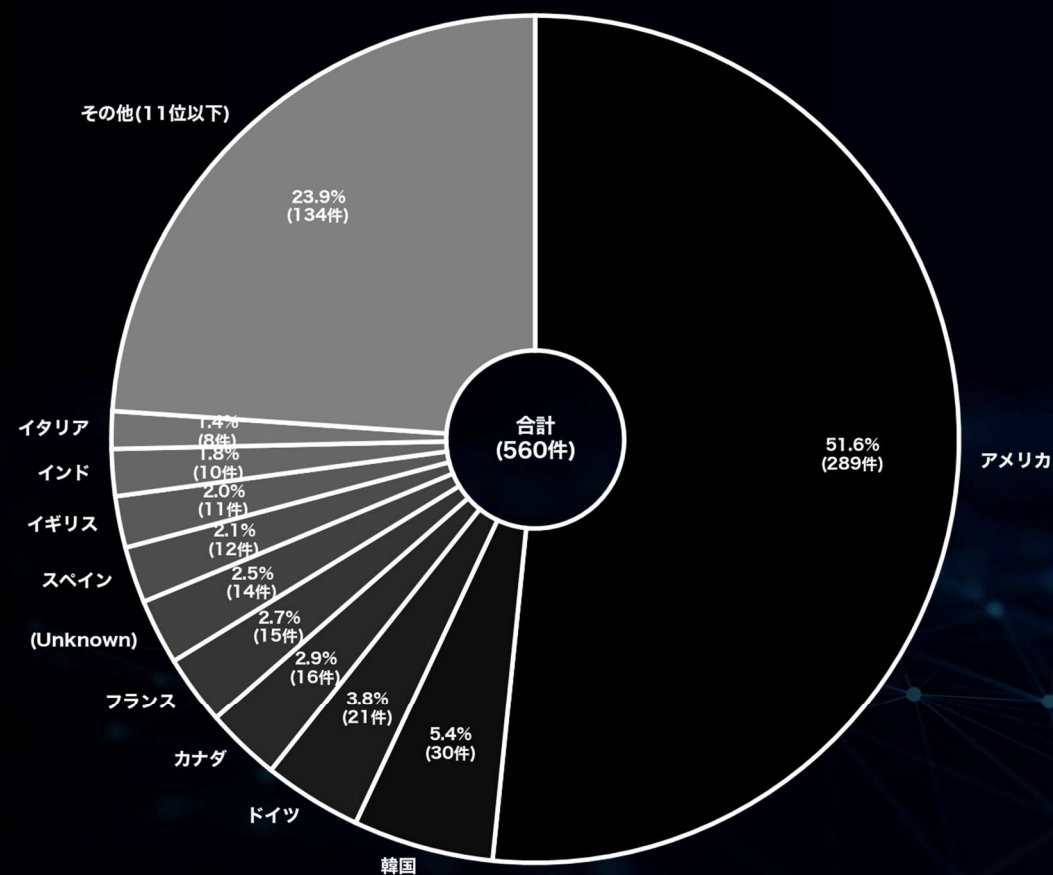
月別内訳 被害国TOP10 (全世界)

(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	289	51.6	- 20
韓国	30	5.4	+ 25
ドイツ	21	3.8	- 12
カナダ	16	2.9	- 7
フランス	15	2.7	+ 8
(Unknown)	14	2.5	- 10
スペイン	12	2.1	+ 6
イギリス	11	2.0	- 18
インド	10	1.8	+ 7
イタリア	8	1.4	- 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)



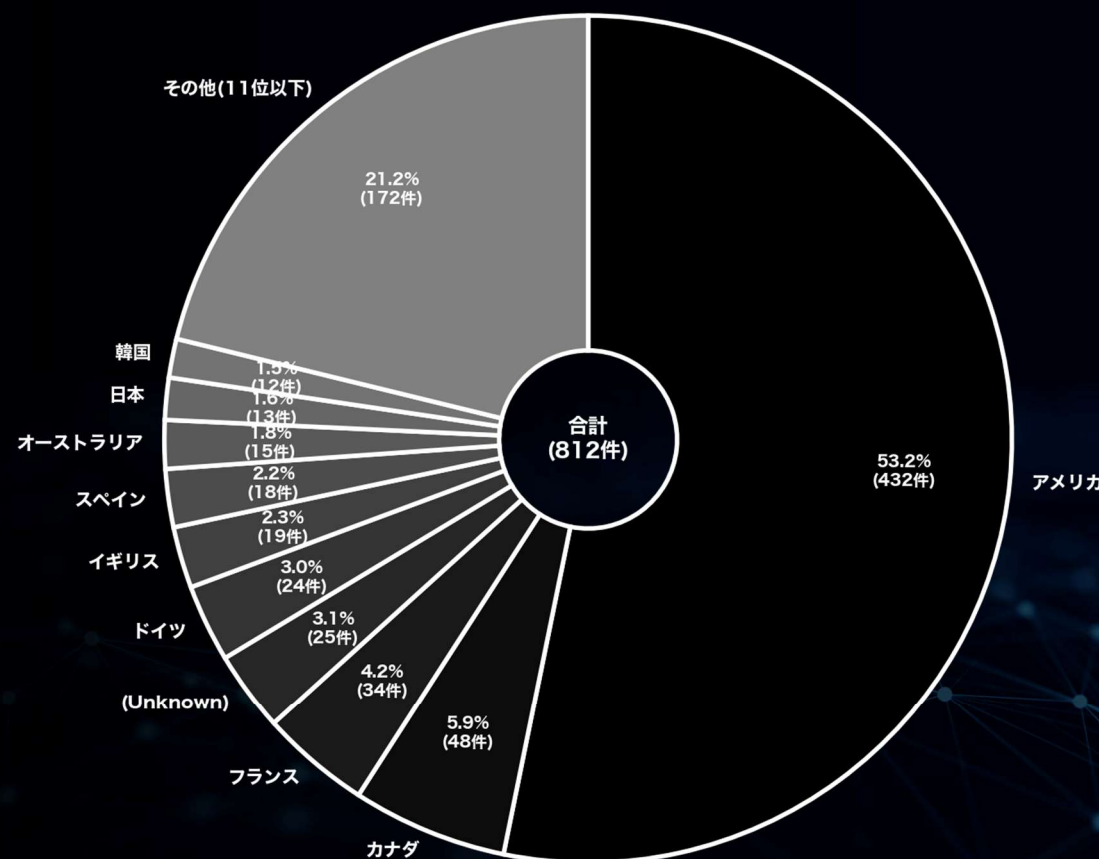
月別内訳 被害国TOP10 (全世界)

(2025年 10 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	432	53.2	+ 143
カナダ	48	5.9	+ 32
フランス	34	4.2	+ 19
(Unknown)	25	3.1	+ 11
ドイツ	24	3.0	+ 3
イギリス	19	2.3	+ 8
スペイン	18	2.2	+ 6
オーストラリア	15	1.8	+ 12
日本	13	1.6	+ 7
韓国	12	1.5	- 18

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



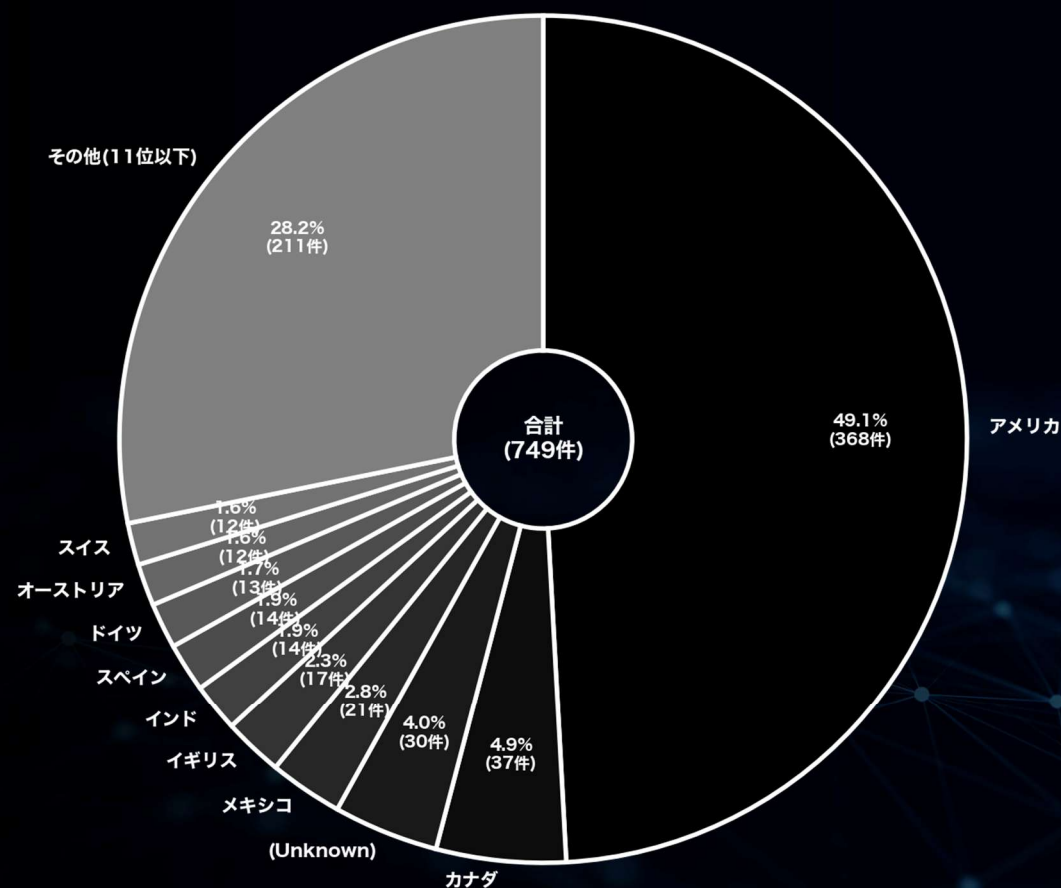
月別内訳 被害国TOP10 (全世界)

(2025年 11 月)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
アメリカ	368	49.1	- 64
カナダ	37	4.9	- 11
(Unknown)	30	4.0	+ 5
メキシコ	21	2.8	+ 17
イギリス	17	2.3	- 2
インド	14	1.9	+ 7
スペイン	14	1.9	- 4
ドイツ	13	1.7	- 11
オーストリア	12	1.6	+ 9
スイス	12	1.6	+ 7

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



被害国 月別統計

(アジア) (過去3ヶ月分)

2025

11

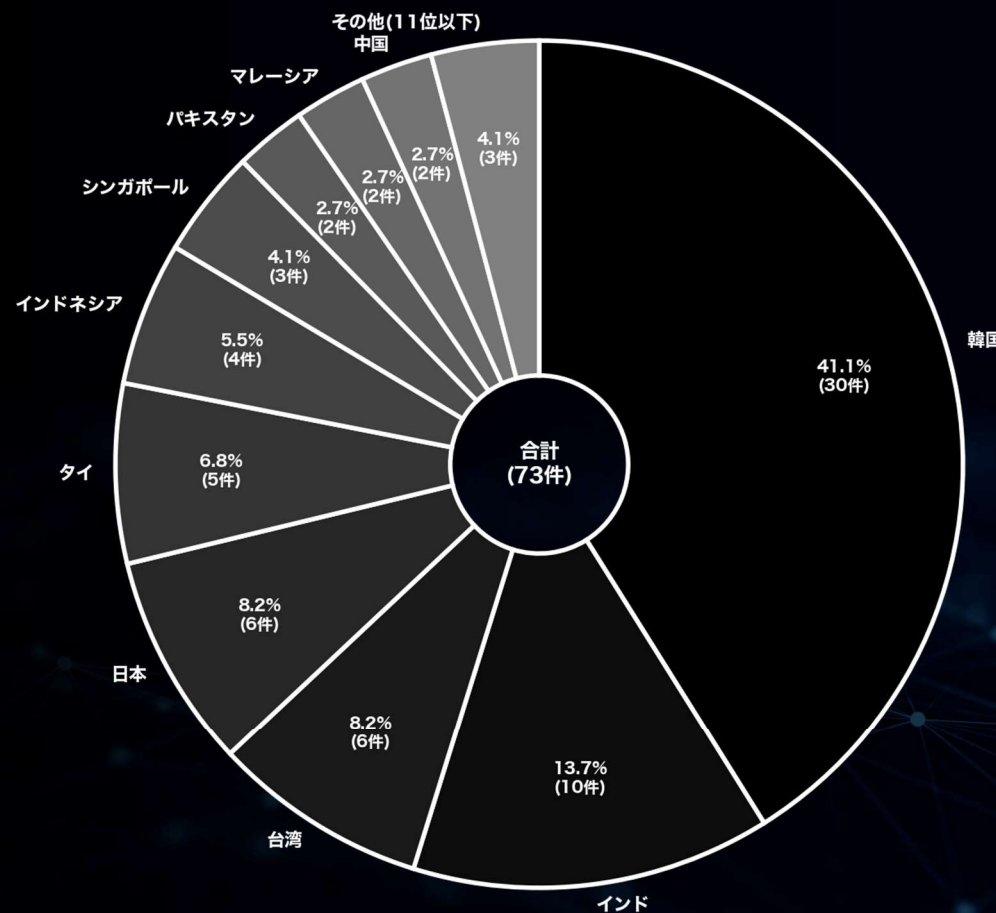
月別内訳 被害国TOP10 (アジア)

(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)



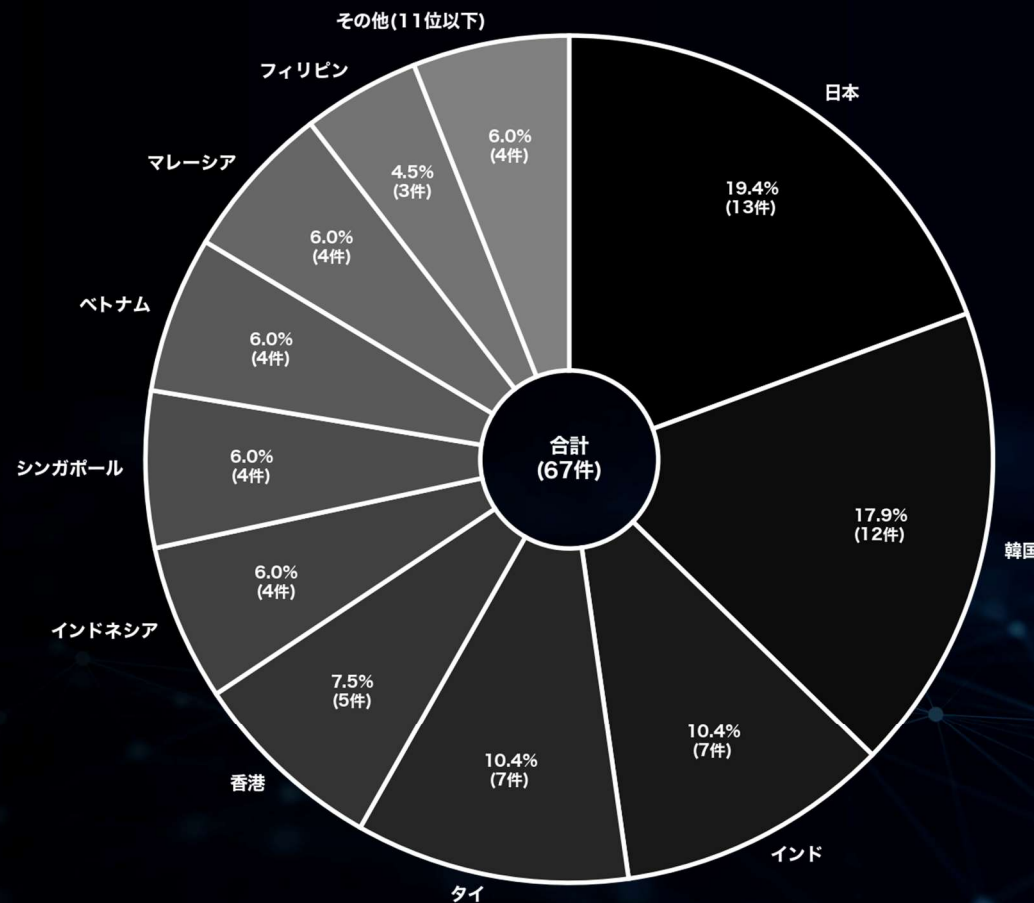
月別内訳 被害国TOP10 (アジア)

(2025年 10 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	13	19.4	+ 7
韓国	12	17.9	- 18
インド	7	10.4	- 3
タイ	7	10.4	+ 2
香港	5	7.5	+ 4
インドネシア	4	6.0	± 0
シンガポール	4	6.0	+ 1
ベトナム	4	6.0	+ 3
マレーシア	4	6.0	+ 2
フィリピン	3	4.5	+ 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)



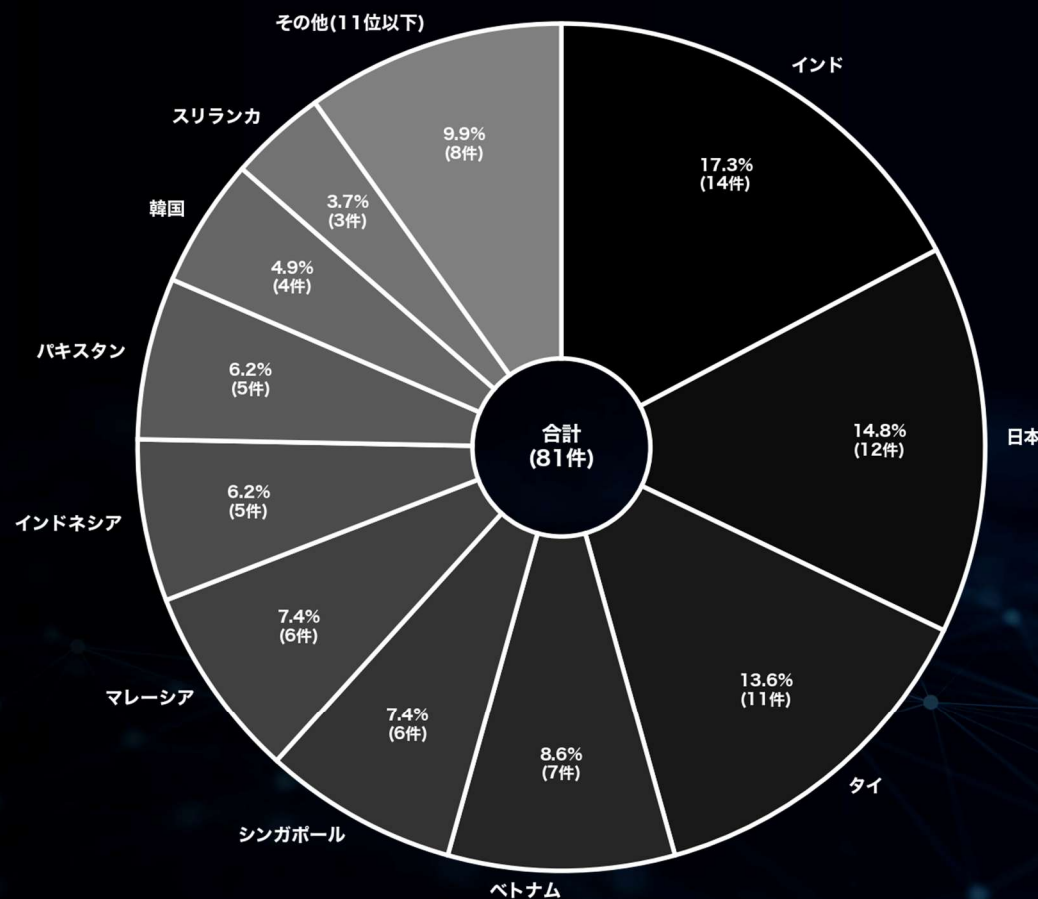
月別内訳 被害国TOP10 (アジア)

(2025年 11 月)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

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

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



業種 月別統計

(全世界) (過去3ヶ月分)

2025

11

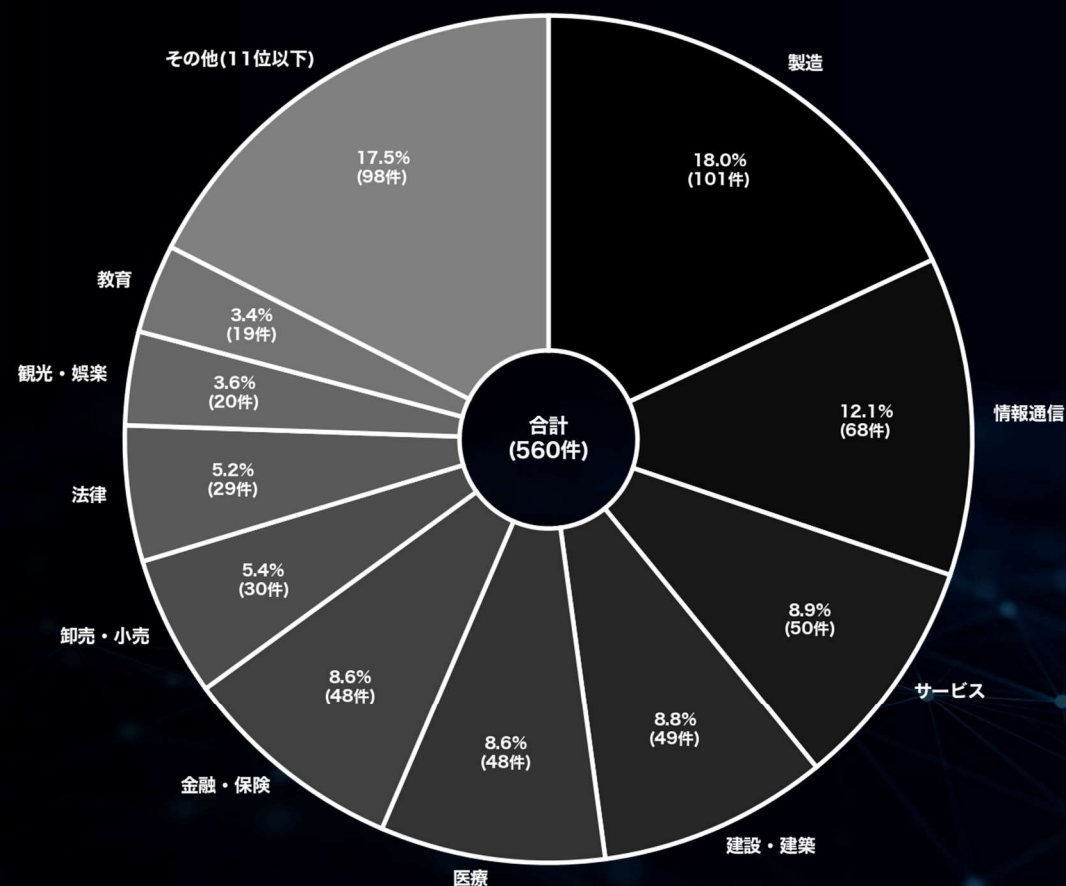
月別内訳 業種 TOP10 (全世界)

(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	101	18.0	- 15
情報通信	68	12.1	+ 22
サービス	50	8.9	- 23
建設・建築	49	8.8	- 6
医療	48	8.6	- 2
金融・保険	48	8.6	+ 22
卸売・小売	30	5.4	- 8
法律	29	5.2	+ 1
観光・娯楽	20	3.6	+ 5
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)



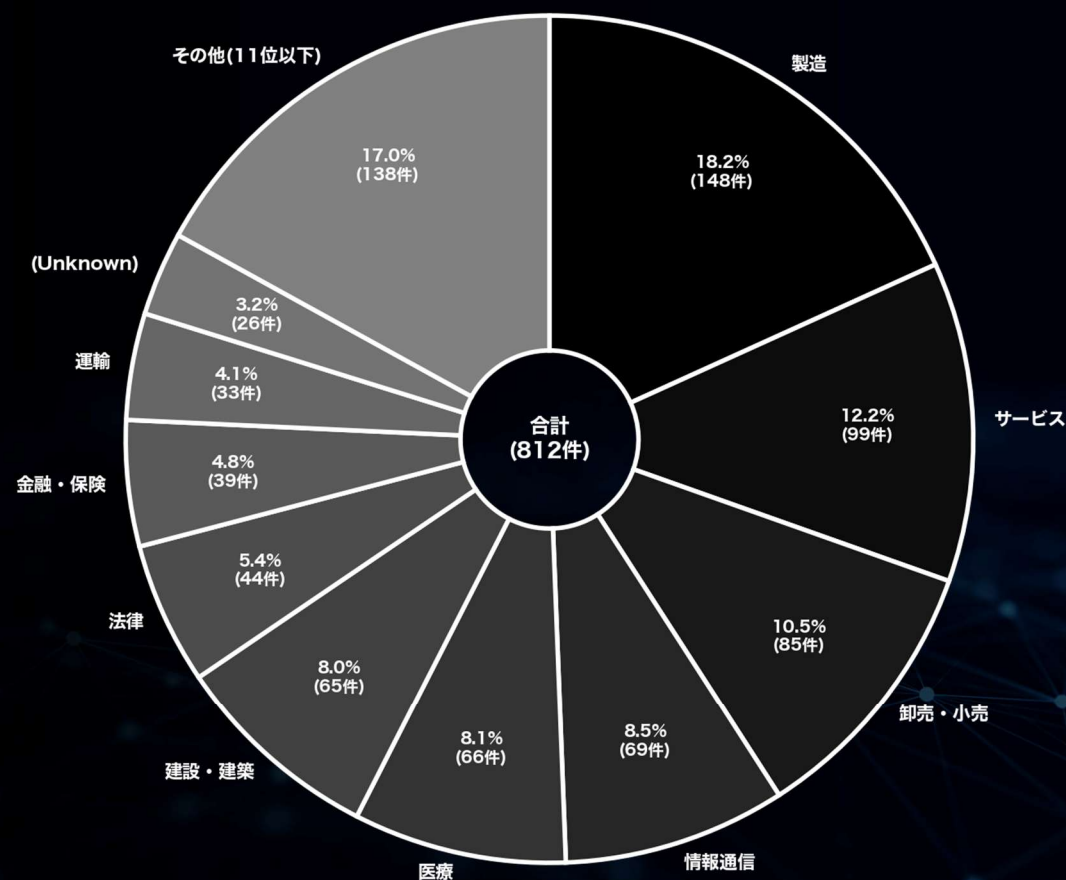
月別内訳 業種 TOP10 (全世界)

(2025年 10 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	148	18.2	+ 47
サービス	99	12.2	+ 48
卸売・小売	85	10.5	+ 56
情報通信	69	8.5	+ 1
医療	66	8.1	+ 18
建設・建築	65	8.0	+ 16
法律	44	5.4	+ 15
金融・保険	39	4.8	- 9
運輸	33	4.1	+ 20
(Unknown)	26	3.2	+ 11

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



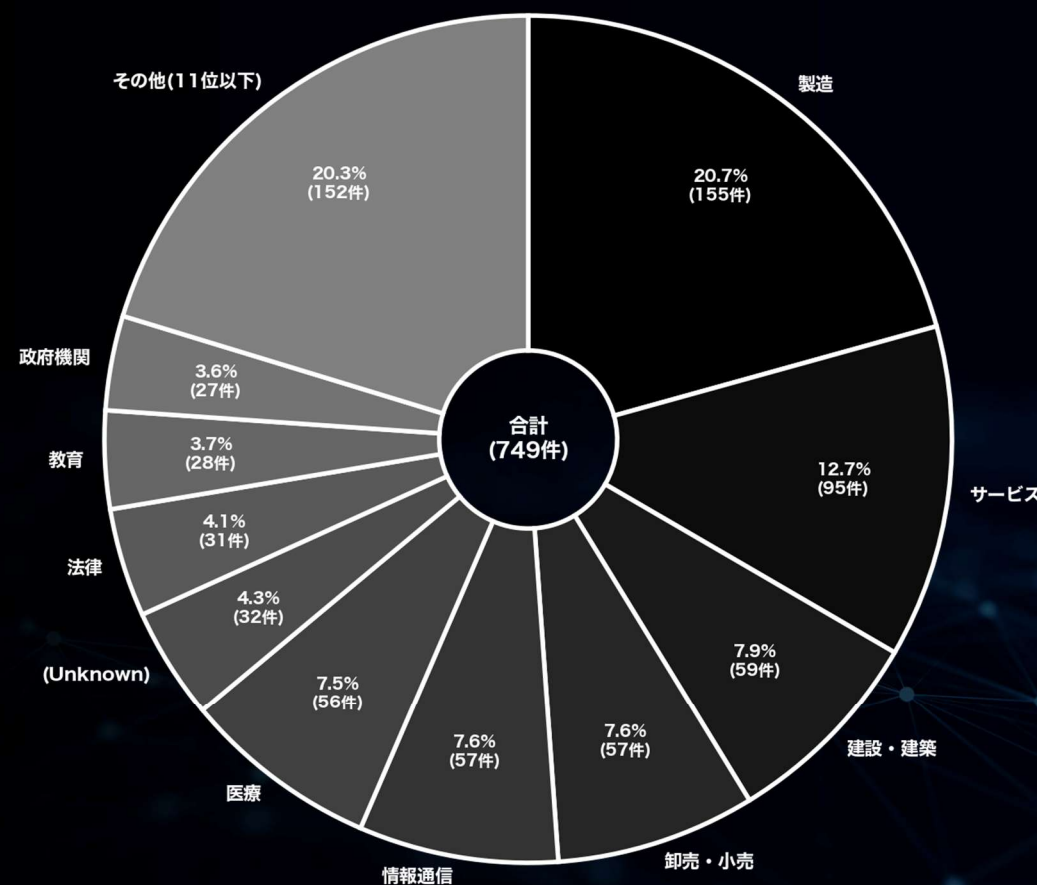
月別内訳 業種 TOP10 (全世界)

(2025年 11 月)

※件数順に降順／同件数のものが含まれる場合は名前順でTOP10までを記載

業種	件数	割合(%)	前月比(件数)
製造	155	20.7	+ 7
サービス	95	12.7	- 4
建設・建築	59	7.9	- 6
卸売・小売	57	7.6	- 28
情報通信	57	7.6	- 12
医療	56	7.5	- 10
(Unknown)	32	4.3	+ 6
法律	31	4.1	- 13
教育	28	3.7	+ 4
政府機関	27	3.6	+ 19

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



被害数の推移に関する統計

(全世界及び国内)

2025

11

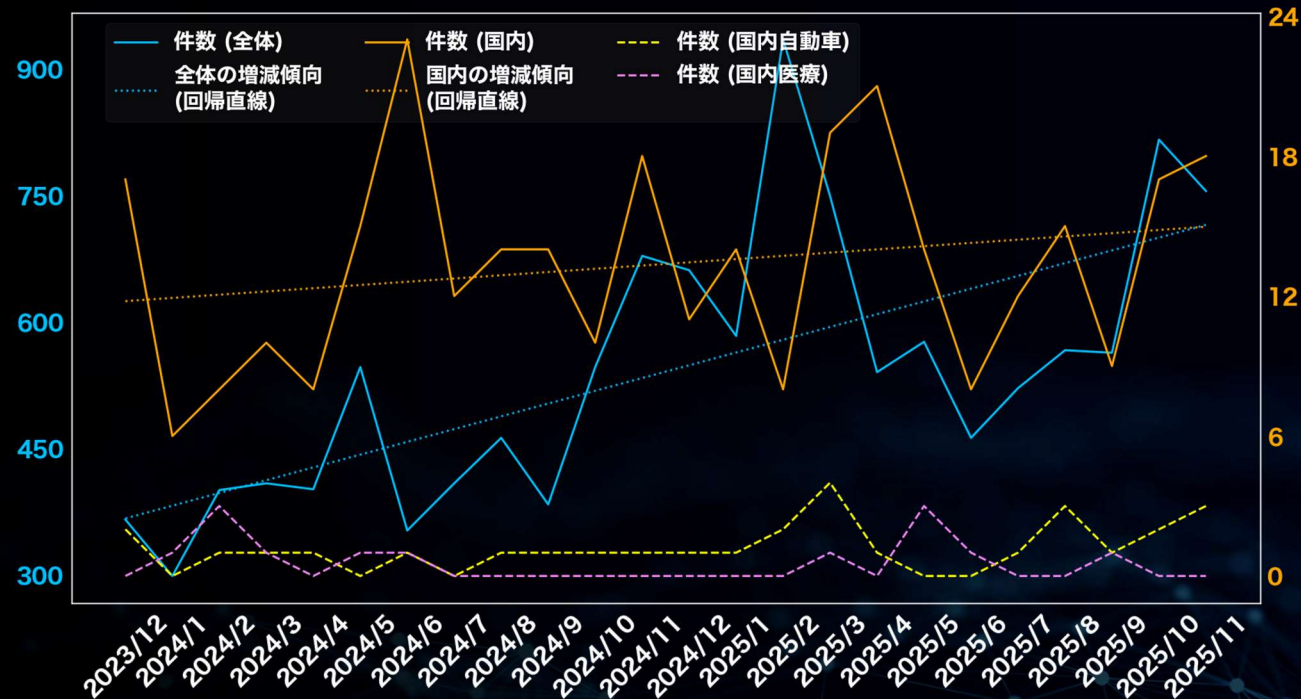
被害数の推移（全世界及び国内） （過去2年間／2023年12月～2025年11月）

※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)
2023/12	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	546	10	1	0
2024/11	678	18	1	0
2024/12	661	11	1	0
2025/1	583	14	1	0
2025/2	935	8	2	0
2025/3	749	19	4	1
2025/4	540	21	1	0
2025/5	576	14	0	3
2025/6	462	8	0	1
2025/7	521	12	1	0
2025/8	566	15	3	0
2025/9	563	9	1	1
2025/10	816	17	2	0
2025/11	755	18	3	0
合計	12974	321	29	13

▼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）

資本金別の統計

(国内)

2025

11

資本金別（国内）

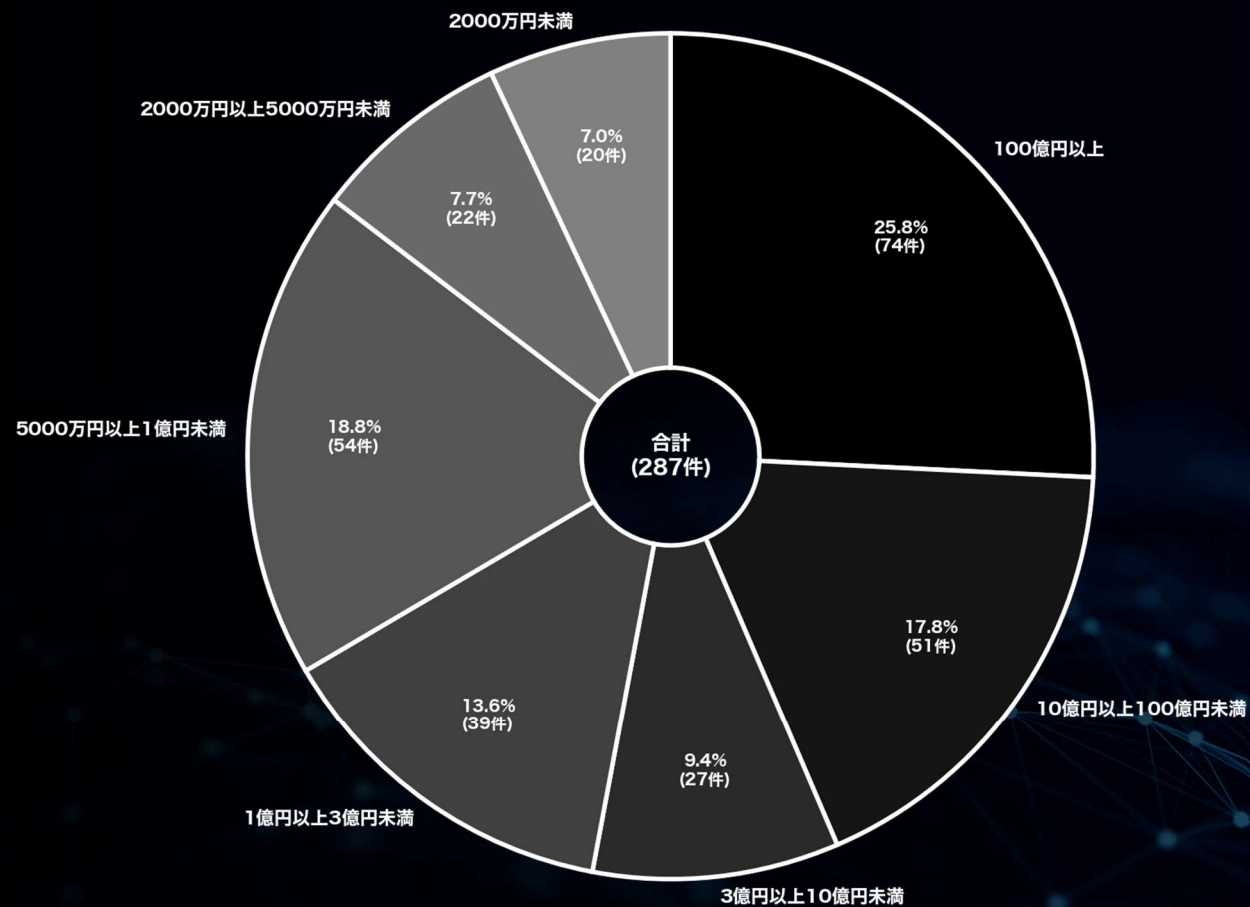
（過去2年間／2023年12月～2025年11月）

※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	74	25.8
10億円以上100億円未満	51	17.8
3億円以上10億円未満	27	9.4
1億円以上3億円未満	39	13.6
5000万円以上1億円未満	54	18.8
2000万円以上5000万円未満	22	7.7
2000万円未満	20	7.0

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）

公表と暴露に関する統計

(国内)

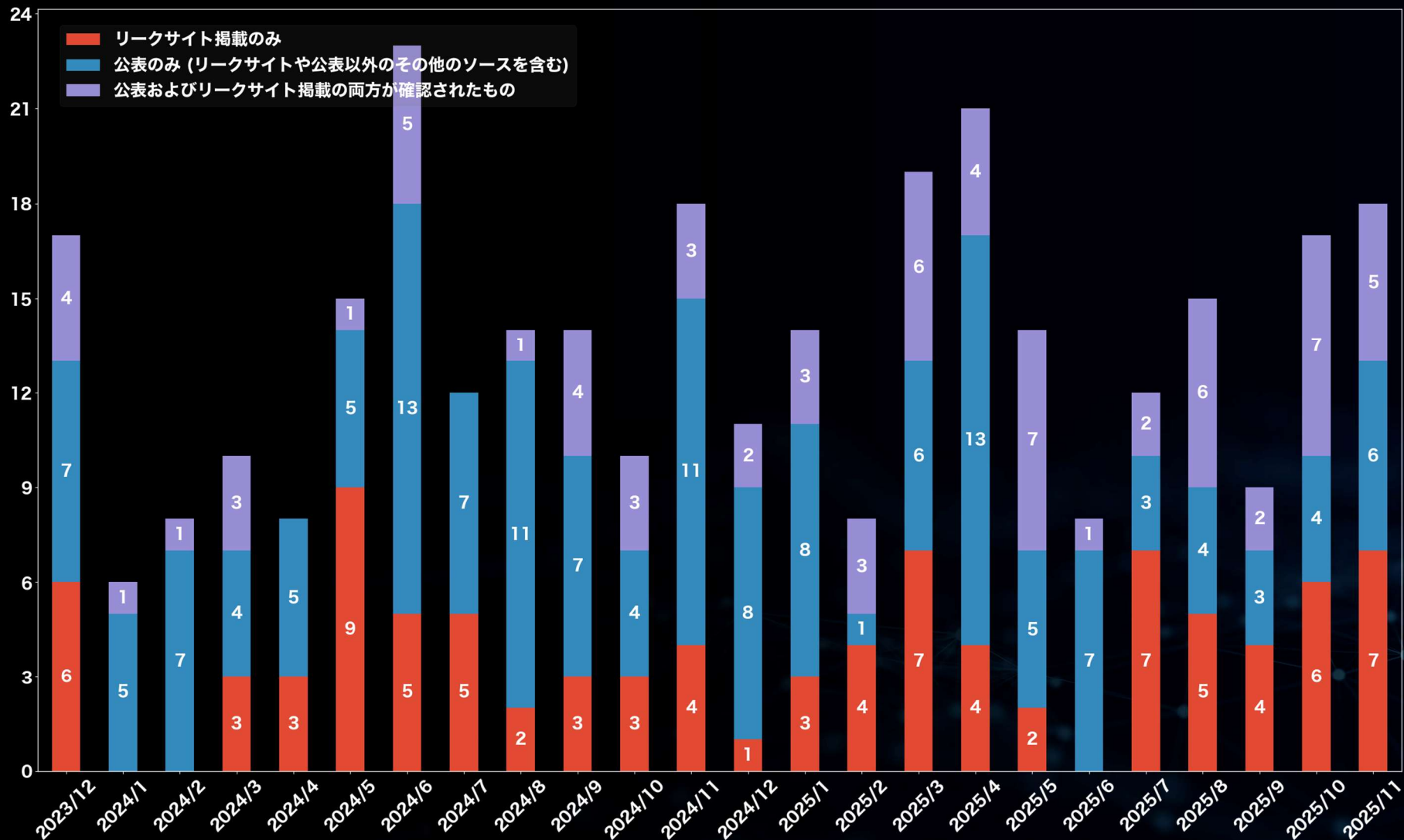
2025

11

公表割合 月別内訳 (国内)

(過去2年間／2023年12月～2025年11月)

▼ランサムウェア攻撃における公表数と掲載数の分析



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

公となった国内被害組織 概要一覧

2025

11

公となった国内被害組織概要一覧 (国内)

(過去1年間／2024年12月～2025年11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
2024/12	(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	CLOP (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)	ソフトウェアメーカー
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
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

被害月	攻撃グループ	業種概要
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	CLOP (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	ポンティングワイヤーメーカー(海外拠点)
2025/3	Qilin (Agenda)	自動制御機器製品メーカー(海外拠点)
2025/3	CACTUS	自動車部品メーカー(海外拠点)
2025/3	(Unknown)	流体制御機器 (バルブ) 製造
2025/3	(Unknown)	ソフトウェア開発
2025/3	Blackout	機器部品メーカー
2025/3	Cicada3301	精密部品メーカー
2025/3	RansomHub	一般機械器具製造業
2025/3	Night Spire	特殊鋼部品メーカー(海外拠点)
2025/3	Night Spire	切削工具メーカー(海外拠点)
2025/3	(Unknown)	百貨店業
2025/3	(Unknown)	鉄鋼製品メーカー(海外拠点)
2025/3	KILLSEC	事務機器メーカー(海外拠点)
2025/4	KILLSEC	情報機器メーカー(海外拠点)
2025/4	AKIRA	大手総合印刷・電子材料メーカー(海外拠点)
2025/4	SARCOMA	大手総合化学メーカー(海外拠点)
2025/4	AKIRA	自動化装置メカ(海外拠点)

被害月	攻撃グループ	業種概要
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

(※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12月～2025年11月)

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

被害月	攻撃グループ	業種概要
2025/5	(Unknown)	特殊鋼・合金メーカー
2025/5	Space Bears	ゴム製品メーカー(海外拠点)
2025/5	PLAY	通信機器メーカー(海外拠点)
2025/6	(Unknown)	錠前・セキュリティ製品の販売
2025/6	(Unknown)	システムインテグレーター
2025/6	Qilin (Agenda)	医療機器メーカー(海外拠点)
2025/6	(Unknown)	ポンプ製造業
2025/6	(Unknown)	大手紳士服チェーン
2025/6	(Unknown)	保険事故調査サービス業
2025/6	(Unknown)	設備工事業
2025/6	(Unknown)	建材・住宅・リフォーム・不動産事業
2025/7	Kawa4096	大手保険会社
2025/7	NightSpire	ゴム製品メーカー(海外拠点)
2025/7	Kawa4096	警備サービス業
2025/7	Dire Wolf	電子デバイス製造・販売(海外拠点)
2025/7	(Unknown)	障害福祉サービス業
2025/7	(Unknown)	衛生管理製品・サービス業
2025/7	INC Ransom	高電圧電気機器メーカー(海外拠点)
2025/7	INC Ransom	ファンデーション資材メーカー
2025/7	LYNX	大手食品メーカー(海外拠点)
2025/7	DEVMAN 2.0	電子部品メーカー
2025/7	SAFEPAY	パレル用補助材料メーカー
2025/7	(Unknown)	知的財産情報提供
2025/8	(Unknown)	ソフトウェア開発
2025/8	Black Nevas	特許事務所
2025/8	D4RK4RMY	大手金融機関
2025/8	Qilin (Agenda)	プラスチック製品製造業
2025/8	Qilin (Agenda)	自動車部品メーカー(海外拠点)

被害月	攻撃グループ	業種概要
2025/8	Qilin (Agenda)	業務用食品卸・加工業
2025/8	(Unknown)	農産物加工・流通
2025/8	Warlock	精密機器メーカー(海外拠点)
2025/8	RansomHouse	電池・電子部品メーカー(海外拠点)
2025/8	Qilin (Agenda)	自動車向けデザイン
2025/8	WORLD LEAKS	毛織物メーカー
2025/8	(Unknown)	業務用・産業用加湿器メーカー
2025/8	(Unknown)	医療・介護事業者向けファクタリング
2025/8	Cephalus	システムインテグレーター
2025/8	Black Nevas	大手自動車メーカー(海外拠点)
2025/9	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)
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

被害月	攻撃グループ	業種概要
2025/10	AKIRA	各種機械鋸・刃物メーカー(海外拠点)
2025/10	(Unknown)	私立学校
2025/10	RansomHouse	有機化学工業品メーカー
2025/10	SAFEPAY	金属加工メーカー
2025/10	(Unknown)	ケーブルテレビ
2025/10	Qilin (Agenda)	食品スーパーマーケット
2025/10	Qilin (Agenda)	総合エネルギー企業
2025/10	Qilin (Agenda)	総合スーパー
2025/10	RansomHouse	大手EC小売事業者
2025/11	(Unknown)	私立大学
2025/11	WORLD LEAKS	プラスチック製品製造業
2025/11	Warlock	サスペンションメーカー
2025/11	Qilin (Agenda)	弁理士法人
2025/11	(Unknown)	システムインテグレーター
2025/11	Qilin (Agenda)	通信機器メーカー
2025/11	CRYPTO24	電子部品メーカー
2025/11	CLOP (CLOP)	ラベル印刷機器メーカー
2025/11	INC Ransom	自動車部品メーカー(海外拠点)
2025/11	(Unknown)	教育委員会
2025/11	(Unknown)	私立学校
2025/11	CLOP (CLOP)	大手精密機器メーカー(海外拠点)
2025/11	CLOP (CLOP)	大手自動車メーカー
2025/11	CLOP (CLOP)	大手総合化学メーカー
2025/11	Sinobi	警報装置メーカー
2025/11	Qilin (Agenda)	大手建設会社(海外拠点)
2025/11	(Unknown)	精密部品製造
2025/11	(Unknown)	国際総合検定機関

(※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12月～2025年11月)

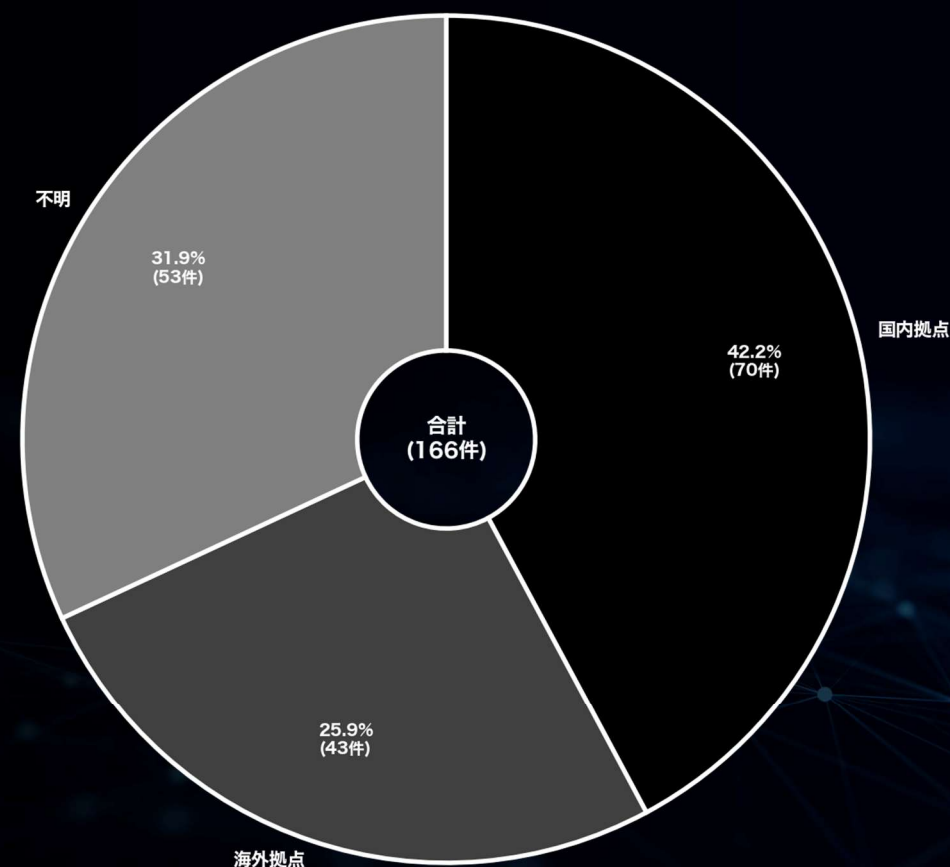
(※左下の補足記載のとおり、リークサイトへの掲載や公表から確認ができた被害組織に限定し算出された値である事にあらためて注意)

▼ランサムウェア攻撃を受けた日本関連組織の拠点別割合

※

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

拠点	件数	割合(%)
国内拠点	70	42.2
海外拠点	43	25.9
不明	53	31.9



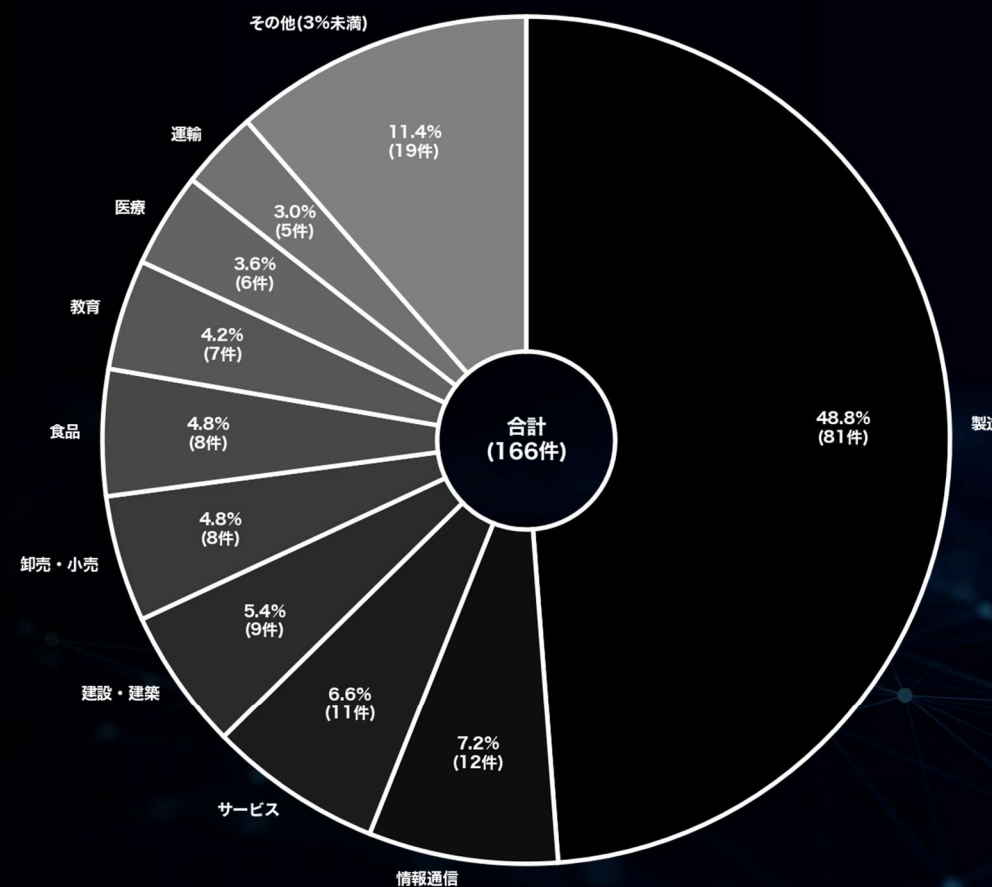
(※本ページの表／グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

公となった国内被害組織における業種割合 (国内)

(過去1年間／2024年12月～2025年11月)

▼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

業種	件数	割合(%)
製造	81	48.8
情報通信	12	7.2
サービス	11	6.6
建設・建築	9	5.4
卸売・小売	8	4.8
食品	8	4.8
教育	7	4.2
医療	6	3.6
運輸	5	3.0
その他(3%未満)	19	11.4



(※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)

2025

11

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・小規模事業者の定義」:<https://www.chusho.meti.go.jp/soshiki/teigi.html>

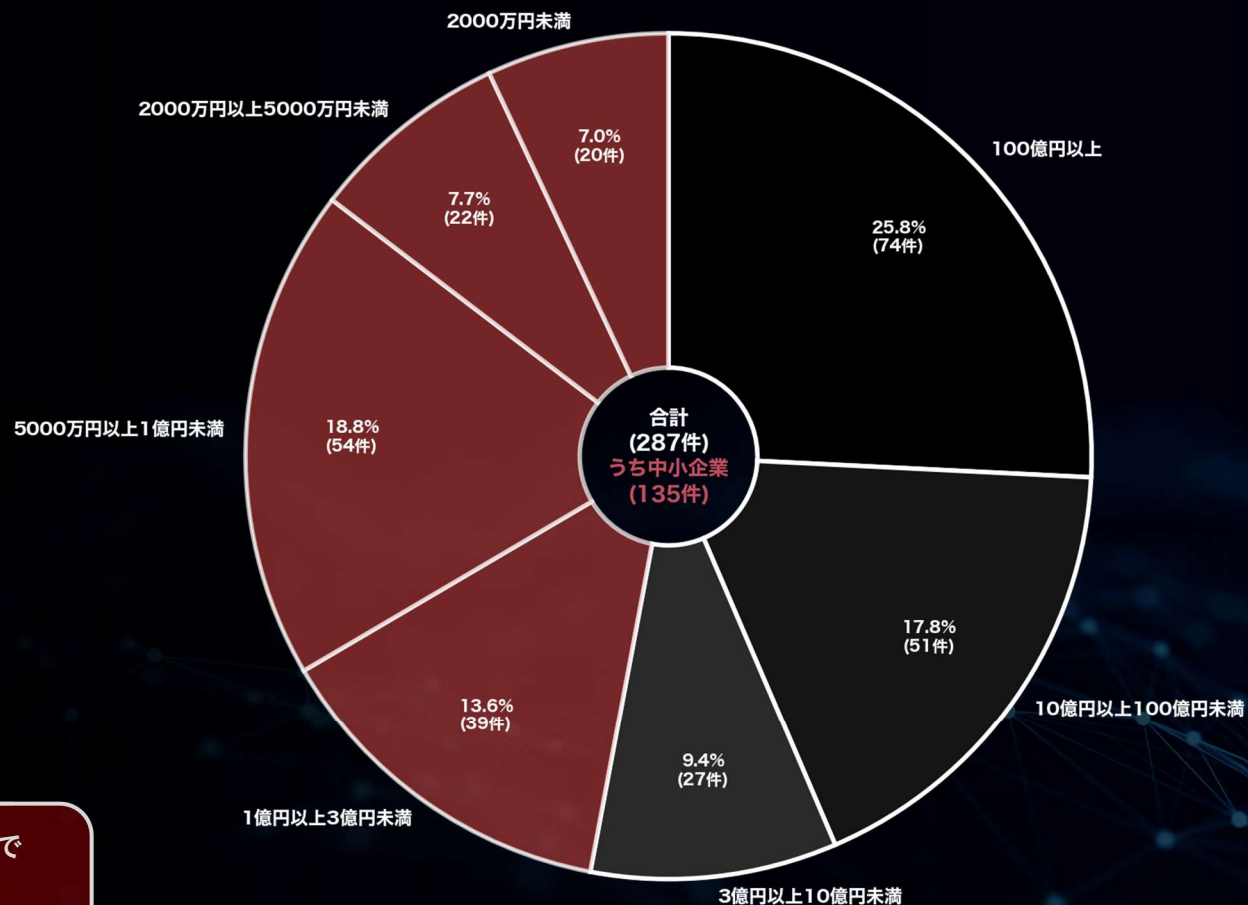
資本金別（国内-中小企業） （過去2年間／2023年12月～2025年11月）

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	74	25.8
10億円以上100億円未満	51	17.8
3億円以上10億円未満	27	9.4
1億円以上3億円未満	39	13.6
5000万円以上1億円未満	54	18.8
2000万円以上5000万円未満	22	7.7
2000万円未満	20	7.0

▼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135件にのぼり、全体の47.1%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。

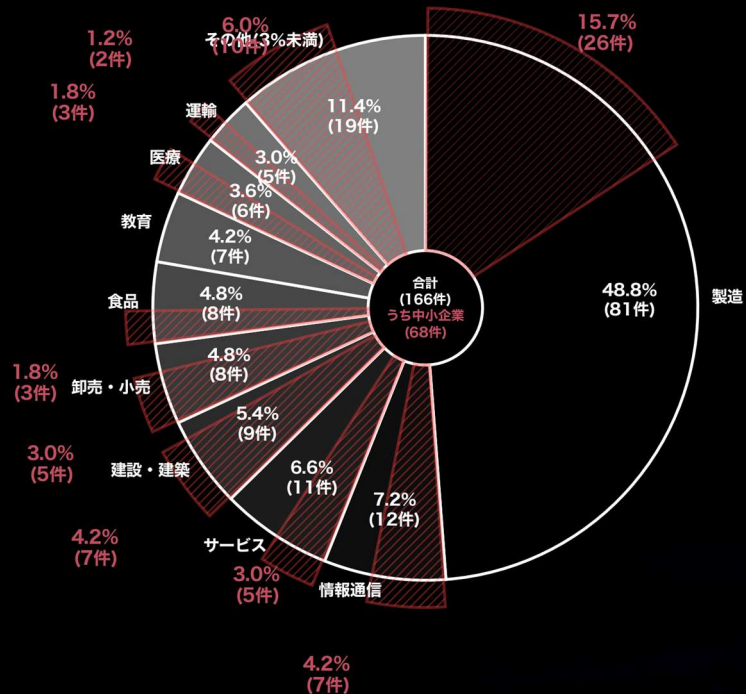
（※本ページの表／グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している）

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12月～2025年11月)

赤色は中小企業を示す

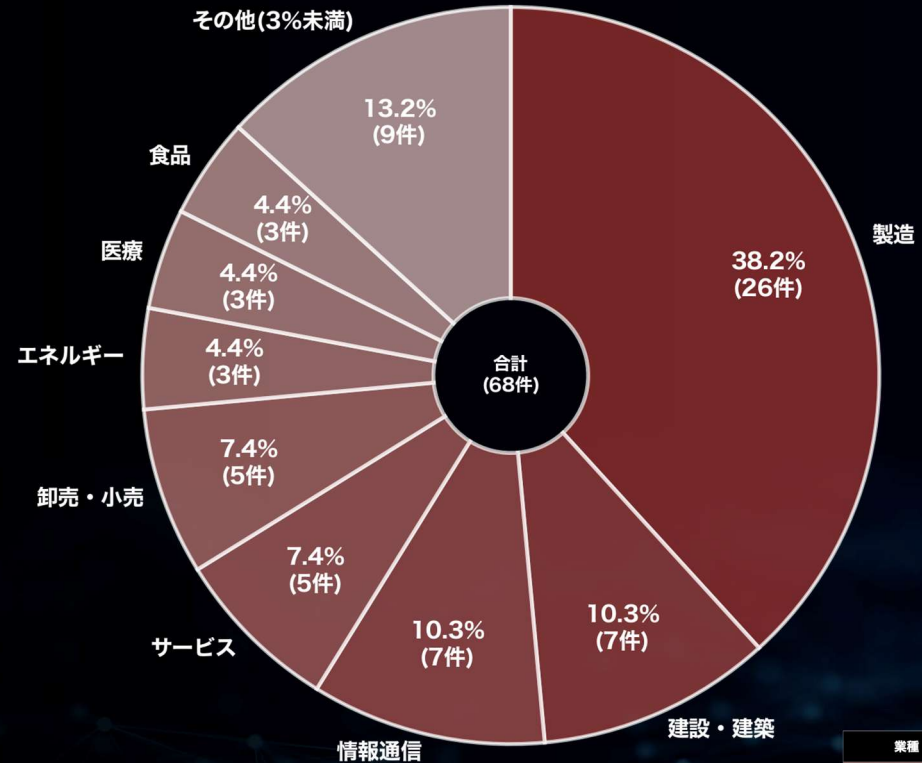
▼全体割合



※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	81 (26)	48.8 (15.7)
情報通信	12 (7)	7.2 (4.2)
サービス	11 (5)	6.6 (3.0)
建設・建築	9 (7)	5.4 (4.2)
卸売・小売	8 (5)	4.8 (3.0)
食品	8 (3)	4.8 (1.8)
教育	7	4.2
医療	6 (3)	3.6 (1.8)
運輸	5 (2)	3.0 (1.2)
その他(3%未満)	19 (10)	11.4 (6.0)

▼中小企業のための割合



業種	件数	割合(%)
製造	26	38.2
建設・建築	7	10.3
情報通信	7	10.3
サービス	5	7.4
卸売・小売	5	7.4
エネルギー	3	4.4
医療	3	4.4
食品	3	4.4
その他(3%未満)	9	13.2

過去1年間の業種別分析においては、中小企業だけに抜粋すると、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。

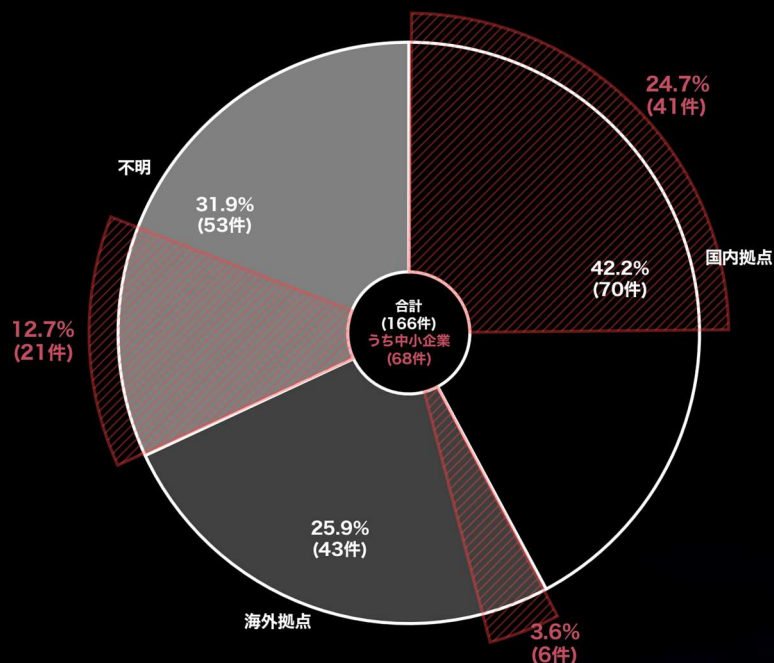
※医療や教育、行政機関など資本金が不明な一部の組織については集計から除外

(※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)

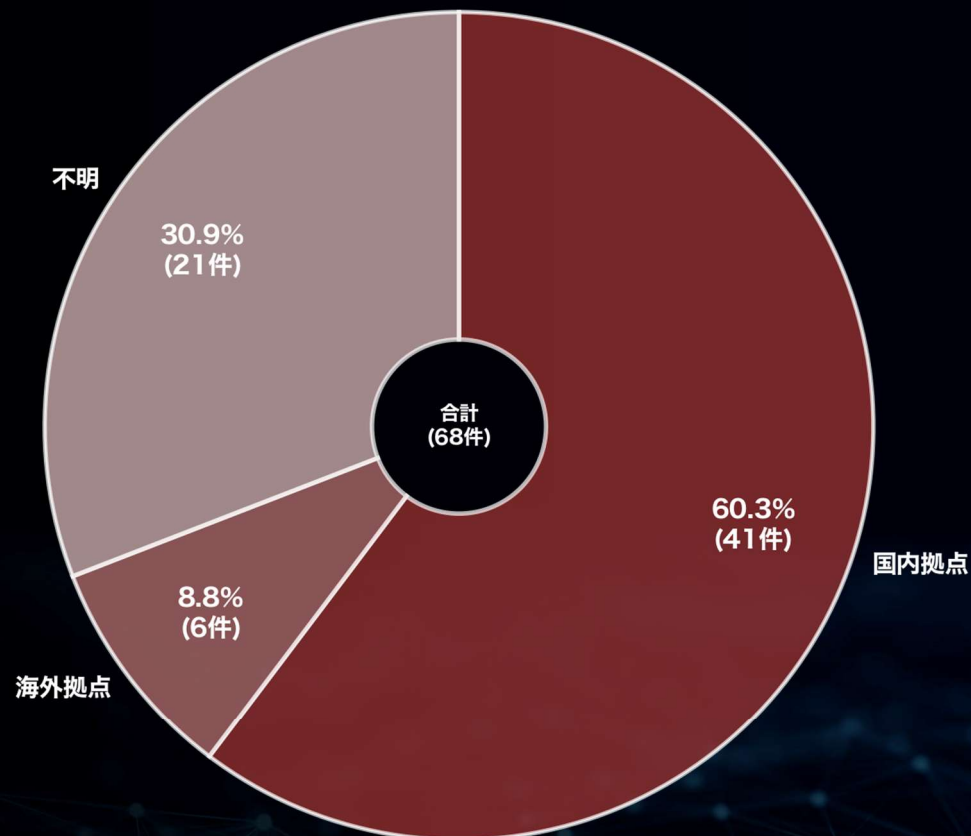
公となった国内被害組織における拠点割合（国内-中小企業） （過去1年間／2024年12月～2025年11月）

赤色は中小企業を示す

▼全体割合



▼中小企業のための割合



※

「国内拠点」：公表等により、国内拠点における被害事案と判断されるケース数
「海外拠点」：公表等により、海外拠点（支社／関係会社）における被害事案と判断されるケース数
「不明」：上記以外、被害拠点の地域的情報が得られなかったケース数
※各数値の()内の数値は、資本金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	70 (41)	42.2 (24.7)
海外拠点	43 (6)	25.9 (3.6)
不明	53 (21)	31.9 (12.7)
合計	166 (68)	100 (41.0)

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	60.3
海外拠点	6	8.8
不明	21	30.9

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12月～2025年11月)

赤色は中小企業を示す

被害月	攻撃グループ	業種概要
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	CLOP (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)	ソフトウェアメーカー
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
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

被害月	攻撃グループ	業種概要
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	CLOP (CLOP)	自動車部品メーカー
2025/3	(Unknown)	粘着テープ製造(海外拠点)
2025/3	Qilin (Agenda)	医療機関
2025/3	RansomHub	リビルド品製造
2025/3	(Unknown)	不動産仲介
2025/3	Night Spire	塗料メーカー
2025/3	Qilin (Agenda)	産業用機器メーカー(海外拠点)
2025/3	Night Spire	ボンディングワイヤメーカー(海外拠点)
2025/3	Qilin (Agenda)	自動制御機器製品メーカー(海外拠点)
2025/3	CACTUS	自動車部品メーカー(海外拠点)
2025/3	(Unknown)	流体制御機器 (バルブ) 製造
2025/3	(Unknown)	ソフトウェア開発
2025/3	Blackout	機器部品メーカー
2025/3	Cicada3301	精密部品メーカー
2025/3	RansomHub	一般機械器具製造業
2025/3	Night Spire	特殊鋼部品メーカー(海外拠点)
2025/3	Night Spire	切削工具メーカー(海外拠点)
2025/3	(Unknown)	百貨店業
2025/3	(Unknown)	鉄鋼製品メーカー(海外拠点)
2025/3	KILLSEC	事務機器メーカー(海外拠点)
2025/4	KILLSEC	情報機器メーカー(海外拠点)
2025/4	AKIRA	大手総合印刷・電子材料メーカー(海外拠点)
2025/4	SARCOMA	大手総合化学メーカー(海外拠点)
2025/4	AKIRA	自動化装置メカ(海外拠点)

被害月	攻撃グループ	業種概要
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

※ (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。

※ 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12月～2025年11月)

赤色は中小企業を示す

被害月	攻撃グループ	業種概要
2025/5	(Unknown)	特殊鋼・合金メーカー
2025/5	Space Bears	ゴム製品メーカー(海外拠点)
2025/5	PLAY	通信機器メーカー(海外拠点)
2025/6	(Unknown)	錠前・セキュリティ製品の販売
2025/6	(Unknown)	システムインテグレーター
2025/6	Qilin (Agenda)	医療機器メーカー(海外拠点)
2025/6	(Unknown)	ポンプ製造業
2025/6	(Unknown)	大手紳士服チェーン
2025/6	(Unknown)	保険事故調査サービス業
2025/6	(Unknown)	設備工事業
2025/6	(Unknown)	建材・住宅・リフォーム・不動産事業
2025/7	Kawa4096	大手保険会社
2025/7	NightSpire	ゴム製品メーカー(海外拠点)
2025/7	Kawa4096	警備サービス業
2025/7	Dire Wolf	電子デバイス製造・販売(海外拠点)
2025/7	(Unknown)	障害福祉サービス業
2025/7	(Unknown)	衛生管理製品・サービス業
2025/7	INC Ransom	高電圧電気機器メーカー(海外拠点)
2025/7	INC Ransom	ファンデーション資材メーカー
2025/7	LYNX	大手食品メーカー(海外拠点)
2025/7	DEVMAN 2.0	電子部品メーカー
2025/7	SAFEPAY	パレル用補助材料メーカー
2025/7	(Unknown)	知的財産情報提供
2025/8	(Unknown)	ソフトウェア開発
2025/8	Black Nevas	特許事務所
2025/8	D4RK4RMY	大手金融機関
2025/8	Qilin (Agenda)	プラスチック製品製造業
2025/8	Qilin (Agenda)	自動車部品メーカー(海外拠点)

被害月	攻撃グループ	業種概要
2025/8	Qilin (Agenda)	業務用食品卸・加工業
2025/8	(Unknown)	農産物加工・流通
2025/8	Warlock	精密機器メーカー(海外拠点)
2025/8	RansomHouse	電池・電子部品メーカー(海外拠点)
2025/8	Qilin (Agenda)	自動車向けデザイン
2025/8	WORLD LEAKS	毛織物メーカー
2025/8	(Unknown)	業務用・産業用加湿器メーカー
2025/8	(Unknown)	医療・介護事業者向けファクタリング
2025/8	Cephalus	システムインテグレーター
2025/8	Black Nevas	大手自動車メーカー(海外拠点)
2025/9	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)
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

被害月	攻撃グループ	業種概要
2025/10	AKIRA	各種機械鋸・刃物メーカー(海外拠点)
2025/10	(Unknown)	私立学校
2025/10	RansomHouse	有機化学工業品メーカー
2025/10	SAFEPAY	金属加工メーカー
2025/10	(Unknown)	ケーブルテレビ
2025/10	Qilin (Agenda)	食品スーパーマーケット
2025/10	Qilin (Agenda)	総合エネルギー企業
2025/10	Qilin (Agenda)	総合スーパー
2025/10	RansomHouse	大手EC小売事業者
2025/11	(Unknown)	私立大学
2025/11	WORLD LEAKS	プラスチック製品製造業
2025/11	Warlock	サスペンションメーカー
2025/11	Qilin (Agenda)	弁理士法人
2025/11	(Unknown)	システムインテグレーター
2025/11	Qilin (Agenda)	通信機器メーカー
2025/11	CRYPTO24	電子部品メーカー
2025/11	CLOP (CLOP)	ラベル印刷機器メーカー
2025/11	INC Ransom	自動車部品メーカー(海外拠点)
2025/11	(Unknown)	教育委員会
2025/11	(Unknown)	私立学校
2025/11	CLOP (CLOP)	大手精密機器メーカー(海外拠点)
2025/11	CLOP (CLOP)	大手自動車メーカー
2025/11	CLOP (CLOP)	大手総合化学メーカー
2025/11	Sinobi	警報装置メーカー
2025/11	Qilin (Agenda)	大手建設会社(海外拠点)
2025/11	(Unknown)	精密部品製造
2025/11	(Unknown)	国際総合検定機関

※ (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。

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

※ 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

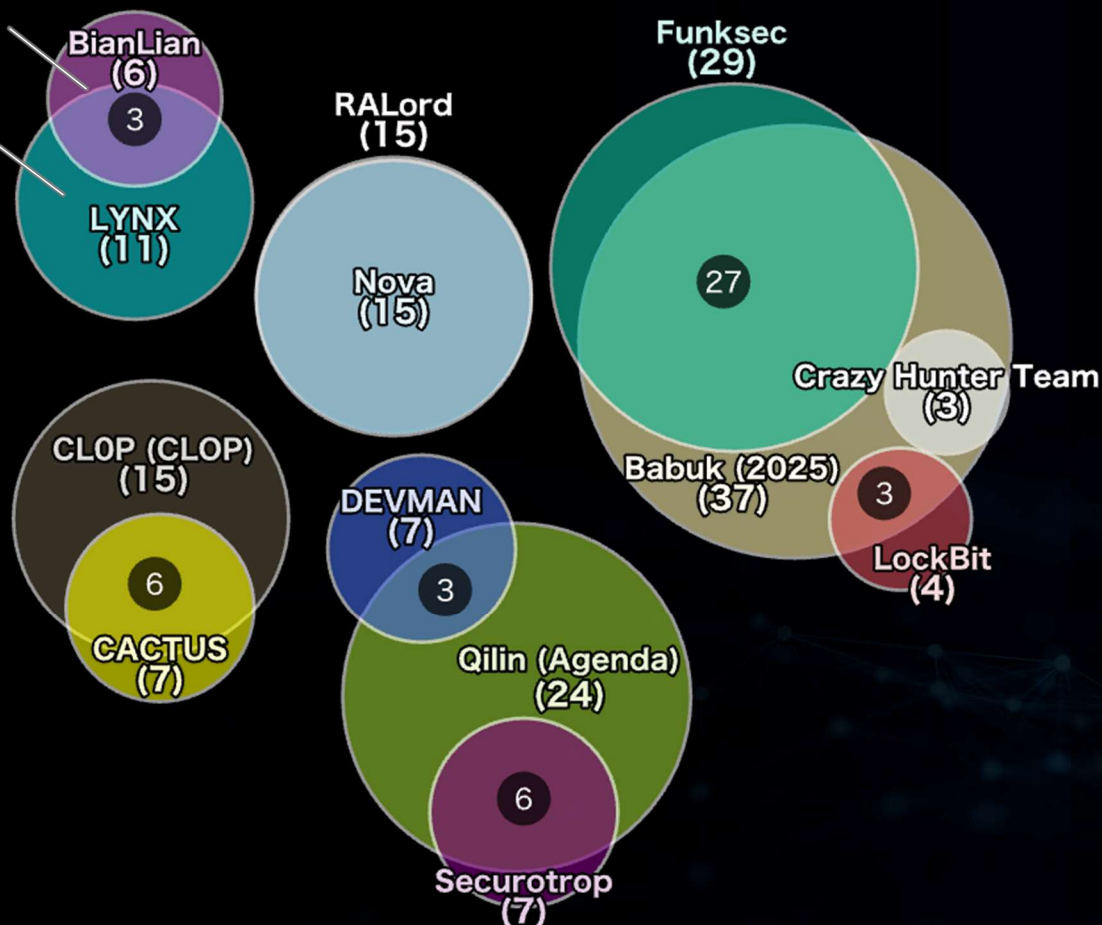
11

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12月～2025年11月) (累計155件) ※多重被害に遭った組織数の累計

※ 円の重なりは他攻撃グループと3件以上の重なりを表している。

※ 重なりのない部分は他攻撃グループと3件未満の事案の重複を表している。



ランサムウェア攻撃の被害の中には、データを盗まれたのちにリークサイトで暴露され、さらに異なる攻撃グループのリークサイトなどから二度三度と繰り返し暴露されるケースがある。

つまり言い換えると、ランサムウェア攻撃の被害組織の中には、複数回にわたってリークサイトに情報が掲載される「多重被害」に遭う組織が存在する。

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。

※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

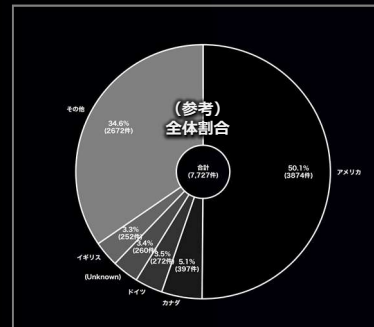
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

多重被害に遭った被害組織の傾向と分析 (全世界)

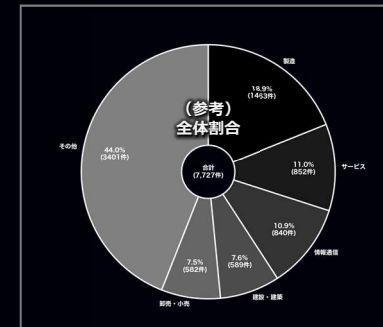
(過去1年間／2024年12月～2025年11月)

※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

(参考比較) 同期間の全データにおける割合



(参考比較) 同期間の全データにおける割合

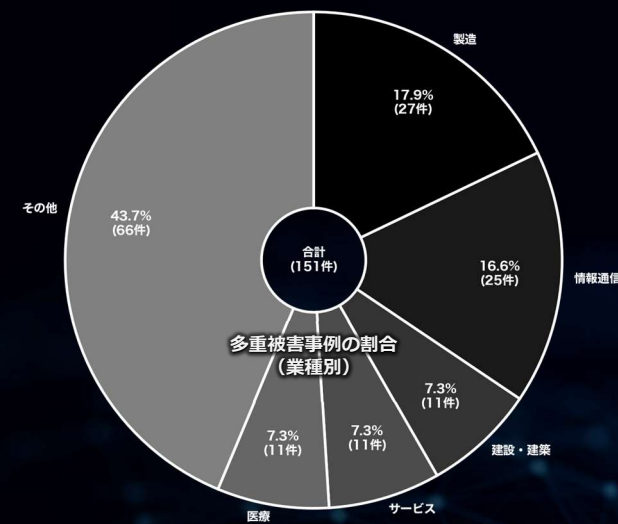
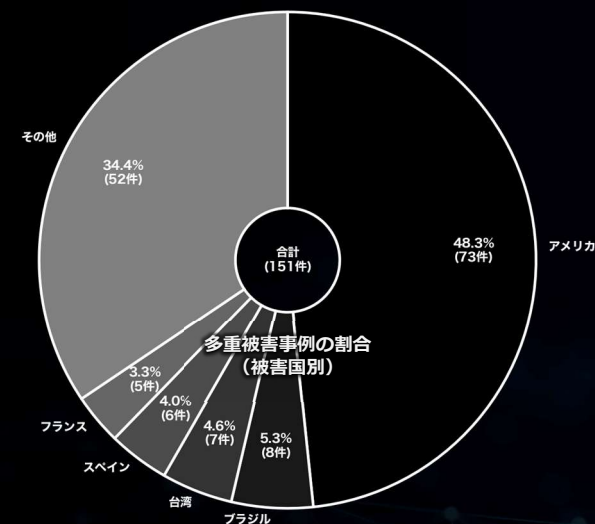
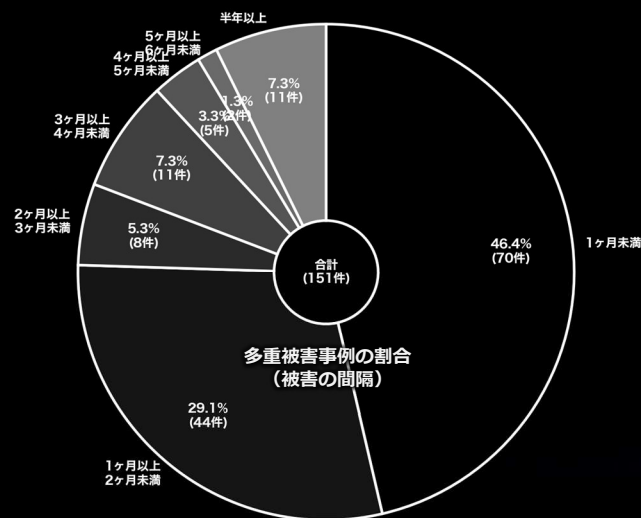


▼被害の間隔

(一度目の被害から二度目の被害までの間隔)

▼被害国別

▼業種別



▶多重被害に遭った組織数の累計：151件 (全体7727件中)

※異なる攻撃グループによるリークサイトへの掲載件数を元に算出

全体母数からの割合は少ないものの、一度ランサムウェア攻撃を受けた被害組織は、異なる時期に異なる攻撃グループによって再びリークサイトへ掲載される被害を繰り返す場合があり、中には3回以上被害に遭うケースもある。これは事後対応が不十分で再び侵入されるケースや、流出した暴露データが裏で共有・拡散され繰り返し脅されるケースなどの背景があると考えられる。被害国や業種の観点ではほぼ全体割合の縮図となっているものの、最も注目すべきは繰り返される「被害の間隔」であり、実に70%以上が一度目の掲載から2ヶ月以内に再び発生していることが判明した。これら多重被害の事例には日本関連の組織も含まれており、一度侵入されデータ窃取されれば、いかなる組織でも多重被害に遭う可能性がある事を示す。こうした被害を防ぐためには、日頃からの対策に加え万が一ランサムウェアの被害に遭っても身代金を支払わない(脅せば支払う組織であると認知されてしまう)ことや、繰り返しの侵入を防ぐために侵入経路の徹底的な洗い出し等の事後対応・再発防止策の実施が不可欠である。

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)

2025

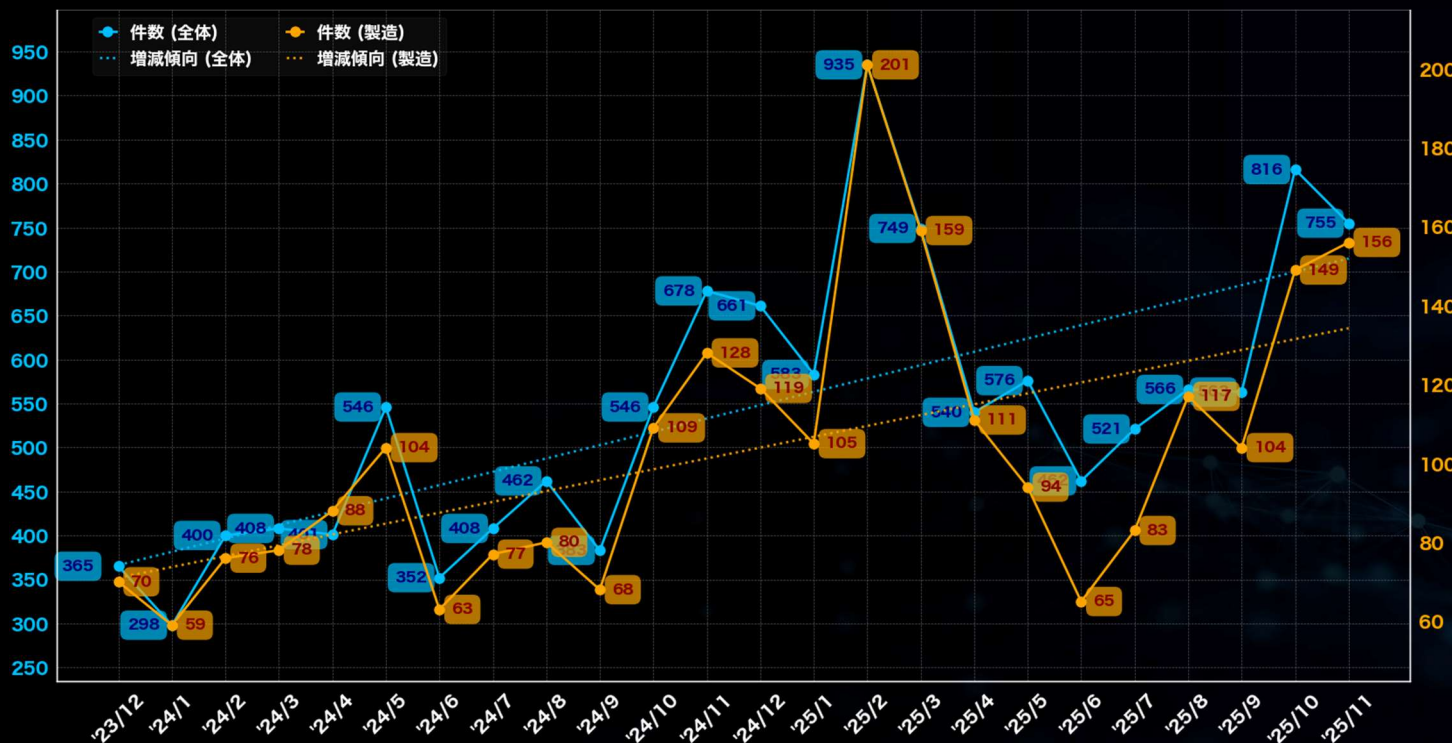
11

業種に関する分析 (全世界)

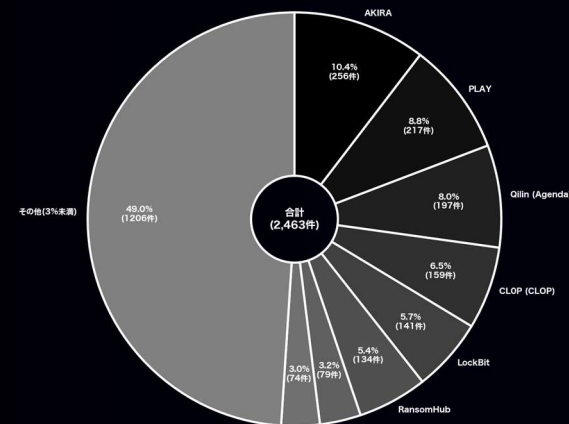
(過去2年間／2023年12月～2025年11月)

製造

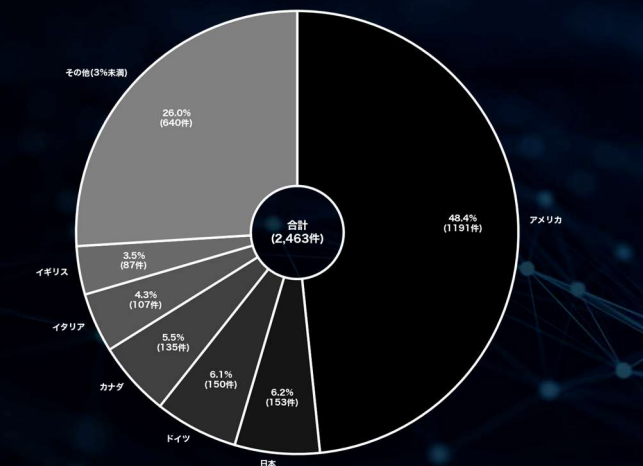
「製造」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、201件の掲載があった。一方、最も少なかった月は2024年1月で、59件であった。被害組織の所在国の割合では、アメリカが約48%と最も多く、次いで日本とドイツがそれぞれ約6%である。攻撃グループについては、少なくとも127のグループが関与しており、特に「AKIRA」が256件のリークサイト掲載を実施している。次いで「PLAY」と「Qilin (Agenda)」がそれぞれ217件と197件の掲載を行っている。製造関連の件数は全体件数に対して高い割合で推移しており、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、長年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



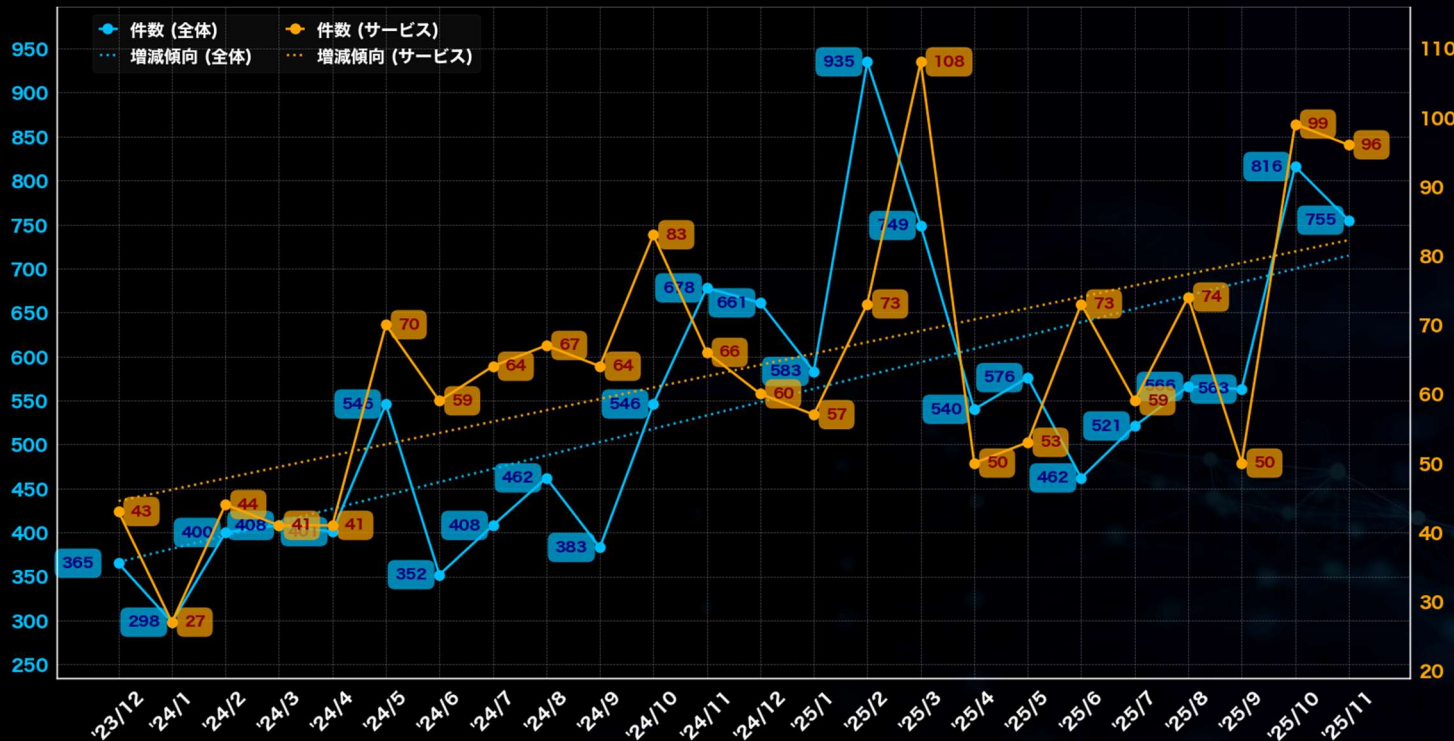
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

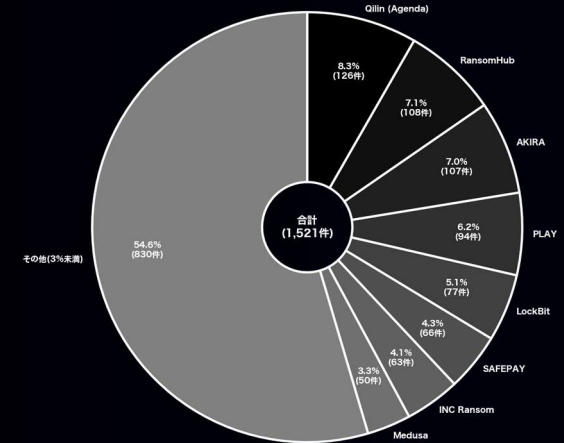
(過去2年間／2023年12月～2025年11月)

サービス

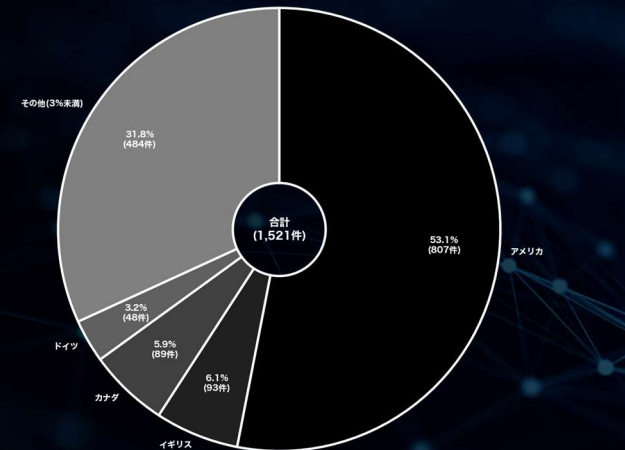
「サービス」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年3月で、108件の掲載があった。一方、最も少なかった月は2024年1月で、27件であった。被害組織の所在国の割合では、アメリカが約53%と最も多く、次いでイギリスとカナダがそれぞれ約6%である。攻撃グループについては、少なくとも123のグループが関与しており、特に「Qilin (Agenda)」が126件のリークサイト掲載を実施している。次いで「RansomHub」と「AKIRA」がそれぞれ108件と107件の掲載を行っている。サービス関連の件数は製造関連と同じく全体件数に対し、高い割合をキープしており、年々その割合は高まっている。



▼攻撃グループ別



▼国別



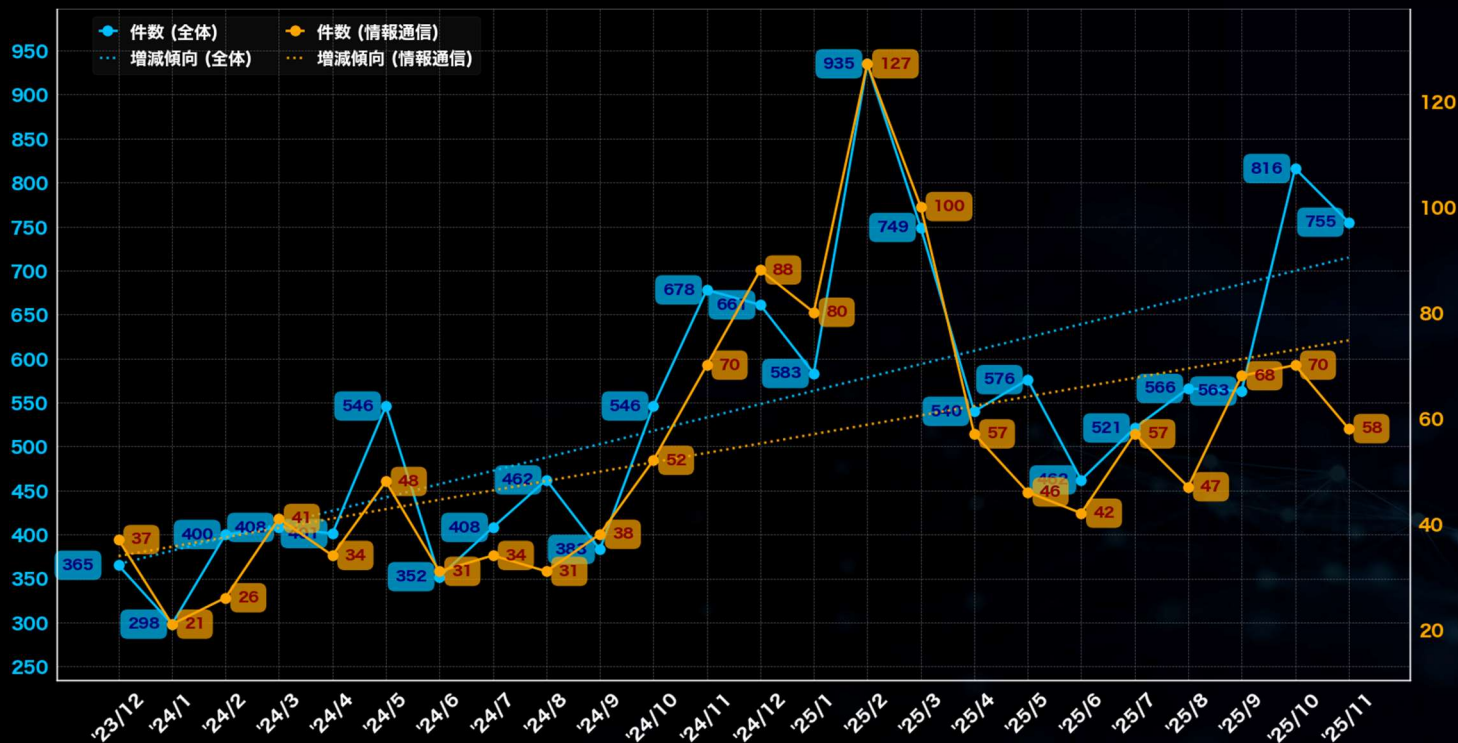
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

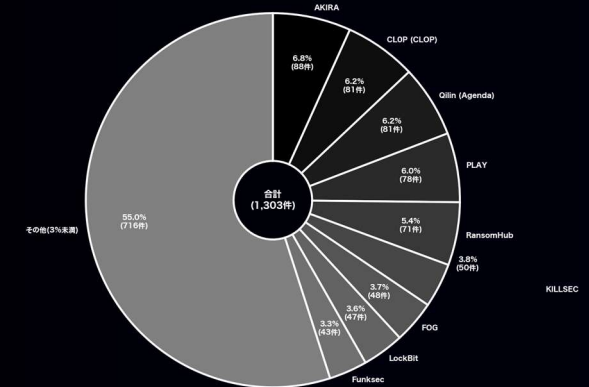
(過去2年間／2023年12月～2025年11月)

情報通信

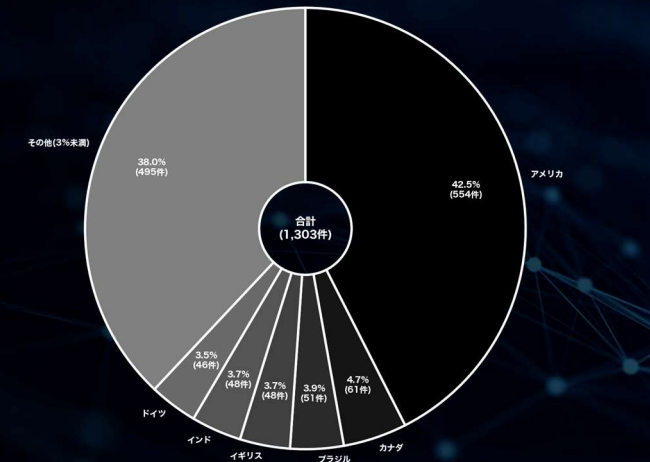
「情報通信」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、127件の掲載があった。一方、最も少なかった月は2024年1月で、21件であった。被害組織の所在国の割合では、アメリカが約43%と最も多く、次いでカナダとブラジルがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも127のグループが関与しており、特に「AKIRA」が88件のリークサイト掲載を実施している。次いで「CLOP (CLOP)」と「Qilin (Agenda)」とがそれぞれ81件の掲載を行っている。過去2年間におけるリークサイト掲載件数は明確な増加傾向にある。



▼攻撃グループ別



▼国別



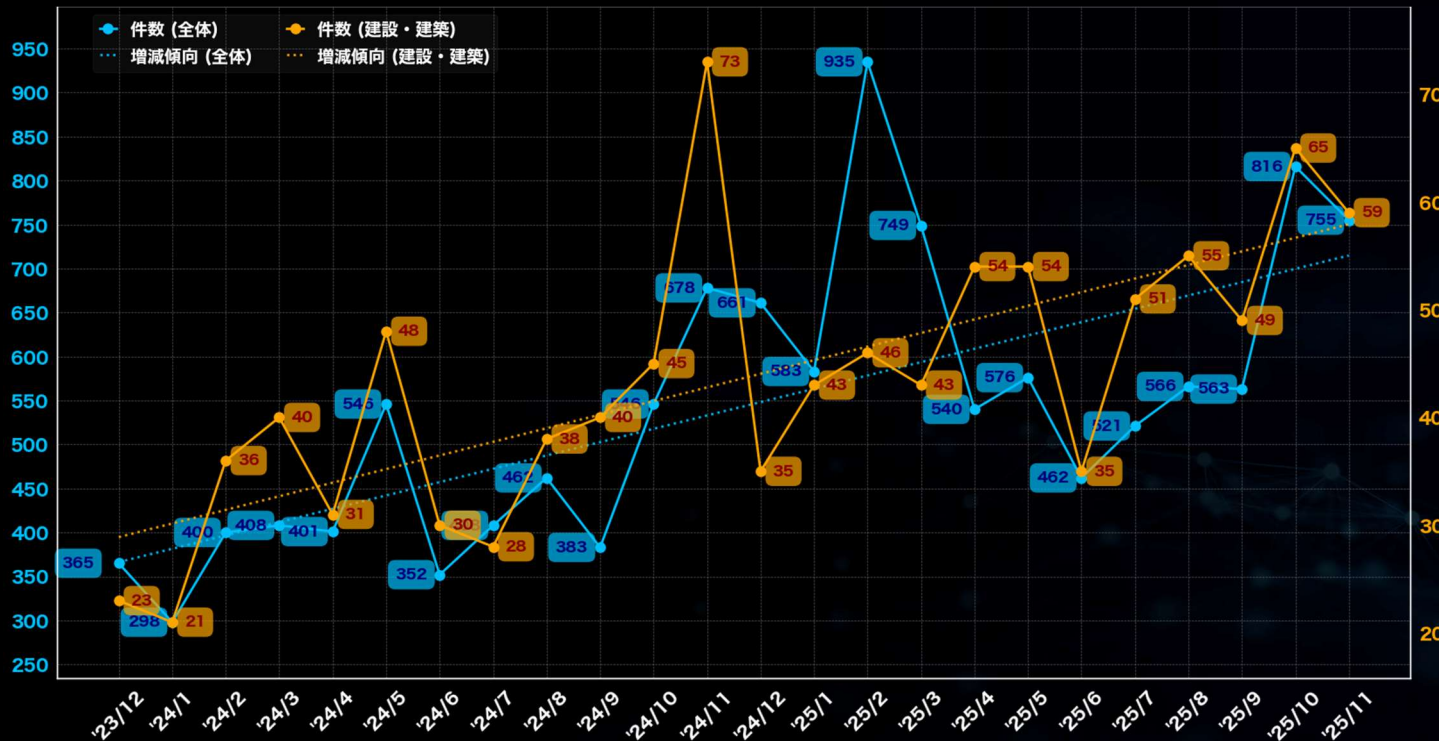
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

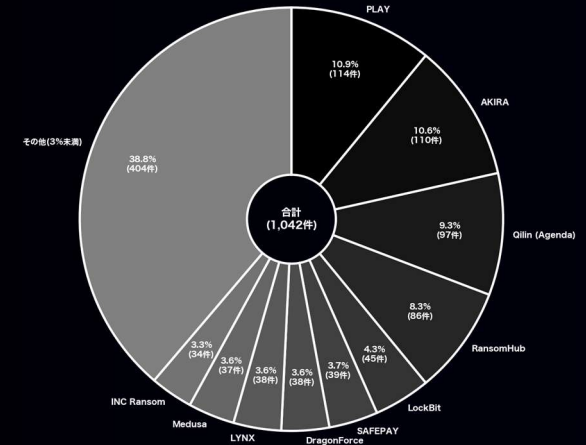
(過去2年間／2023年12月～2025年11月)

建設・建築

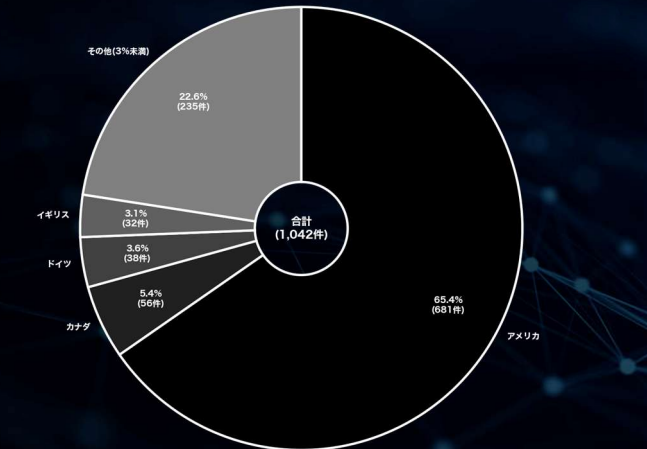
「建設・建築」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最もかった月は2024年11月で、73件の掲載があった。一方、最も少なかった月は2024年1月で、21件であった。被害組織の所在国の割合では、アメリカが約65%と最も多く、次いでカナダとドイツがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも97のグループが関与しており、特に「PLAY」が114件のリークサイト掲載を実施している。次いで「AKIRA」と「Qilin (Agenda)」がそれぞれ110件と97件の掲載を行っている。製造関連などと比べると件数は少ないものの、明確な増加傾向にある。



▼攻撃グループ別



▼国別



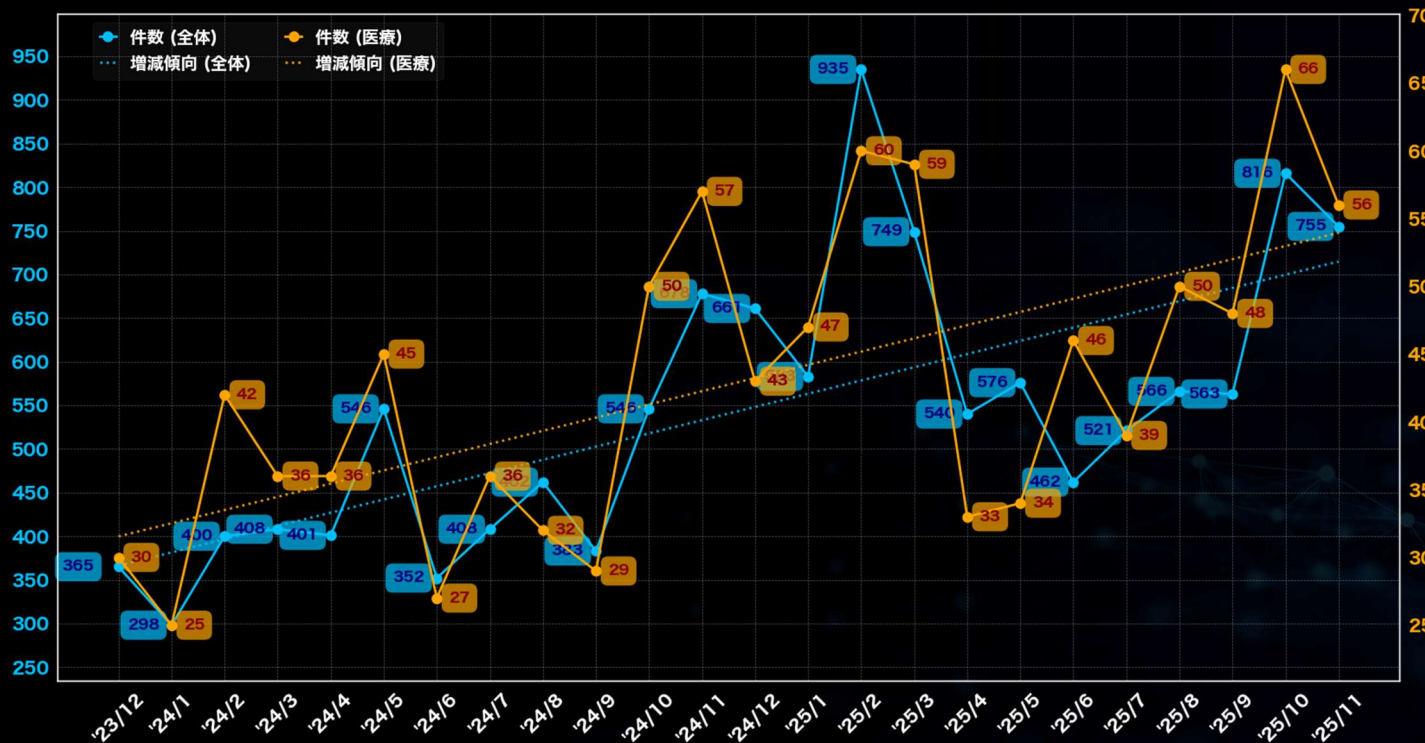
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

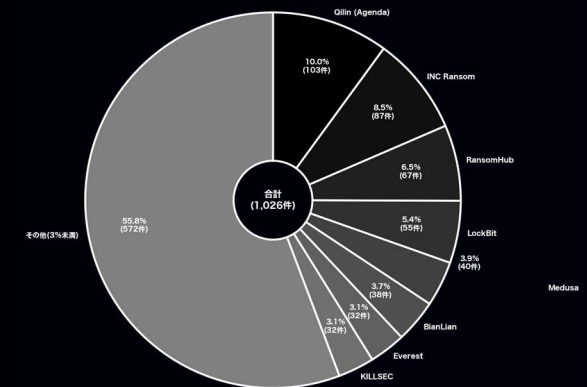
(過去2年間／2023年12月～2025年11月)

医療

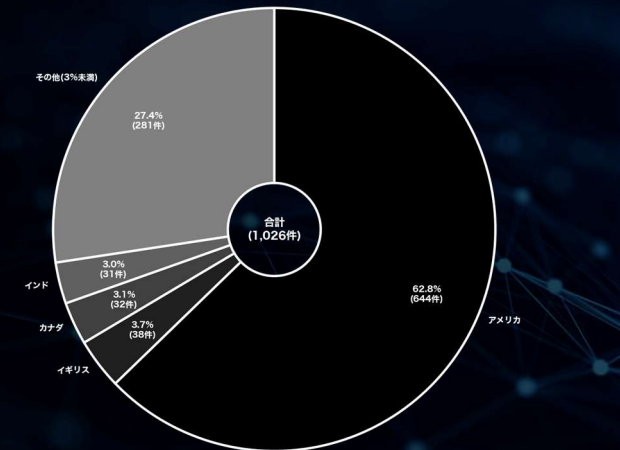
「医療」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年10月で、66件の掲載があった。一方、最も少なかった月は2024年1月で、25件であった。被害組織の所在国の割合では、アメリカが約63%と最も多く、次いでイギリス、カナダがそれぞれ約4%と約3%である。攻撃グループについては、少なくとも108のグループが関与しており、特に「Qilin (Agenda)」が103件のリークサイト掲載を実施している。次いで「INC Ransom」と「RansomHub」がそれぞれ87件と67件の掲載を行っている。かつては低水準だった医療関連の被害数は2023年3月頃に増加し、その後も高い水準が維持が継続している。この変化の背景には、攻撃グループが生存競争の中で業種を問わない攻撃へと方針を転換していった可能性も否定できない。また、国別に見る傾向としてアメリカにおける被害が非常に高い割合を占めている点が顕著である。



▼攻撃グループ別



▼国別



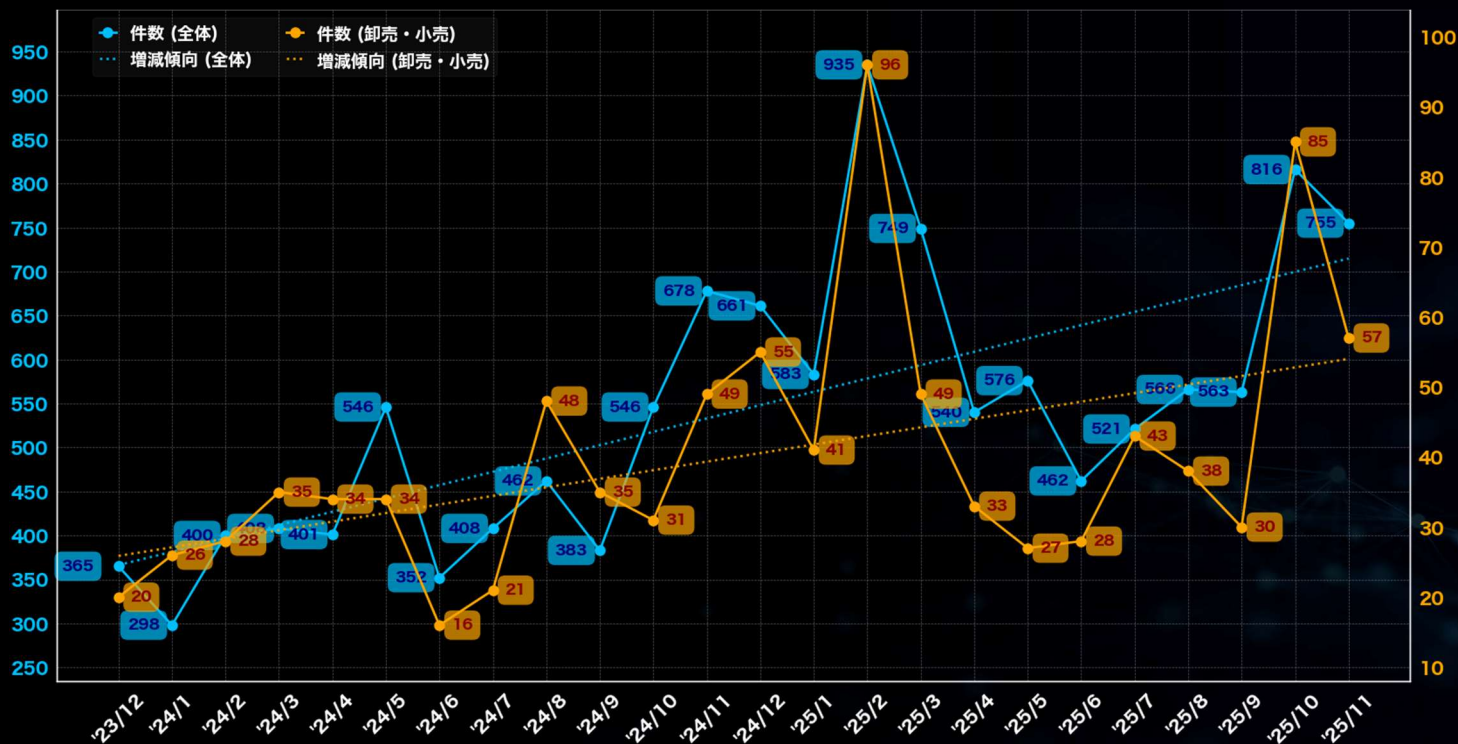
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

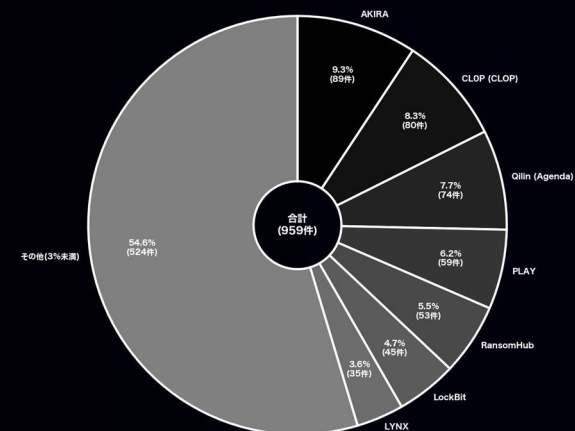
(過去2年間／2023年12月～2025年11月)

卸売・小売

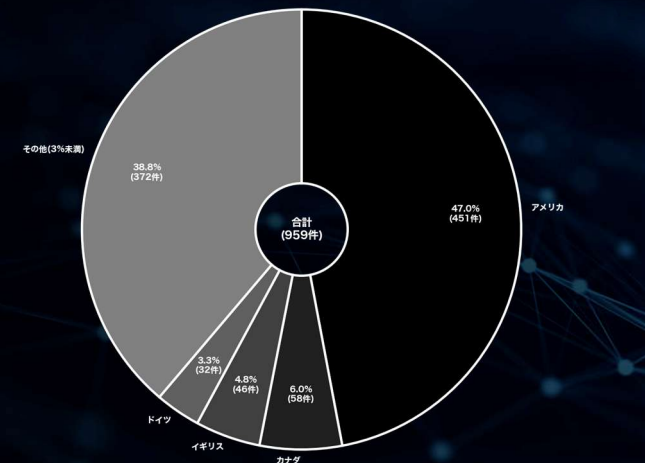
「卸売・小売」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、96件の掲載があった。一方、最も少なかった月は2024年6月で、16件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いでカナダとイギリスがそれぞれ約6%と約5%である。攻撃グループについては、少なくとも102のグループが関与しており、特に「AKIRA」が89件のリークサイト掲載を実施している。次いで「CL0P (CLOP)」と「Qilin (Agenda)」が80件と74件の掲載を行っている。卸売・小売関連は大きな増減の波があるものの、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



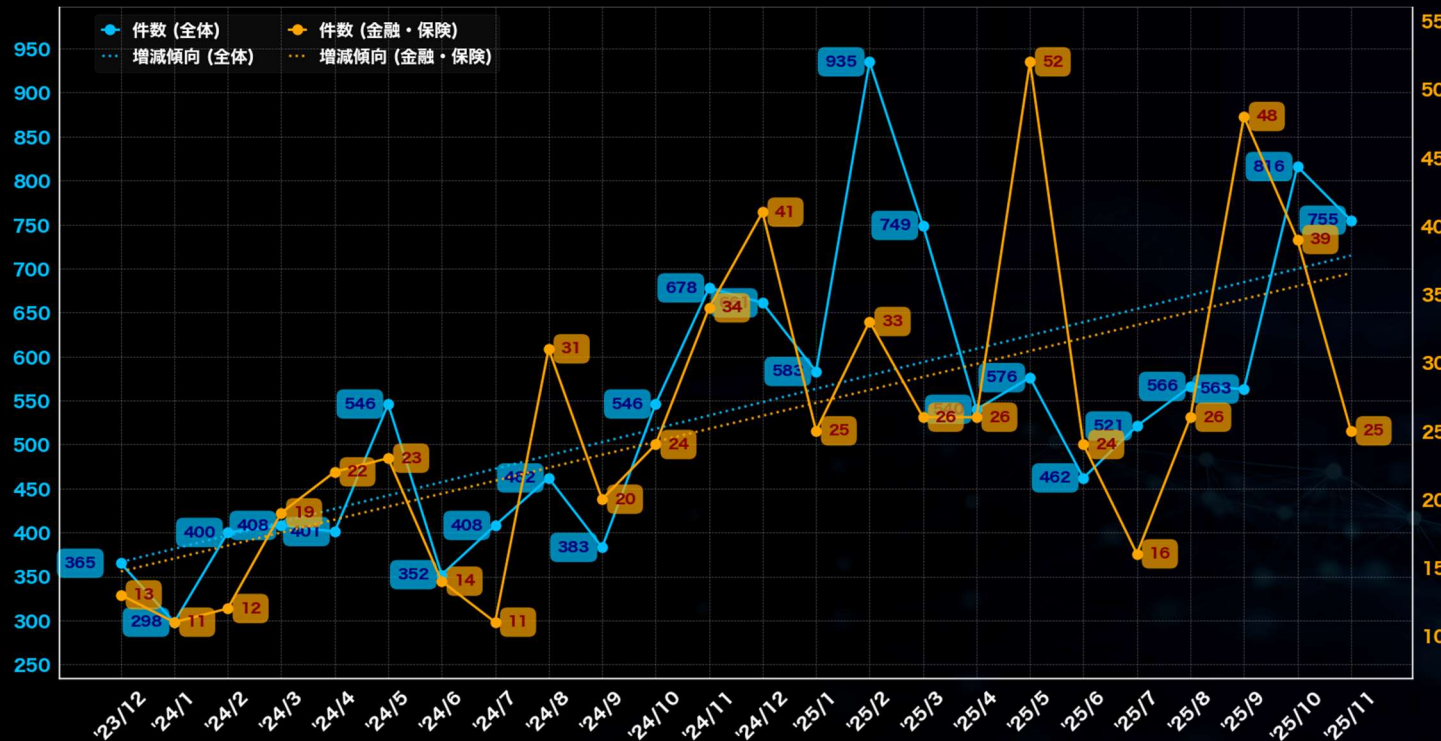
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

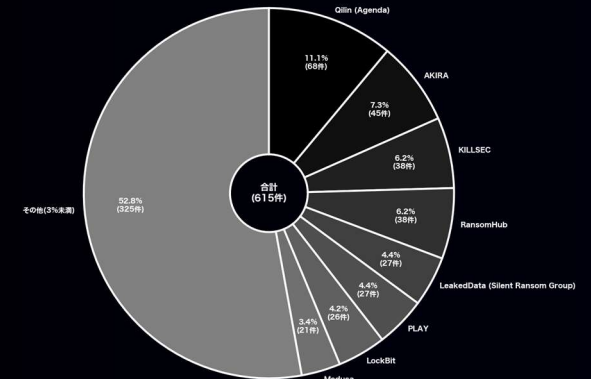
(過去2年間／2023年12月～2025年11月)

金融・保険

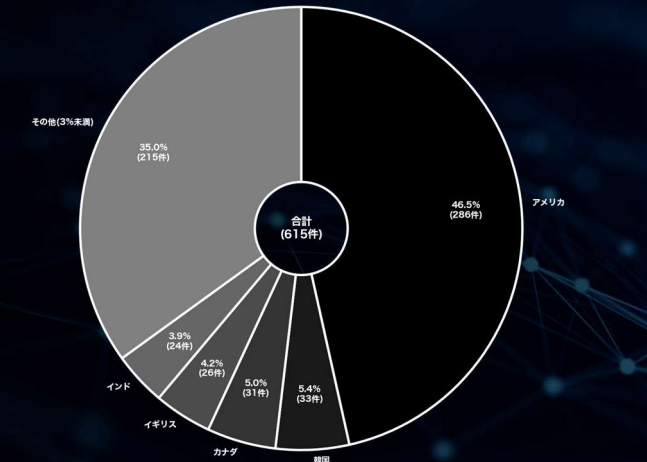
「金融・保険」業界に対するランサムウェア攻撃のリークサイト掲載件数は、最も多かった月が2025年5月で、52件の掲載があった。一方、最も少なかった月は2024年1月および7月で、11件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いで韓国とカナダがそれぞれ約5%である。攻撃グループについては、少なくとも101のグループが関与しており、特に「Qilin (Agenda)」が68件のリークサイト掲載を実施している。次いで「AKIRA」と「KILLSEC」がそれぞれ45件と38件の掲載を行っている。金融・保険関連は全体件数に対する割合は低いものの明確な増加傾向にある。



▼攻撃グループ別



▼国別



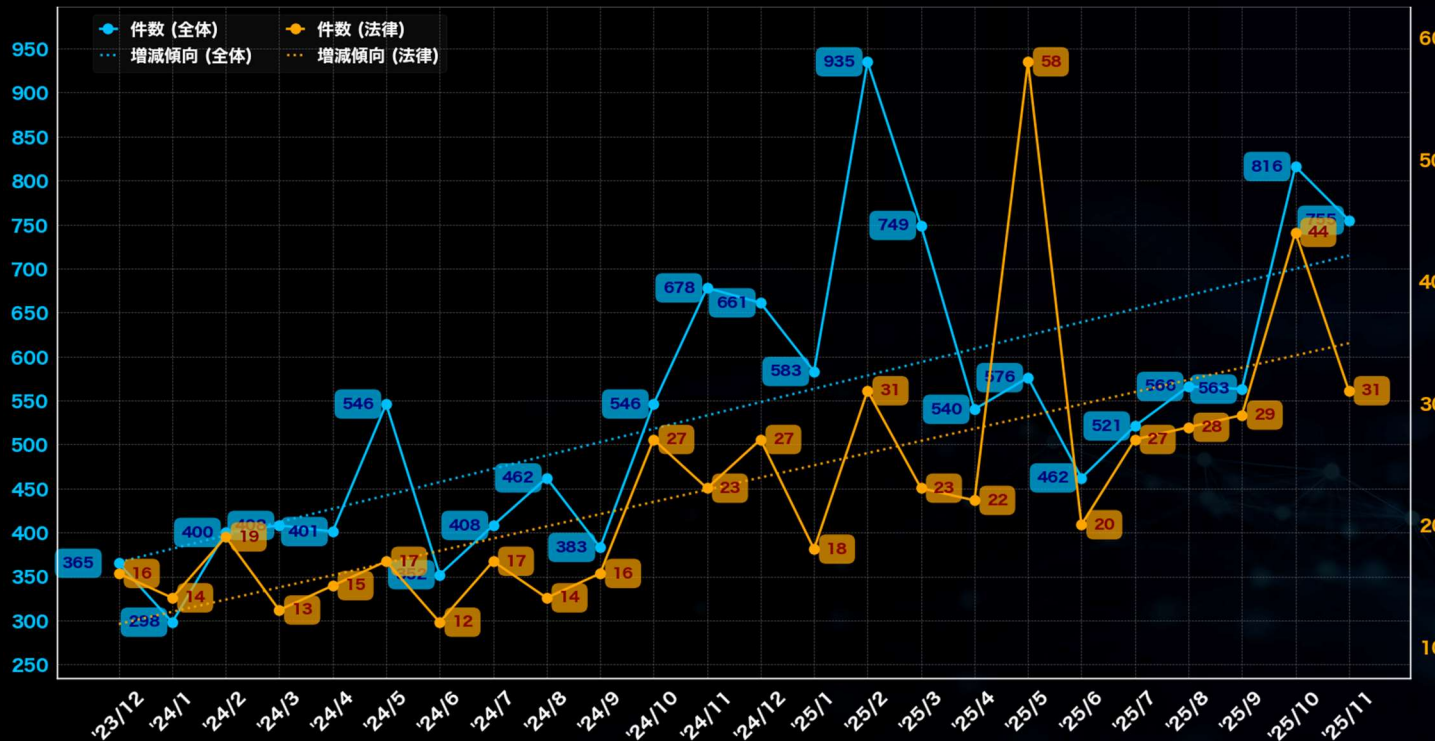
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

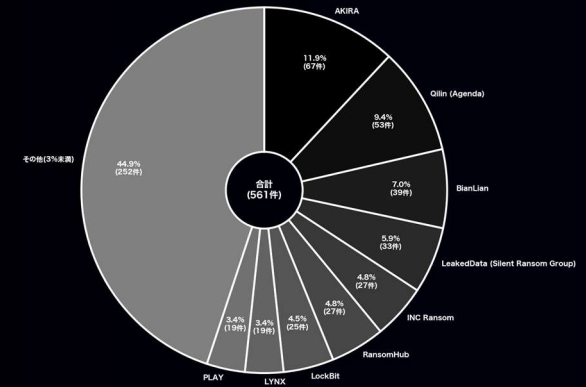
(過去2年間／2023年12月～2025年11月)

法律

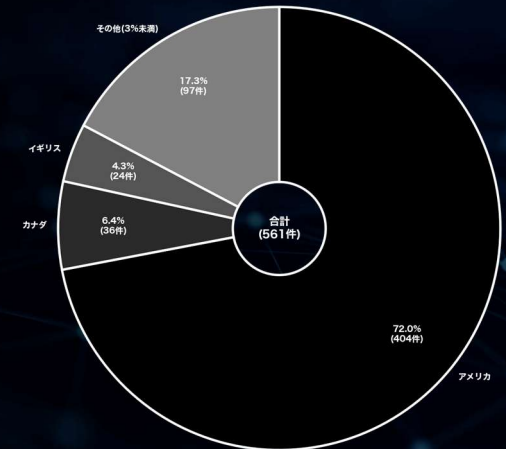
「法律」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年5月で、58件の掲載があった。一方、最も少なかった月は2024年6月で、12件であった。被害組織の所在国の割合では、アメリカが約72%と最も多く、次いでカナダとイギリスがそれぞれ約6%と約4%である。攻撃グループについては、少なくとも80のグループが関与しており、特に「AKIRA」が67件のリークサイト掲載を実施している。次いで「Qilin (Agenda)」と「BianLian」がそれぞれ53件と39件の掲載を行っている。法律関連は2023年末以降、減少傾向が見られたが、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



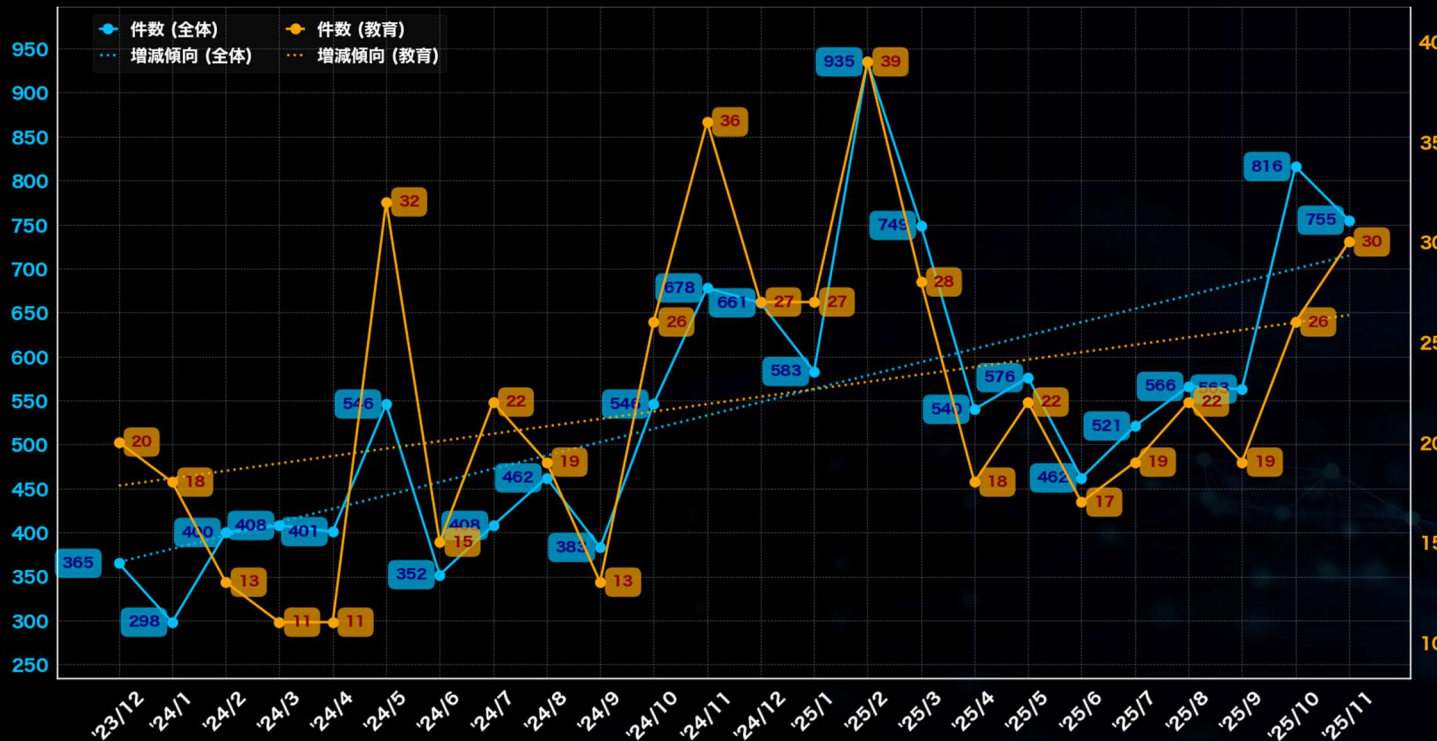
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

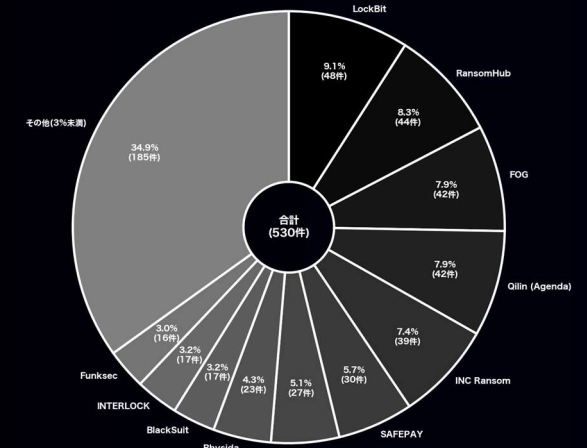
(過去2年間／2023年12月～2025年11月)

教育

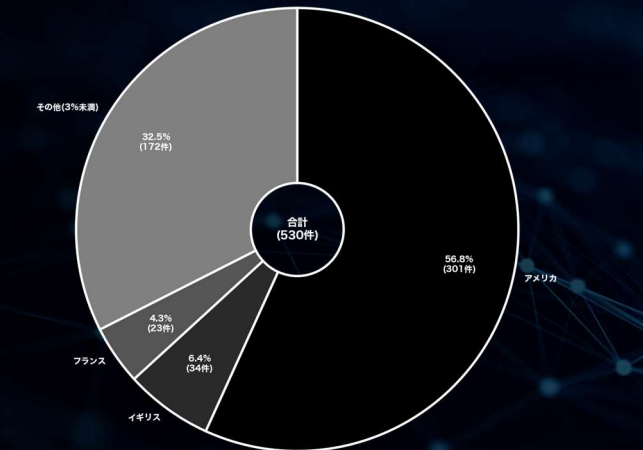
「教育」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、39件の掲載があった。一方、最も少なかった月は2024年3月と4月で、11件であった。被害組織の所在国の割合では、アメリカが約57%と最も多く、次いでイギリスとフランスがそれぞれ約6%と約4%である。攻撃グループについては、少なくとも81のグループが関与しており、特に「LockBit」が48件のリークサイト掲載を実施している。次いで「RansomHub」と「FOG」がそれぞれ44件と42件の掲載を行っている。過去2年間の推移は緩やかな増加傾向となっている。



▼攻撃グループ別



▼国別



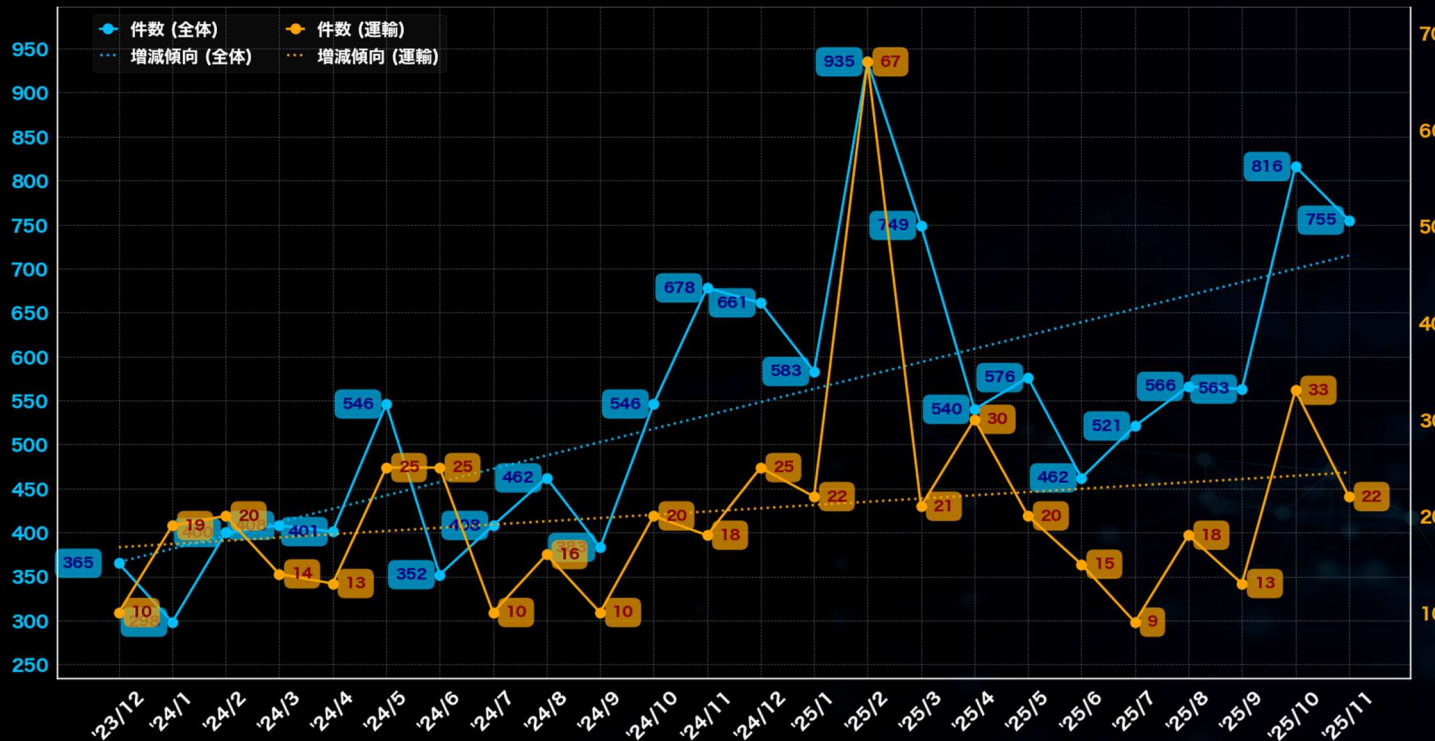
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

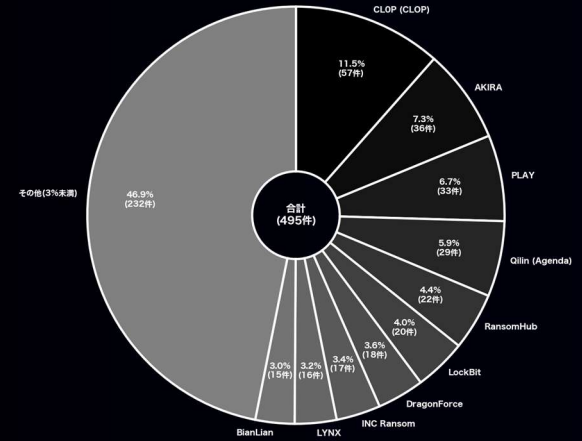
(過去2年間／2023年12月～2025年11月)

運輸

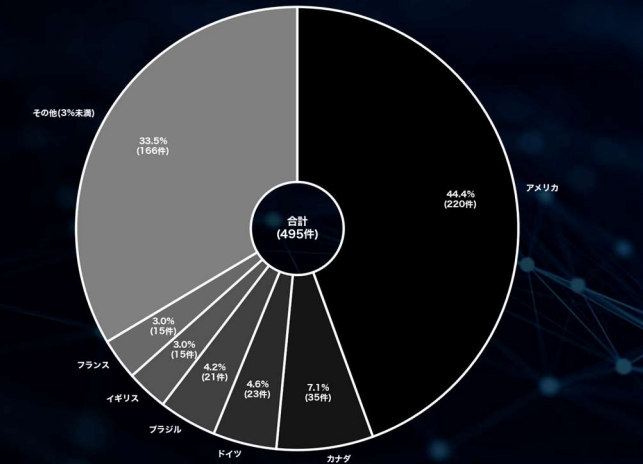
「運輸」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、67件の掲載があった。一方、最も少なかった月は2025年7月で9件であった。被害組織の所在国の割合では、アメリカが約44%と最も多く、次いでカナダとドイツがそれぞれ約7%と約5%である。攻撃グループについては、少なくとも87のグループが関与しており、特に「CLOP (CLOP)」が57件のリークサイト掲載を実施している。次いで「AKIRA」と「PLAY」がそれぞれ36件と33件の掲載を行っている。運輸関係は全体件数に対する割合こそ低く、過去2年間では著しく被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)

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 :

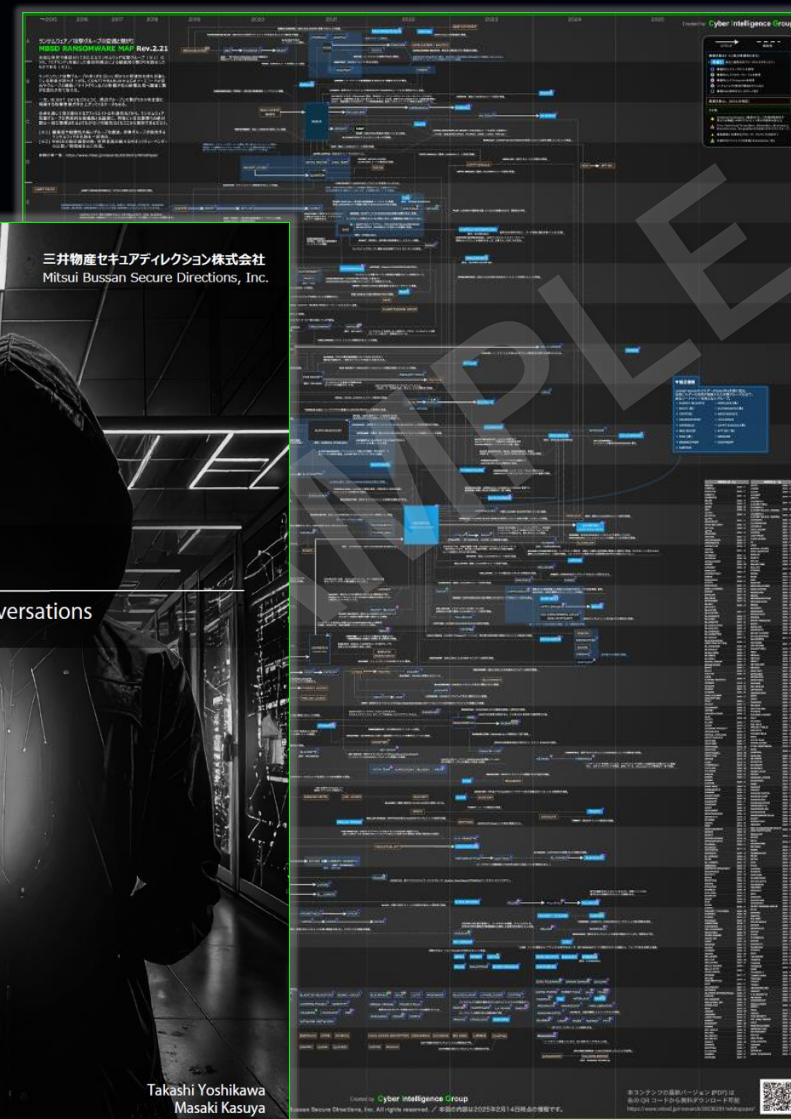
<https://www.mbsd.jp/research/cig/>

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

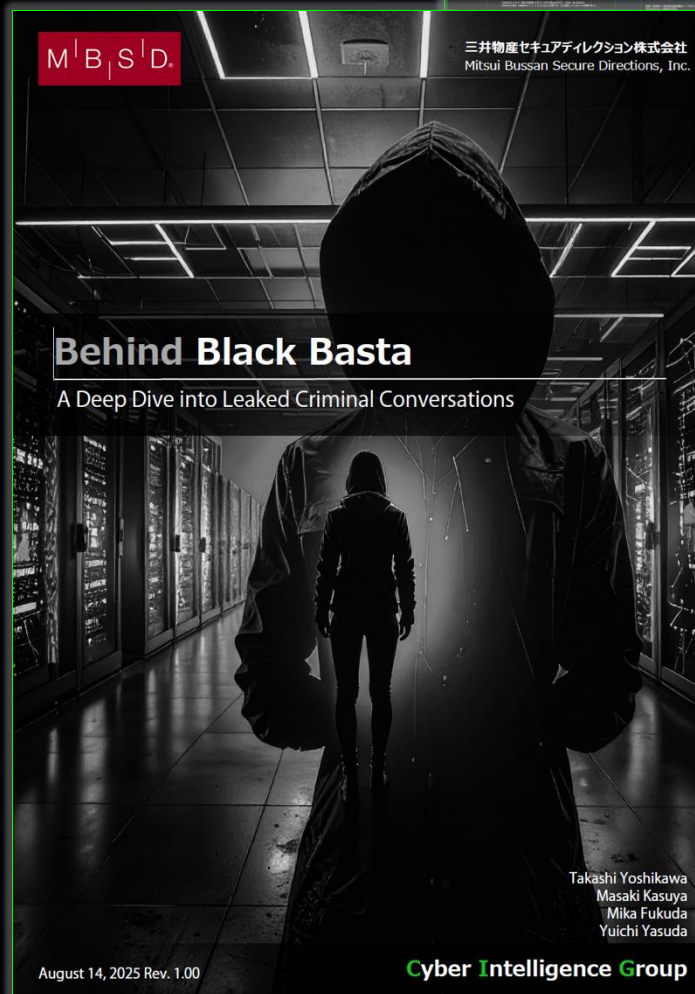
- 分析レポート :

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

MBSD RANSOMWARE MAP (Rev.2)



Black Basta 内部チャット分析レポート



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