

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5月号 Rev 1.00 (2025年4月分)

2025

4

目次

総括と監視対象（レポート①～③）

今月のハイライト	p.3
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.4
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.5

グローバル統計（レポート④～⑯）

年間統計（全世界）	p.6～7
攻撃グループTOP10（全世界）	p.8～11
被害国TOP10（全世界）	p.12～15
被害国TOP10（アジア）	p.16～19
業種TOP10（全世界）	p.20～23

日本関連組織を対象とした統計（レポート⑰～⑳）

被害数の推移に関する統計（全世界及び国内）	p.24～25
資本金別 月別統計（国内）	p.26～27
公表と暴露に関する統計（国内）	p.28～29
公となった国内被害組織 概要一覧	p.30～32
公となった国内被害組織における拠点割合	p.33
公となった国内被害組織における業種割合	p.34

中小企業における被害分析（レポート㉓～㉖）

資本金別 月別統計（中小企業）	p.36
公となった国内被害組織における業種割合（中小企業）	p.37
公となった国内被害組織における拠点割合（中小企業）	p.38
公となった国内被害組織 概要一覧（中小企業）	p.39～40

多重被害に関する分析（レポート㉗～㉘）

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.42
多重被害に遭った被害組織の傾向と分析	p.43

業種に関する分析（レポート㉙）

業種に関する分析 - 製造	p.45
業種に関する分析 - サービス	p.46
業種に関する分析 - 情報通信	p.47
業種に関する分析 - 医療	p.48
業種に関する分析 - 建設・建築	p.49
業種に関する分析 - 卸売・小売	p.50
業種に関する分析 - 金融・保険	p.51
業種に関する分析 - 教育	p.52
業種に関する分析 - 運輸	p.53
業種に関する分析 - 法律	p.54

その他

CIGのコンテンツ紹介	p.55
本資料に関する留意事項及び二次利用について	p.56

2025

4

総括と監視対象

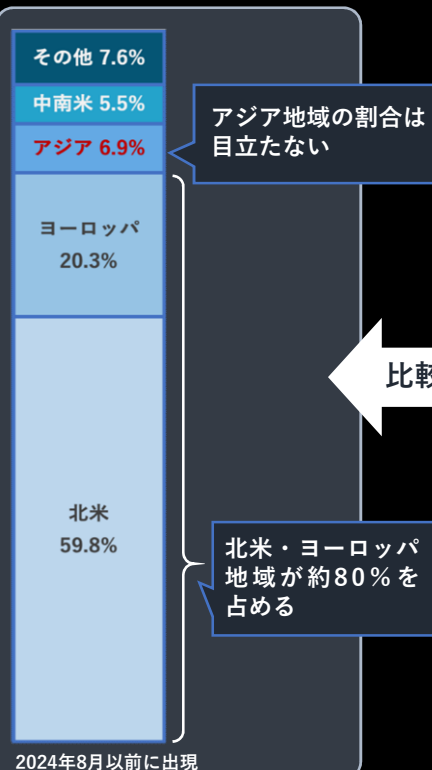
今月のハイライト

● 新興グループのアジア掲載割合が相対的に高い傾向

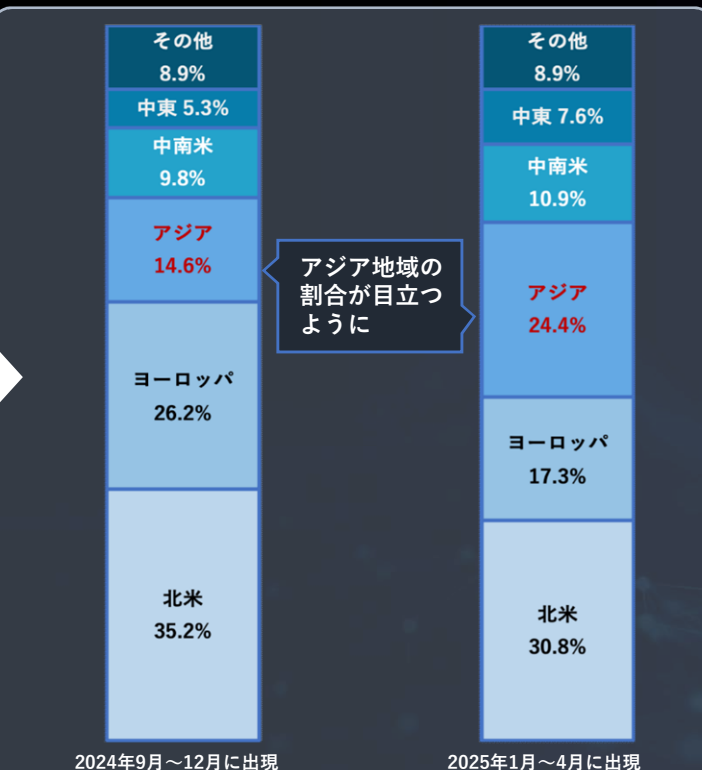
2024年8月以前に出現した攻撃グループのリークサイト掲載割合を分析すると、北米・ヨーロッパ地域が約8割を占める。一方、最近ではアジア地域の被害組織を多く掲載する新興グループが複数出現している。攻撃グループ全体で見ると大きな変化は見られないが、新興グループの新たな動向に注意が必要である。

出現時期でみる地域別掲載割合

既存グループ



新興グループ



比較

アジア地域の掲載割合が高い新興グループ

アジア地域の掲載割合が大きいグループやアジアの特定の国を標的とするグループが直近で複数出現。

Crazy Hunter Team

リークサイト出現：2025年3月頃
掲載件数：10件
アジアの割合：100% (全て台湾)



NightSpire

リークサイト出現：2025年3月頃
掲載件数：39件
アジアの割合：約39% (日本関連組織も複数含まれる)



CRYPTO24

リークサイト出現：2025年4月頃
掲載件数：8件
アジアの割合：50%



▲ 掲載集計：2024年5月（もしくは出現）～2025年4月

▲ 掲載集計：出現～2025年4月

2024年9月以降に出現した新興グループでは、アジア地域の掲載割合が顕著に目立つようになってきたことがわかる。新興グループの掲載数は依然少ないため傾向の偏りには留意が必要だが、日本を含むアジア地域では一層の警戒が必要である。

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：236 ^(※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：48

● 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)

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

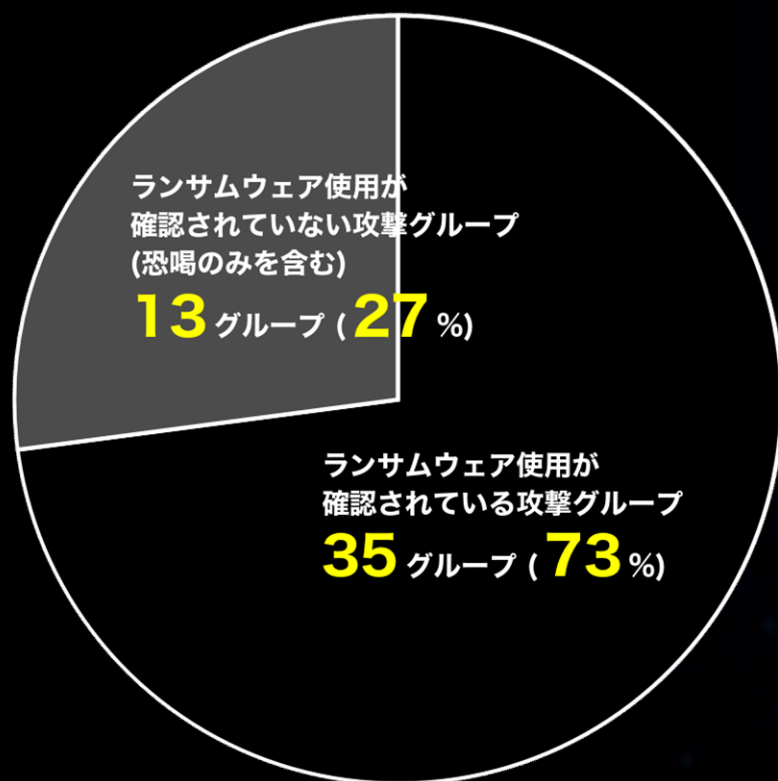
※1) レポート公開月に出現した攻撃グループは次月号に反映

※2) 活動停止した攻撃グループを含む

監視中のランサムウェア攻撃グループ情報 (ランサムウェア使用の割合)

●現在活動中の攻撃グループにおけるランサムウェア使用の割合 (2025年 **4**月)

(※当月にリークサイト掲載を確認した攻撃グループ全 **48**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4月に活動中である事が確認された全48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

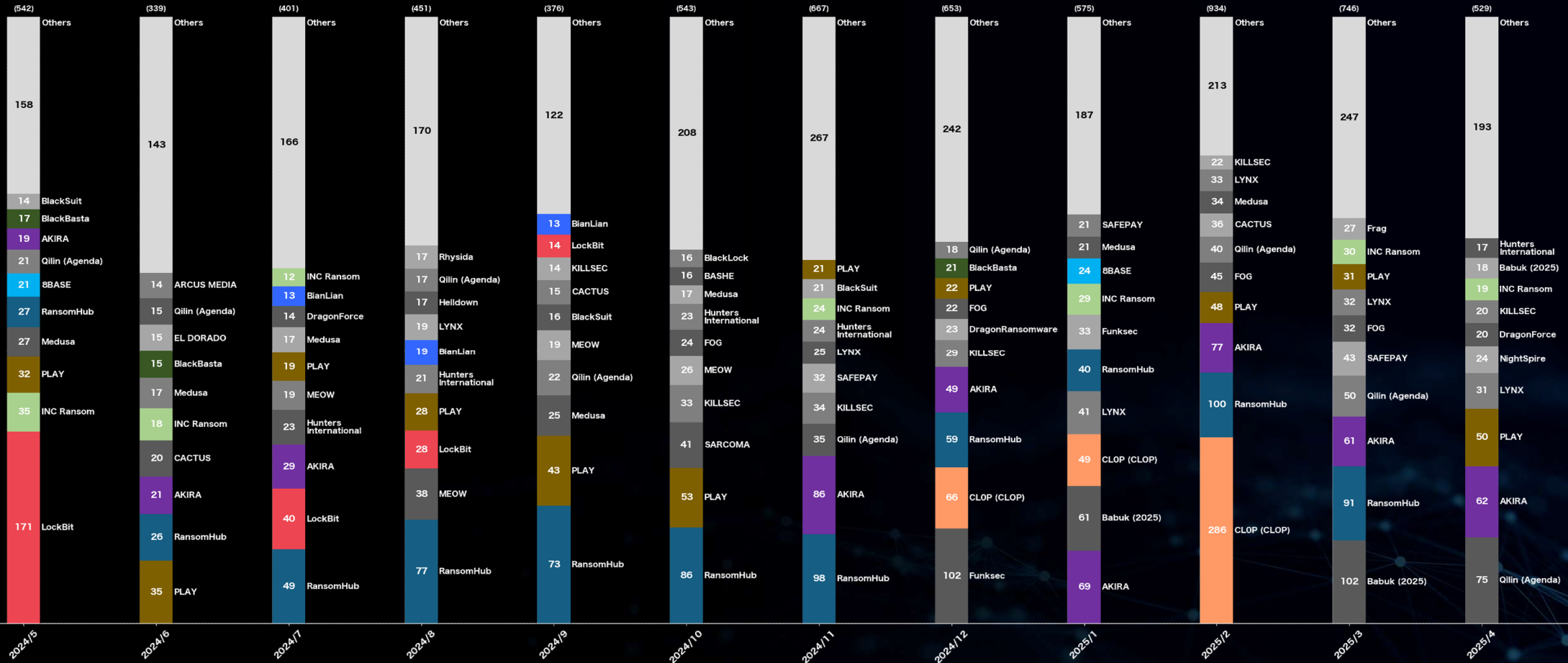
(全世界)

2025

4

攻撃グループ割合で見る被害数の年間統計 (全世界)

(過去1年間／2024年5月～2025年4月)



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

攻撃グループ 月別統計

(全世界) (過去3ヶ月分)

2025

4

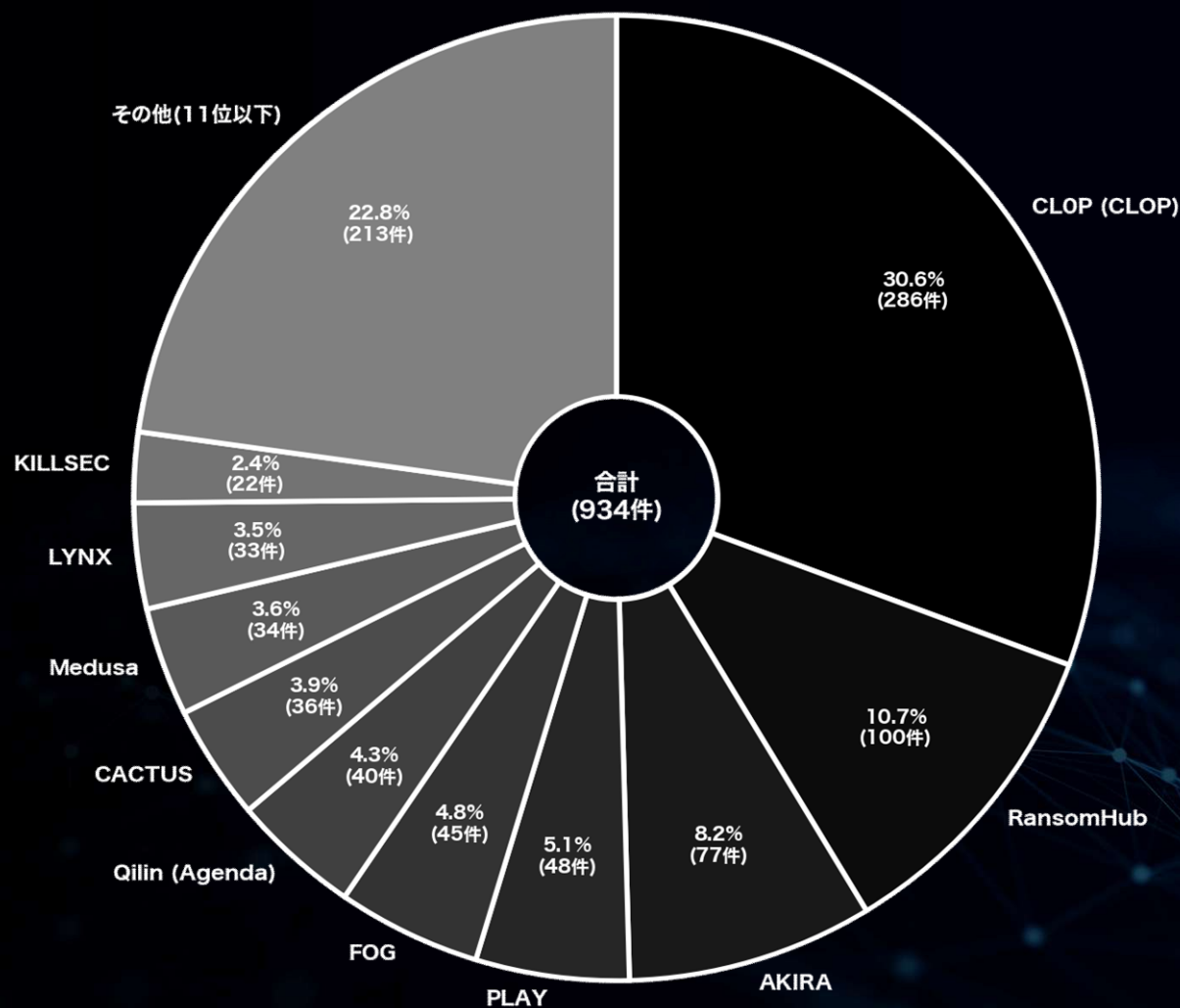
月別内訳 攻撃グループ TOP10 (全世界)

(2025年 2 月)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

攻撃グループ名	件数	割合(%)	前月比(件数)
CLOP (CLOP)	286	30.6	+ 237
RansomHub	100	10.7	+ 60
AKIRA	77	8.2	+ 8
PLAY	48	5.1	+ 37
FOG	45	4.8	+ 30
Qilin (Agenda)	40	4.3	+ 21
CACTUS	36	3.9	+ 27
Medusa	34	3.6	+ 13
LYNX	33	3.5	- 8
KILLSEC	22	2.4	+ 13

▼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)



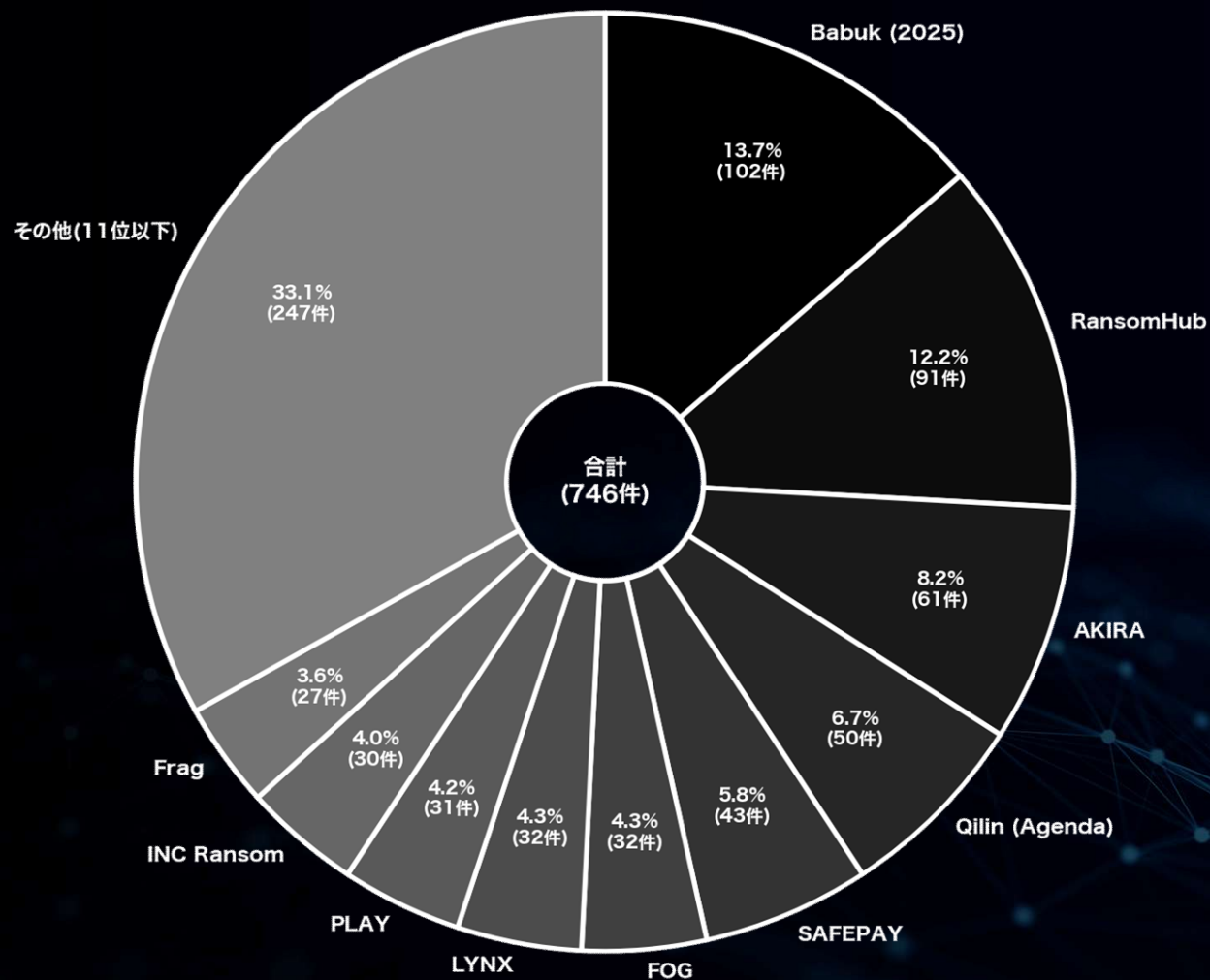
月別内訳 攻撃グループ TOP10 (全世界)

(2025年 3 月)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

攻撃グループ名	件数	割合(%)	前月比(件数)
Babuk (2025)	102	13.7	+ 102
RansomHub	91	12.2	- 9
AKIRA	61	8.2	- 16
Qilin (Agenda)	50	6.7	+ 10
SAFEPAY	43	5.8	+ 31
FOG	32	4.3	- 13
LYNX	32	4.3	- 1
PLAY	31	4.2	- 17
INC Ransom	30	4.0	+ 17
Frag	27	3.6	+ 27

▼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)



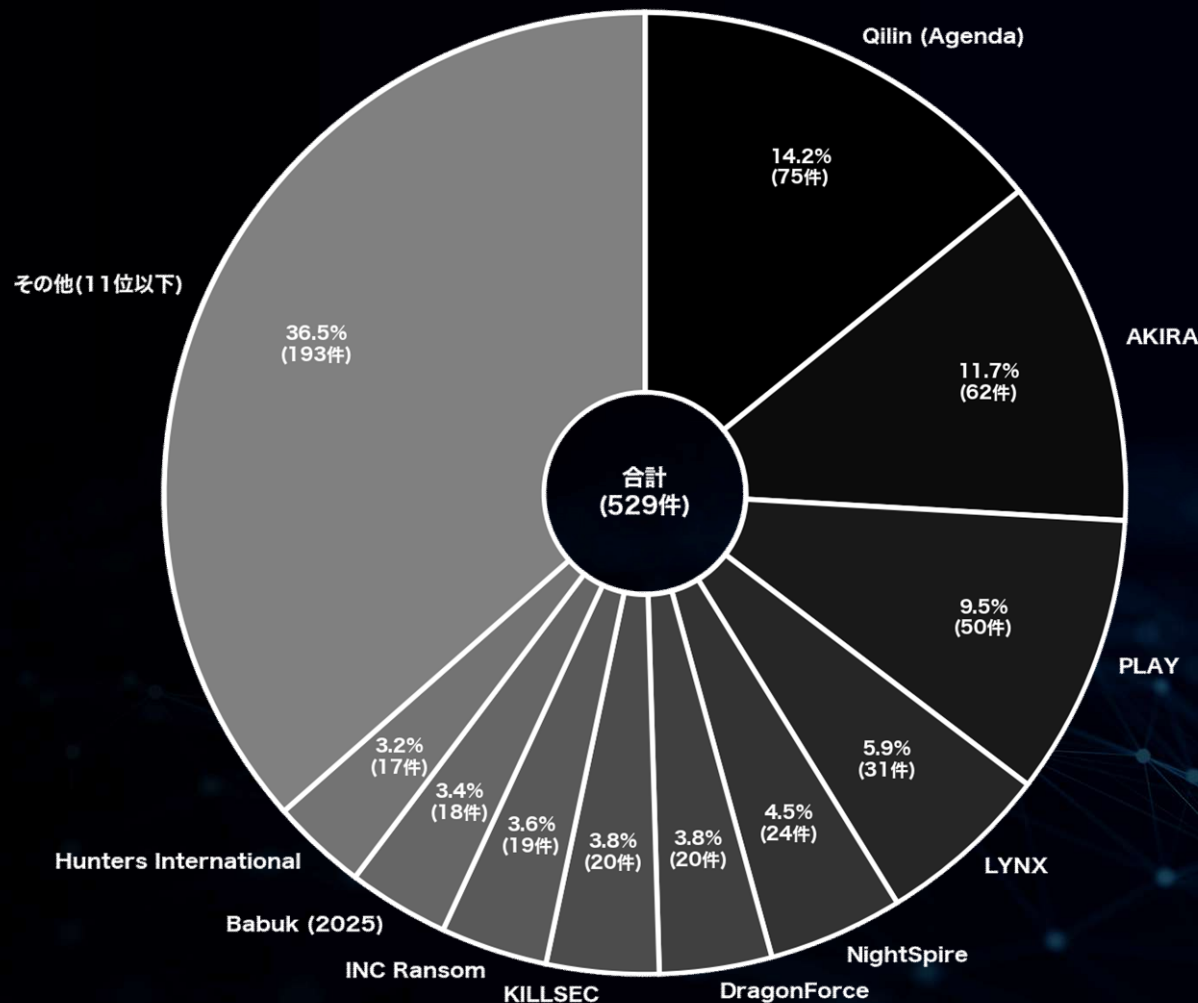
月別内訳 攻撃グループ TOP10 (全世界)

(2025年 4 月)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

攻撃グループ名	件数	割合(%)	前月比(件数)
Qilin (Agenda)	75	14.2	+ 25
AKIRA	62	11.7	+ 1
PLAY	50	9.5	+ 19
LYNX	31	5.9	- 1
NightSpire	24	4.5	+ 9
DragonForce	20	3.8	+ 5
KILLSEC	20	3.8	+ 3
INC Ransom	19	3.6	- 11
Babuk (2025)	18	3.4	- 84
Hunters International	17	3.2	+ 11

▼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

4

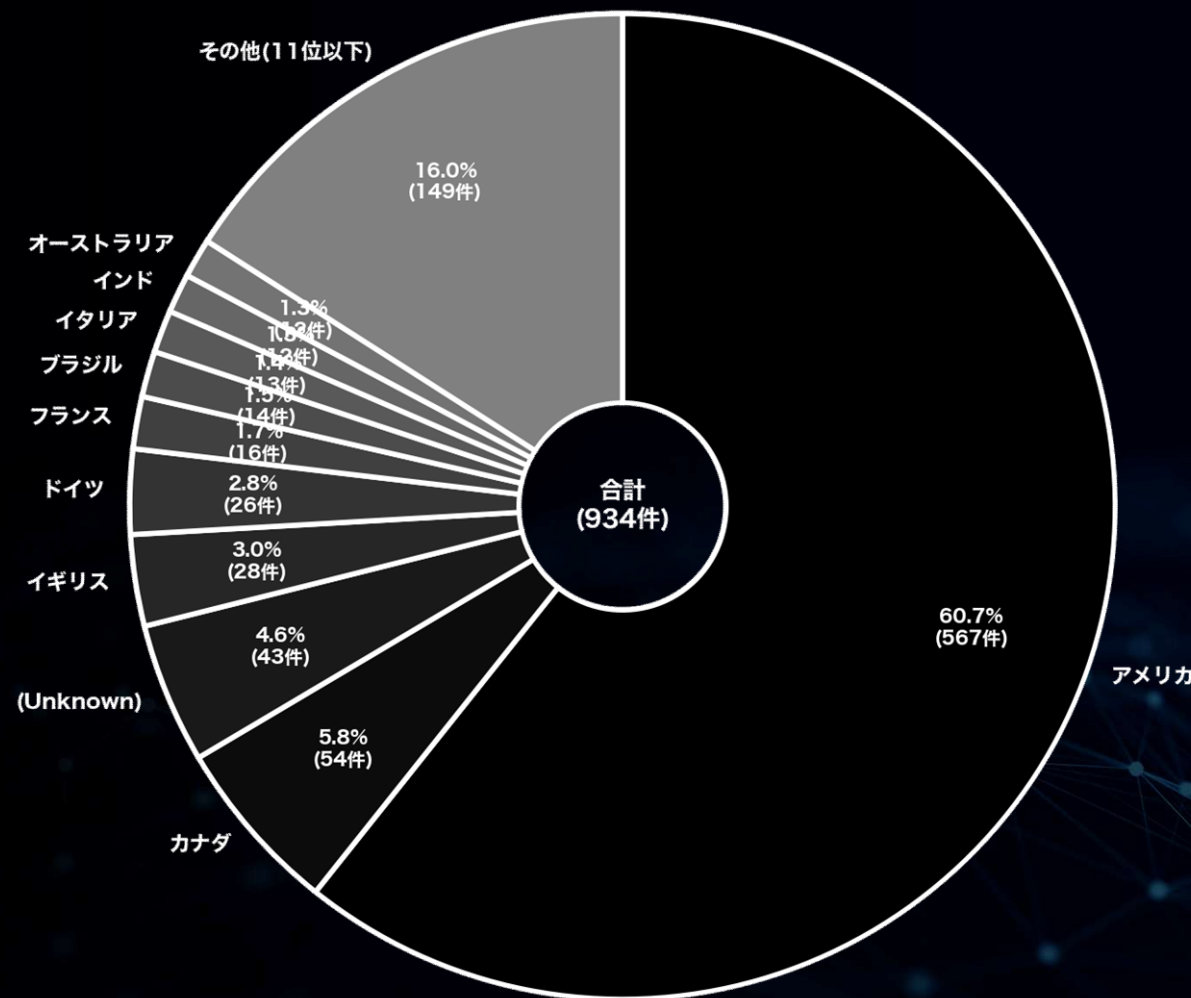
月別内訳 被害国TOP10 (全世界)

(2025年 2 月)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
アメリカ	567	60.7	+ 307
カナダ	54	5.8	+ 25
(Unknown)	43	4.6	+ 24
イギリス	28	3.0	± 0
ドイツ	26	2.8	+ 16
フランス	16	1.7	- 2
ブラジル	14	1.5	- 7
イタリア	13	1.4	+ 1
インド	12	1.3	- 7
オーストラリア	12	1.3	± 0

▼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)



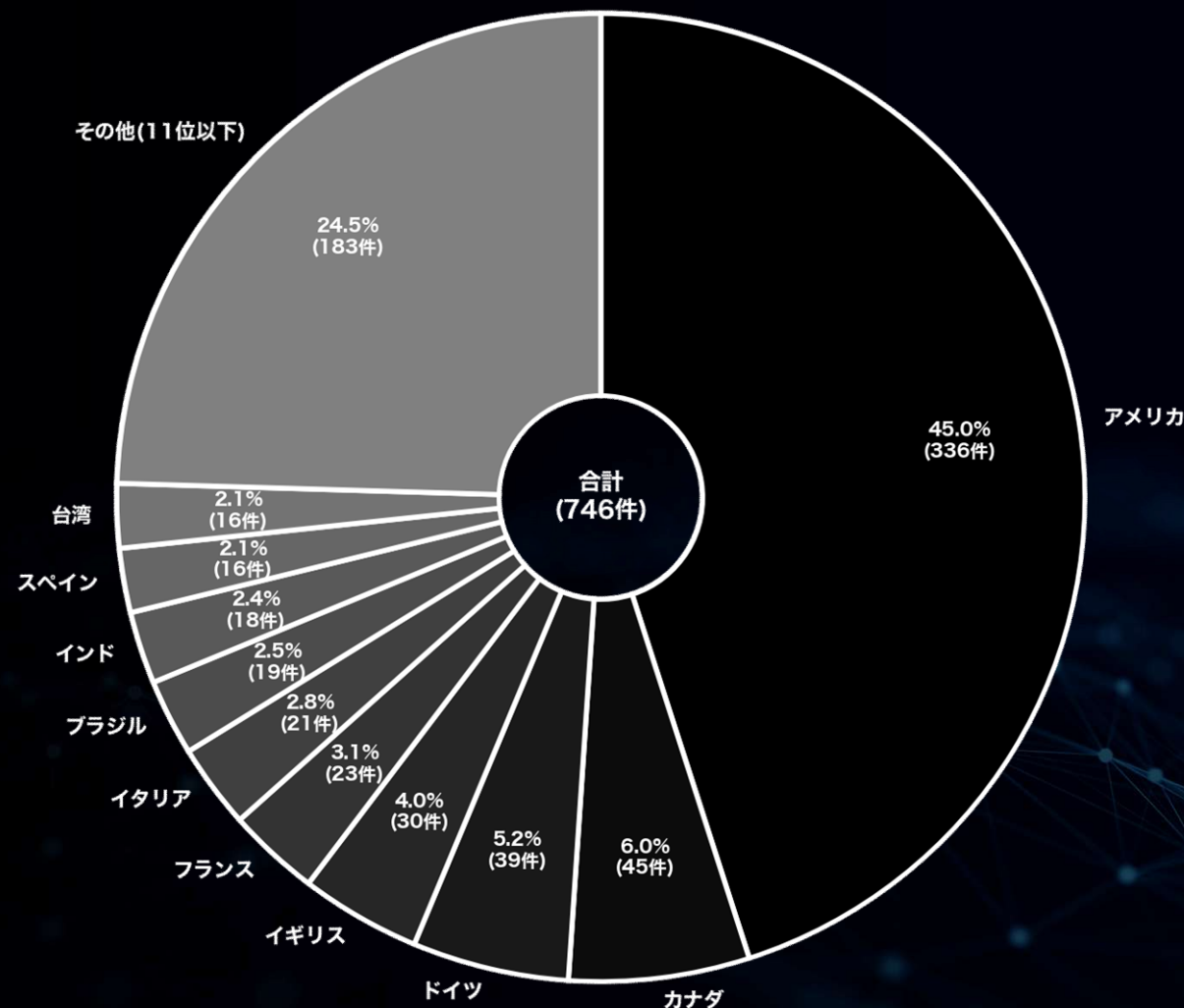
月別内訳 被害国TOP10 (全世界)

(2025年 3 月)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
アメリカ	336	45.0	- 231
カナダ	45	6.0	- 9
ドイツ	39	5.2	+ 13
イギリス	30	4.0	+ 2
フランス	23	3.1	+ 7
イタリア	21	2.8	+ 8
ブラジル	19	2.5	+ 5
インド	18	2.4	+ 6
スペイン	16	2.1	+ 6
台湾	16	2.1	+ 9

▼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)



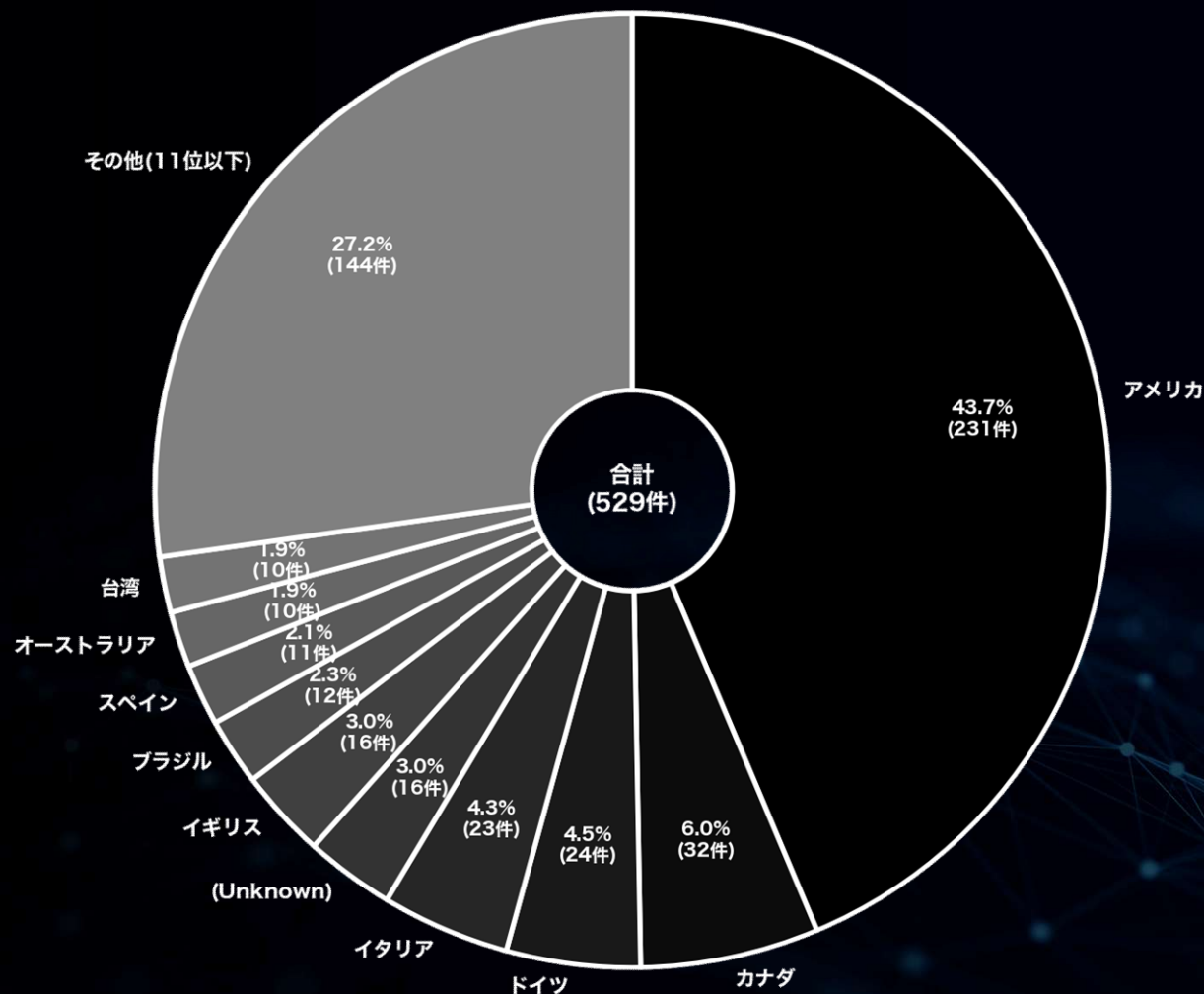
月別内訳 被害国TOP10 (全世界)

(2025年 4 月)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
アメリカ	231	43.7	- 105
カナダ	32	6.0	- 13
ドイツ	24	4.5	- 15
イタリア	23	4.3	+ 2
(Unknown)	16	3.0	+ 1
イギリス	16	3.0	- 14
ブラジル	12	2.3	- 7
スペイン	11	2.1	- 5
オーストラリア	10	1.9	+ 2
台湾	10	1.9	- 6

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



被害国 月別統計

(アジア) (過去3ヶ月分)

2025

4

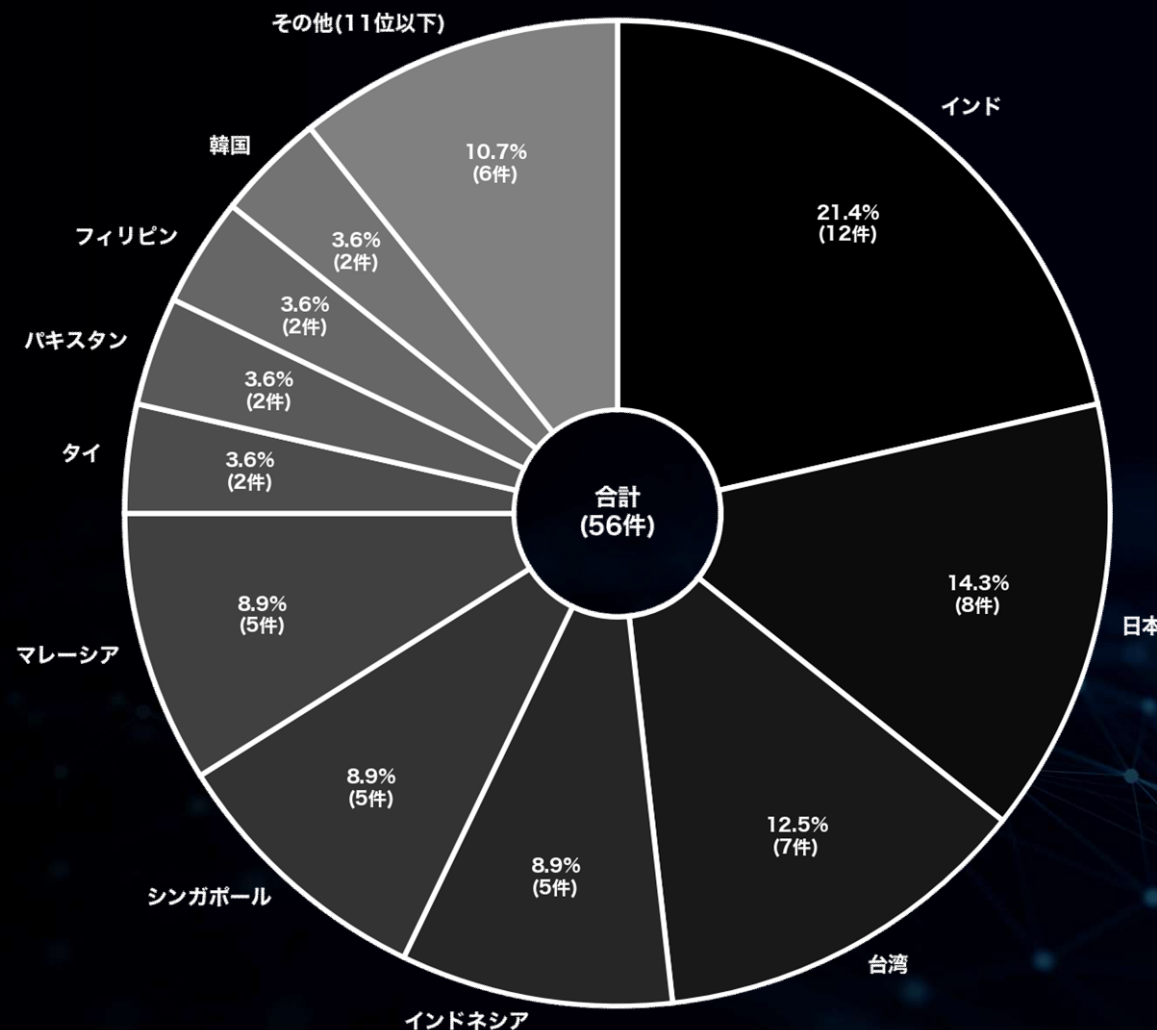
月別内訳 被害国TOP10 (アジア)

(2025年 2 月)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
インド	12	21.4	- 7
日本	8	14.3	+ 2
台湾	7	12.5	+ 6
インドネシア	5	8.9	+ 1
シンガポール	5	8.9	± 0
マレーシア	5	8.9	+ 1
タイ	2	3.6	- 3
パキスタン	2	3.6	- 2
フィリピン	2	3.6	+ 2
韓国	2	3.6	+ 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)



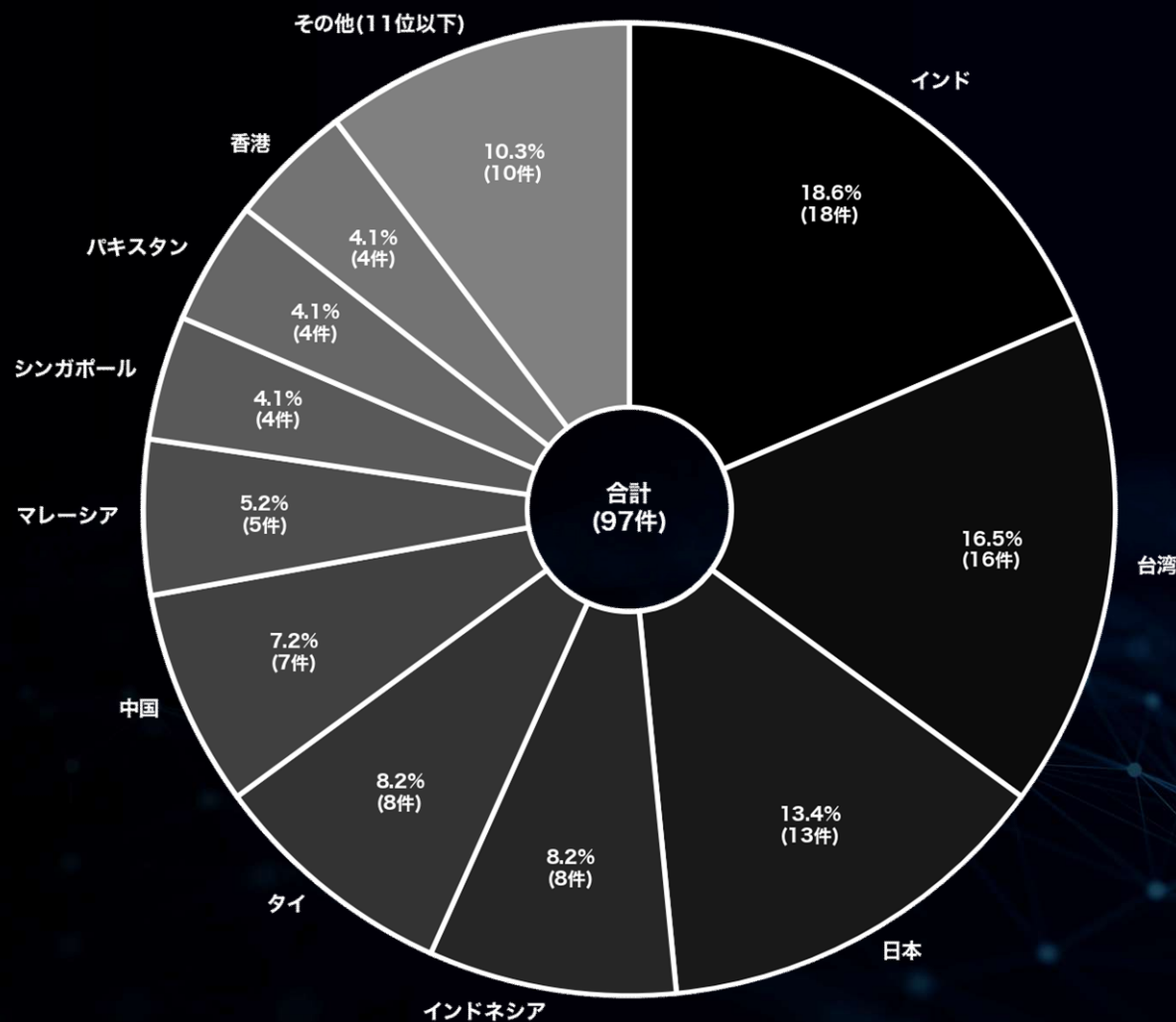
月別内訳 被害国TOP10 (アジア)

(2025年 3 月)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
インド	18	18.6	+ 6
台湾	16	16.5	+ 9
日本	13	13.4	+ 5
インドネシア	8	8.2	+ 3
タイ	8	8.2	+ 6
中国	7	7.2	+ 6
マレーシア	5	5.2	± 0
シンガポール	4	4.1	- 1
パキスタン	4	4.1	+ 2
香港	4	4.1	+ 2

▼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)



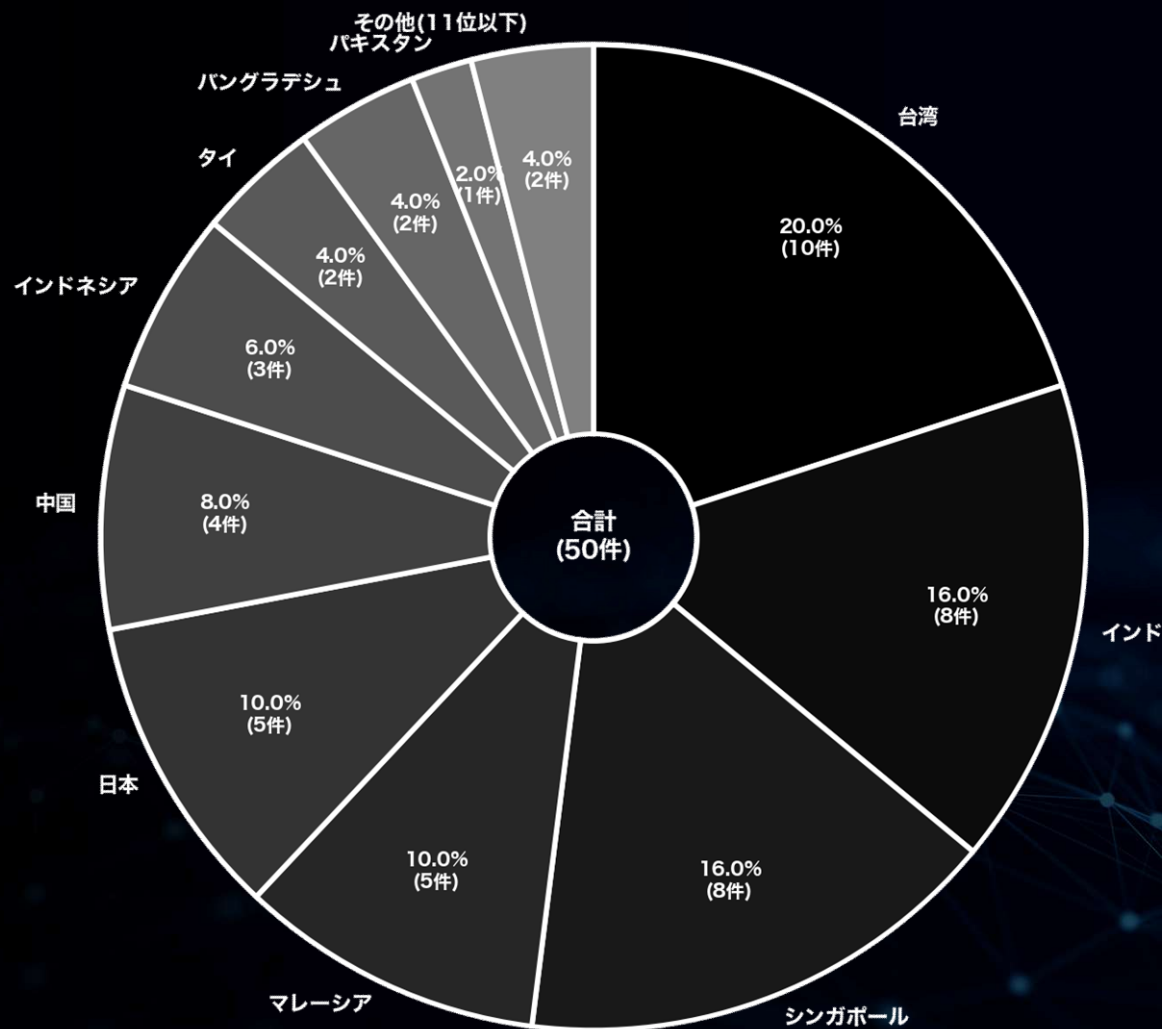
月別内訳 被害国TOP10 (アジア)

(2025年 4 月)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
台湾	10	20.0	- 6
インド	8	16.0	- 10
シンガポール	8	16.0	+ 4
マレーシア	5	10.0	± 0
日本	5	10.0	- 8
中国	4	8.0	- 3
インドネシア	3	6.0	- 5
タイ	2	4.0	- 6
バングラデシュ	2	4.0	+ 2
パキスタン	1	2.0	- 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

4

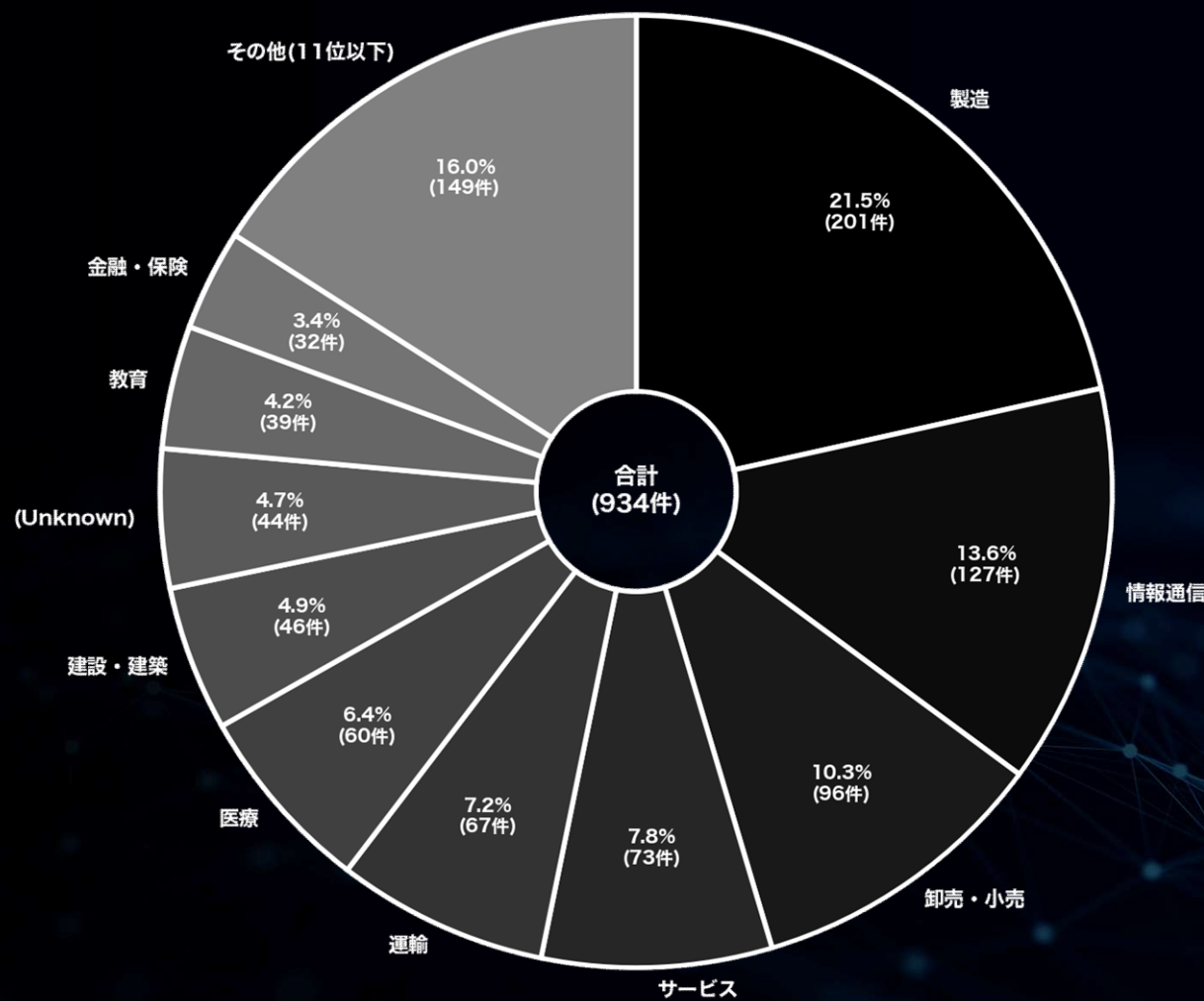
月別内訳 業種 TOP10 (全世界)

(2025年 2 月)

※件数順に降順／同件数のものが含まれる場合は名前順でTOP10までを記載

業種	件数	割合(%)	前月比(件数)
製造	201	21.5	+ 97
情報通信	127	13.6	+ 50
卸売・小売	96	10.3	+ 55
サービス	73	7.8	+ 16
運輸	67	7.2	+ 46
医療	60	6.4	+ 13
建設・建築	46	4.9	+ 3
(Unknown)	44	4.7	+ 25
教育	39	4.2	+ 12
金融・保険	32	3.4	+ 8

▼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)



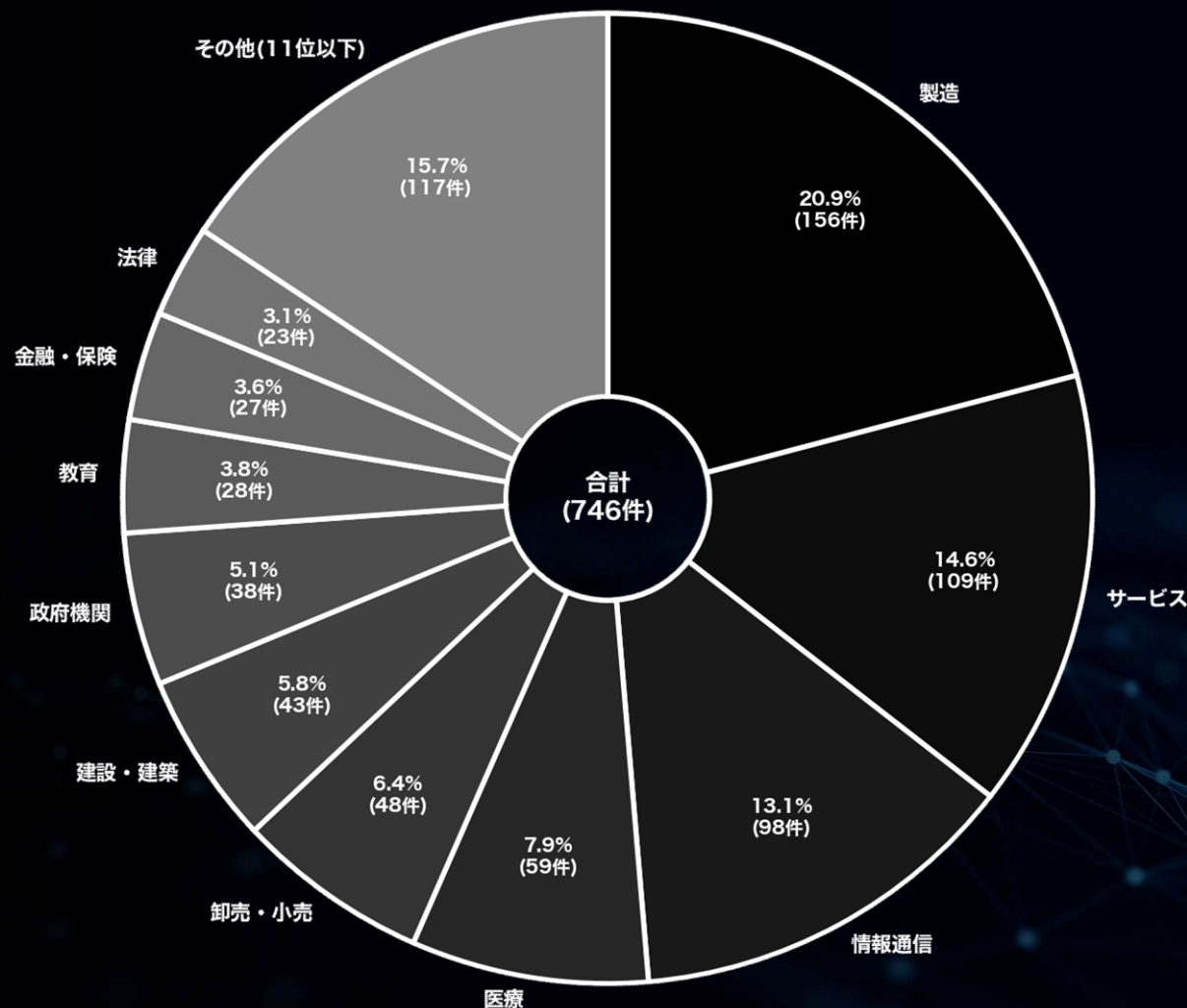
月別内訳 業種 TOP10 (全世界)

(2025年 3 月)

※件数順に降順／同件数のものが含まれる場合は名前順でTOP10までを記載

業種	件数	割合(%)	前月比(件数)
製造	156	20.9	- 45
サービス	109	14.6	+ 36
情報通信	98	13.1	- 29
医療	59	7.9	- 1
卸売・小売	48	6.4	- 48
建設・建築	43	5.8	- 3
政府機関	38	5.1	+ 33
教育	28	3.8	- 11
金融・保険	27	3.6	- 5
法律	23	3.1	- 8

▼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)



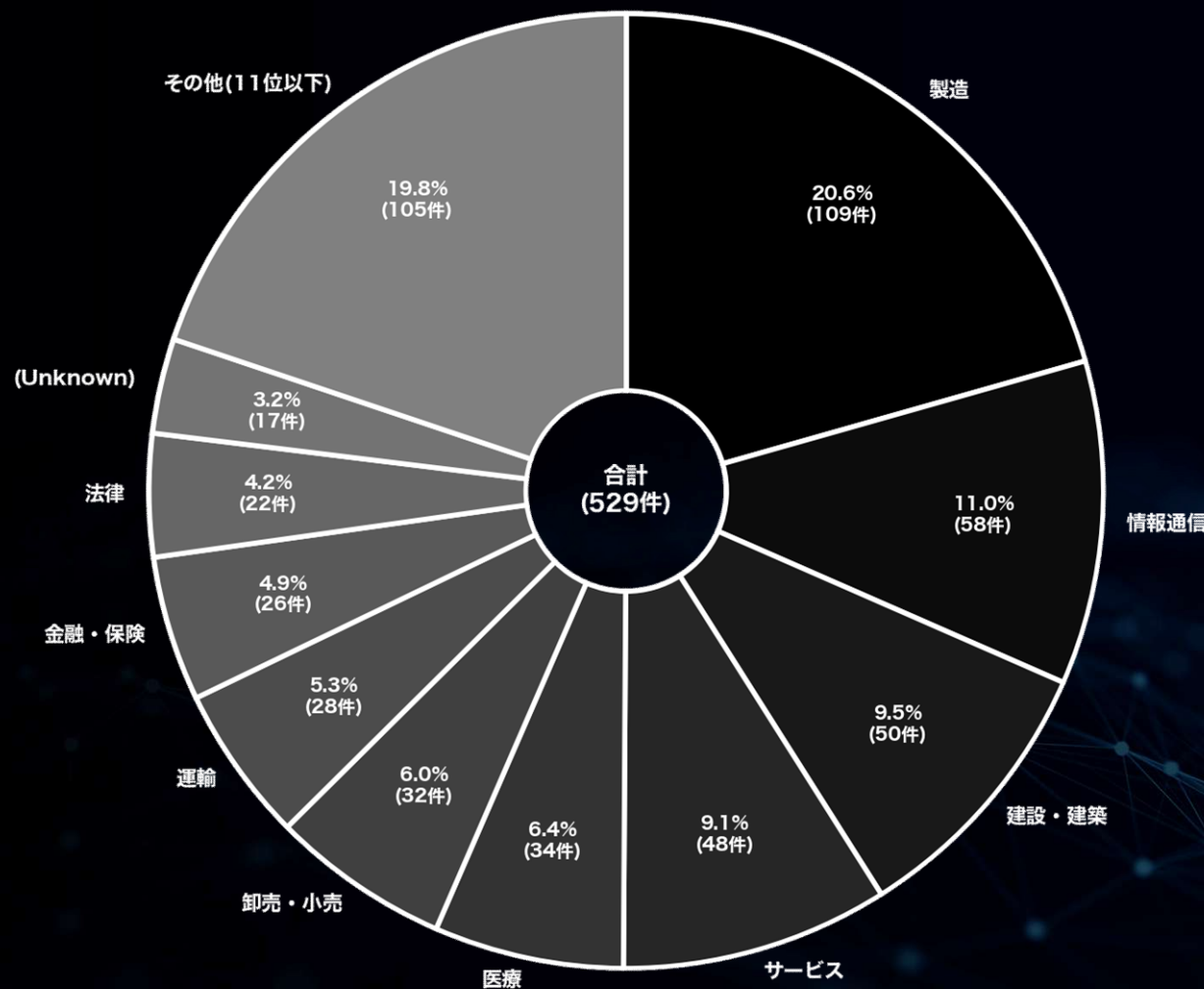
月別内訳 業種 TOP10 (全世界)

(2025年 4 月)

※件数順に降順／同件数のものが含まれる場合は名前順でTOP10までを記載

業種	件数	割合(%)	前月比(件数)
製造	109	20.6	- 47
情報通信	58	11.0	- 40
建設・建築	50	9.5	+ 7
サービス	48	9.1	- 61
医療	34	6.4	- 25
卸売・小売	32	6.0	- 16
運輸	28	5.3	+ 7
金融・保険	26	4.9	- 1
法律	22	4.2	- 1
(Unknown)	17	3.2	+ 2

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



2025

4

被害数の推移に関する統計

(全世界及び国内)

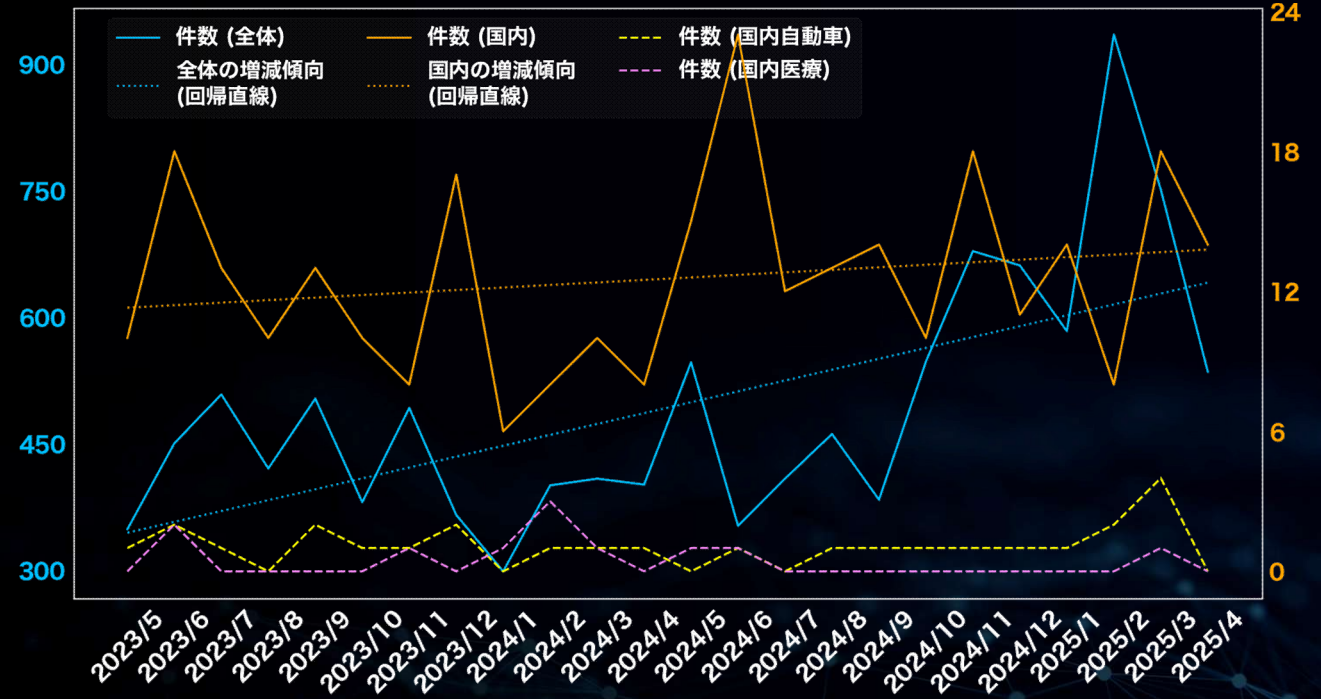
被害数の推移（全世界及び国内） （過去2年間／2023年5月～2025年4月）

※件数には公表や報道から判明した数も含む

期間	件数 (全体)	件数 (国内)	件数 (国内自動車)	件数 (国内医療)
2023/5	348	10	1	0
2023/6	450	18	2	2
2023/7	508	13	1	0
2023/8	420	10	0	0
2023/9	503	13	2	0
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	461	13	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	751	18	4	1
2025/4	535	14	0	0
合計	11813	301	26	11

▼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 月別統計

(国内)

2025

4

月別内訳 資本金別 (国内)

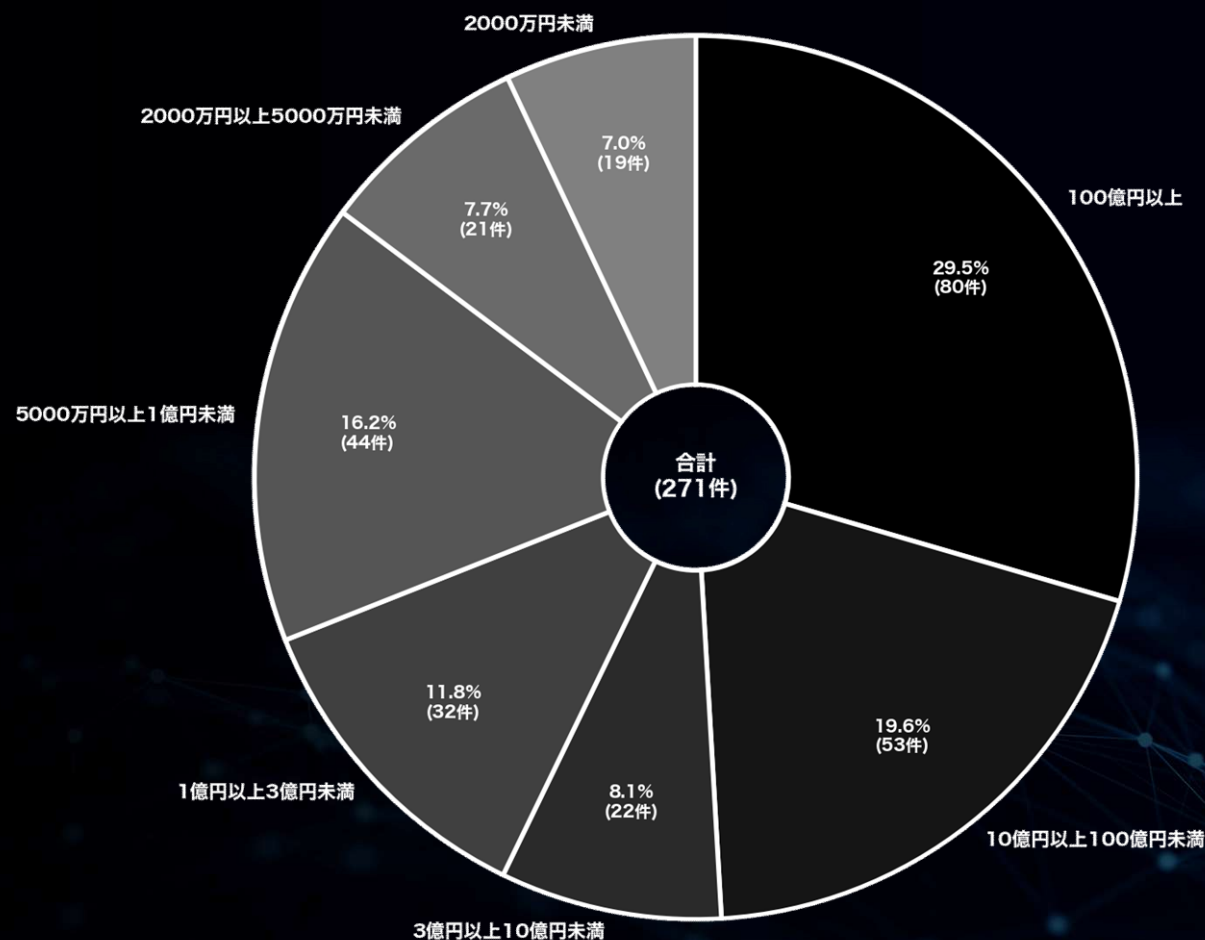
(過去2年間／2023年5月～2025年4月)

※資本金順に降順 / 資本金情報を公表していない一部の被害組織は除外

資本金	件数	割合(%)
100億円以上	80	29.5
10億円以上100億円未満	53	19.6
3億円以上10億円未満	22	8.1
1億円以上3億円未満	32	11.8
5000万円以上1億円未満	44	16.2
2000万円以上5000万円未満	21	7.7
2000万円未満	19	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)

2025

4

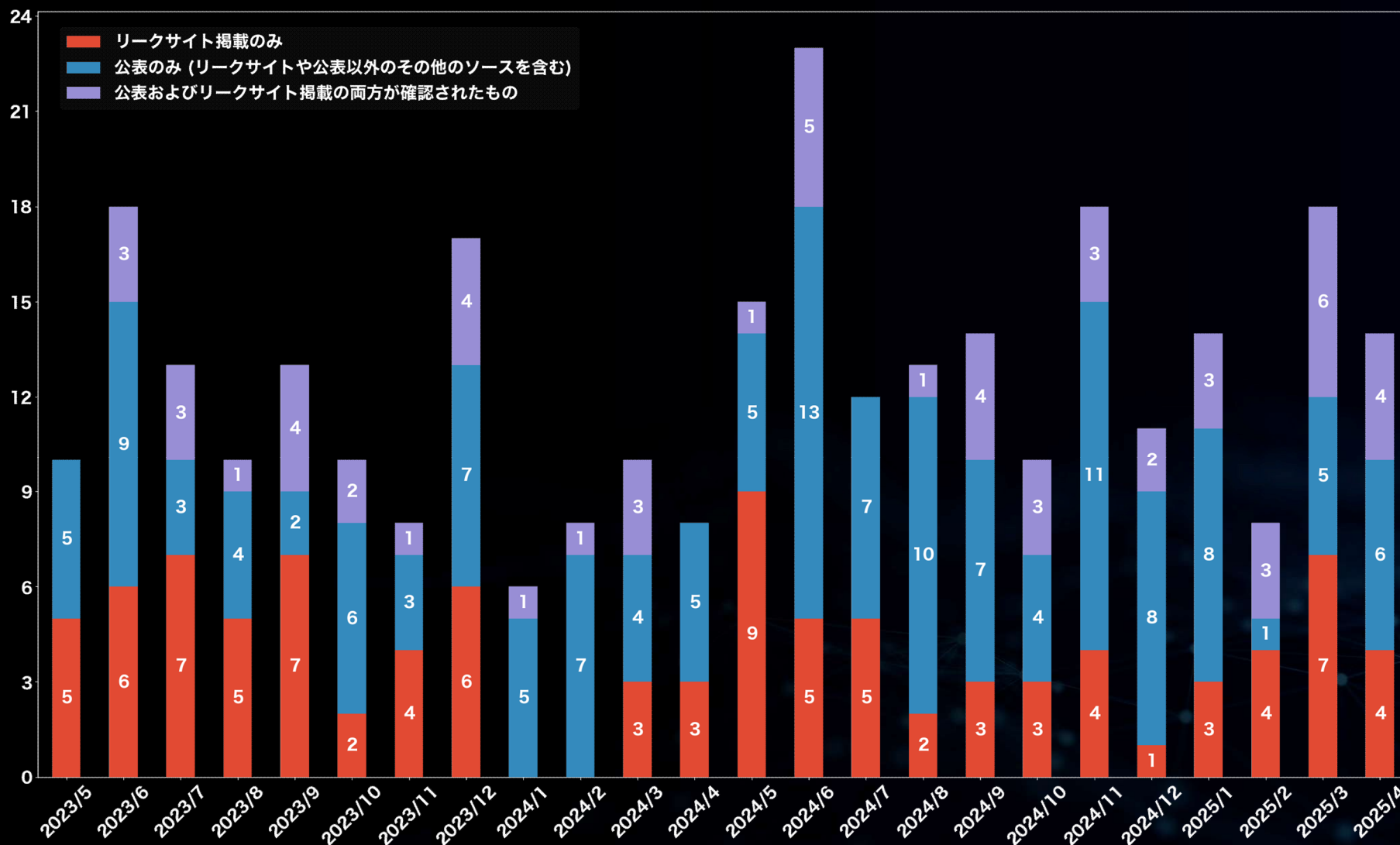
公表と暴露に関する統計

(国内)

公表割合 月別内訳 (国内)

(過去2年間／2023年5月～2025年4月)

▼ランサムウェア攻撃における公表数と掲載数の分析



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

2025

4

公となった国内被害組織 概要一覧

公となった国内被害組織概要一覧 (国内)

(過去1年間／2024年5月～2025年4月)

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

被害月	攻撃グループ	業種概要
2024/5	LockBit	製紙会社(海外拠点)
2024/5	(Unknown)	総合物流事業者
2024/5	Hunters International	音響関連機器メーカー(海外拠点)
2024/5	CLOP (CLOP)	大手文房具メーカー(海外拠点)
2024/5	(Unknown)	化学製品メーカー
2024/5	Ransomhub	ソフトウェア企業
2024/5	RansomHouse	建築部品メーカー
2024/5	(Unknown)	アルバム企画・制作
2024/5	(Unknown)	地方独立行政法人
2024/5	(Unknown)	不動産管理会社
2024/5	LockBit	ITサービス会社(海外拠点)
2024/5	8BASE	協同組合
2024/5	8BASE	OAサプライ用品メーカー
2024/5	8BASE	農業機械販売会社
2024/5	8BASE	税理士法人
2024/6	8BASE	電動機メーカー(海外拠点)
2024/6	8BASE	ITサービス会社
2024/6	(Unknown)	電子機器メーカー
2024/6	Phobos	総合ITサービス企業
2024/6	AKIRA	大手電機メーカー(海外拠点)
2024/6	(Unknown)	製業会社
2024/6	(Unknown)	機械部品メーカー
2024/6	(Unknown)	化学メーカー(海外拠点)
2024/6	BlackSuit	大手出版社
2024/6	(Unknown)	総合会計・コンサルティンググループ
2024/6	(Unknown)	大手オフィス家具メーカー
2024/6	(Unknown)	通信機器販売業者
2024/6	CACTUS	アパレルメーカー
2024/6	INC Ransom	工業機械メーカー(海外拠点)

被害月	攻撃グループ	業種概要
2024/6	(Unknown)	仏具メーカー
2024/6	(Unknown)	建設コンサルタント会社
2024/6	CACTUS	内装材メーカー(海外拠点)
2024/6	8BASE	RS
2024/6	8BASE	総合建設メーカー
2024/6	LockBit	通信機器メーカー
2024/6	(Unknown)	食品メーカー
2024/6	(Unknown)	総合エンジニアリング会社
2024/6	(Unknown)	建設コンサルタント会社
2024/7	(Unknown)	商業印刷業
2024/7	Ransomhub	大手システムインテグレーター(海外拠点)
2024/7	(Unknown)	電子機器メーカー(海外拠点)
2024/7	Lockbit	レンタルサービス会社
2024/7	(Unknown)	印刷サービス会社
2024/7	(Unknown)	大手総合ディスプレイ企業
2024/7	(Unknown)	青果販売会社
2024/7	Hunters International	光学レンズメーカー
2024/7	Ransomhub	大手建設会社
2024/7	MEOOW	空調機器メーカー
2024/7	(Unknown)	無線通信機器メーカー
2024/7	CACTUS	電子部品メーカー(海外拠点)
2024/8	(Unknown)	介護サービスプロバイダー
2024/8	Everest	精密機器メーカー(海外拠点)
2024/8	(Unknown)	システムインテグレーター
2024/8	(Unknown)	ペット用品メーカー
2024/8	(Unknown)	ヘルスケア用品メーカー
2024/8	(Unknown)	化学製品商社
2024/8	(Unknown)	海運技術ソリューションプロバイダー
2024/8	(Unknown)	学校法人

被害月	攻撃グループ	業種概要
2024/8	(Unknown)	公益財団法人
2024/8	(Unknown)	保険サービスプロバイダー
2024/8	(Unknown)	電子機器メーカー
2024/8	Everest	大手化学メーカー
2024/8	RansomHub	大手自動車メーカー(海外拠点)
2024/9	RansomHub	アミューズメント機器メーカー
2024/9	Cicada3301	化学メーカー
2024/9	RansomHub	大手輸送用機器メーカー(海外拠点)
2024/9	(Unknown)	学校法人
2024/9	(Unknown)	情報通信サービス会社
2024/9	(Unknown)	物流サービス会社
2024/9	(Unknown)	物流サービス会社
2024/9	Brain Cipher	大手商社(海外拠点)
2024/9	(Unknown)	包装資材製造メーカー
2024/9	(Unknown)	食品輸入商社
2024/9	RansomHub	産業用機器メーカー
2024/9	RansomHub	産業ソリューションプロバイダー
2024/9	Medusa	情報通信サービス会社
2024/9	(Unknown)	保育サービスプロバイダー
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	MEOOW	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

(※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5月～2025年4月)

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

被害月	攻撃グループ	業種概要
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)	ソフトウェアメーカー
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
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	CLOP (CLOP)	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
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
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

被害月	攻撃グループ	業種概要
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)	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)
2025/4	(Unknown)	総合エンジニアリング企業
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)	私立大学
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	Termite	光応用製品メーカー(海外拠点)

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

※ 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5月～2025年4月)

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

▼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

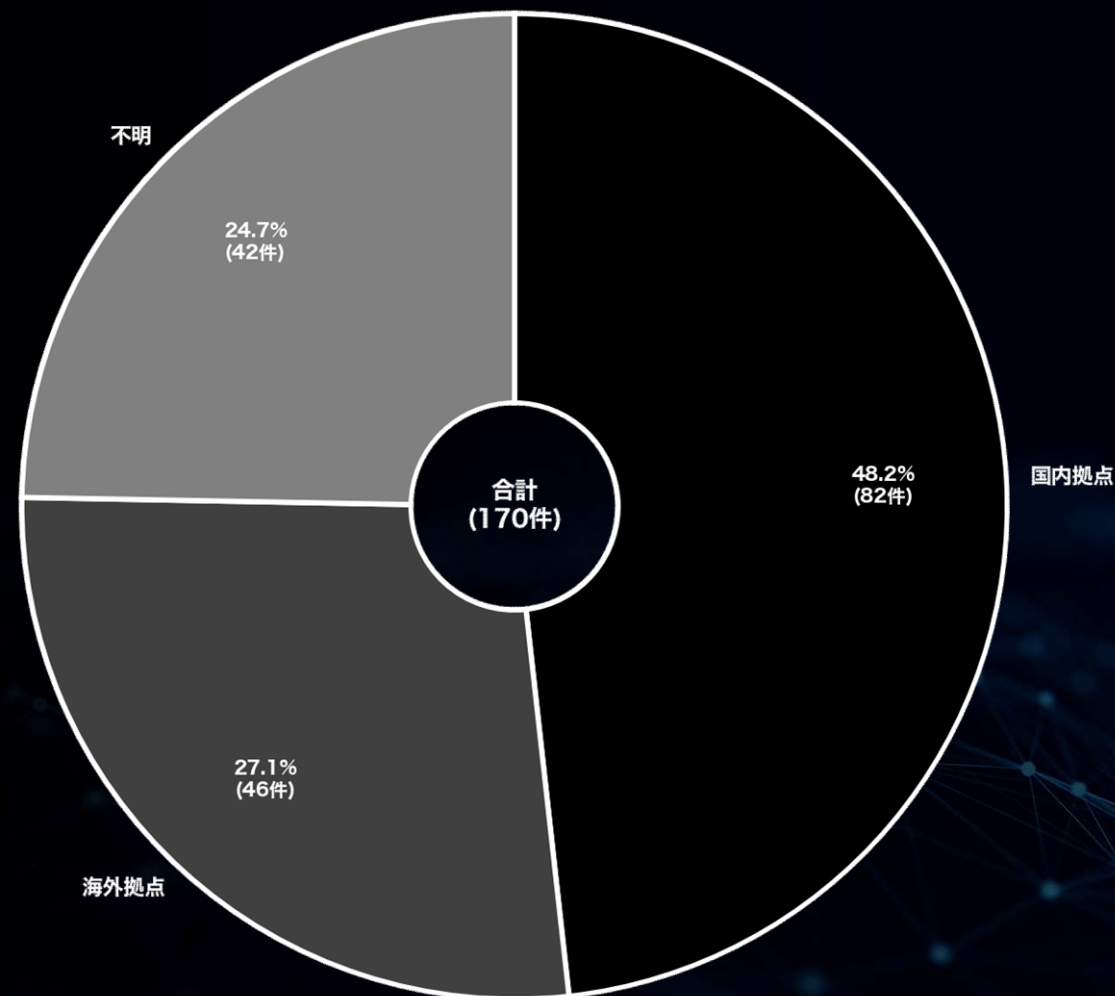
※

「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	82	48.2
海外拠点	46	27.1
不明	42	24.7



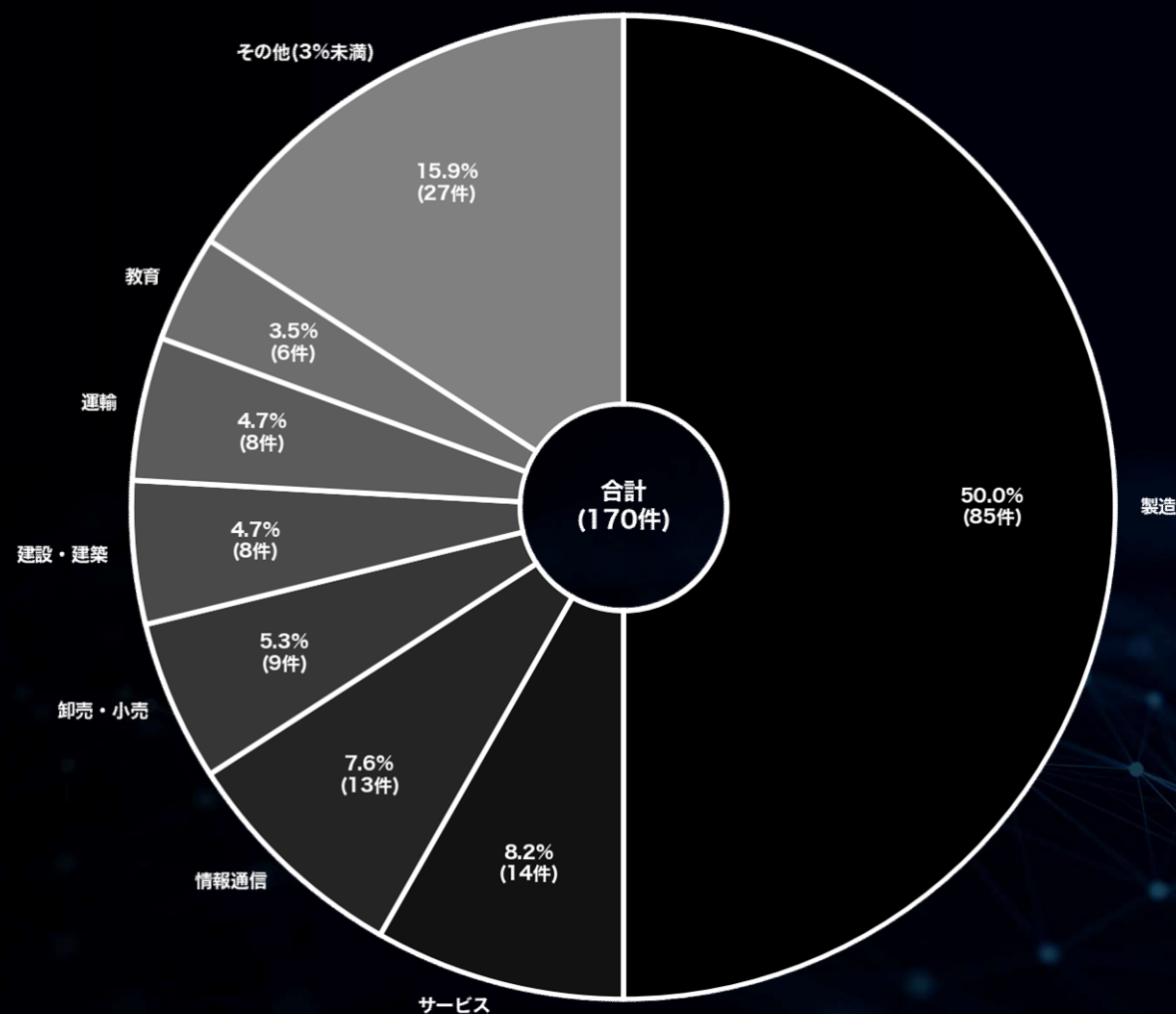
(※本ページの表／グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

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5月～2025年4月)

業種	件数	割合(%)
製造	85	50.0
サービス	14	8.2
情報通信	13	7.6
卸売・小売	9	5.3
建設・建築	8	4.7
運輸	8	4.7
教育	6	3.5
その他(3%未満)	27	15.9

▼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)

2025

4

中小企業における被害分析

(国内)

中小企業の定義※は業種により法的に異なるが、本資料では中小企業を『資本金3億円未満の組織』と定義する。
※中小企業庁「中小企業・小規模事業者の定義」:<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5月～2025年4月)

赤色は中小企業を示す

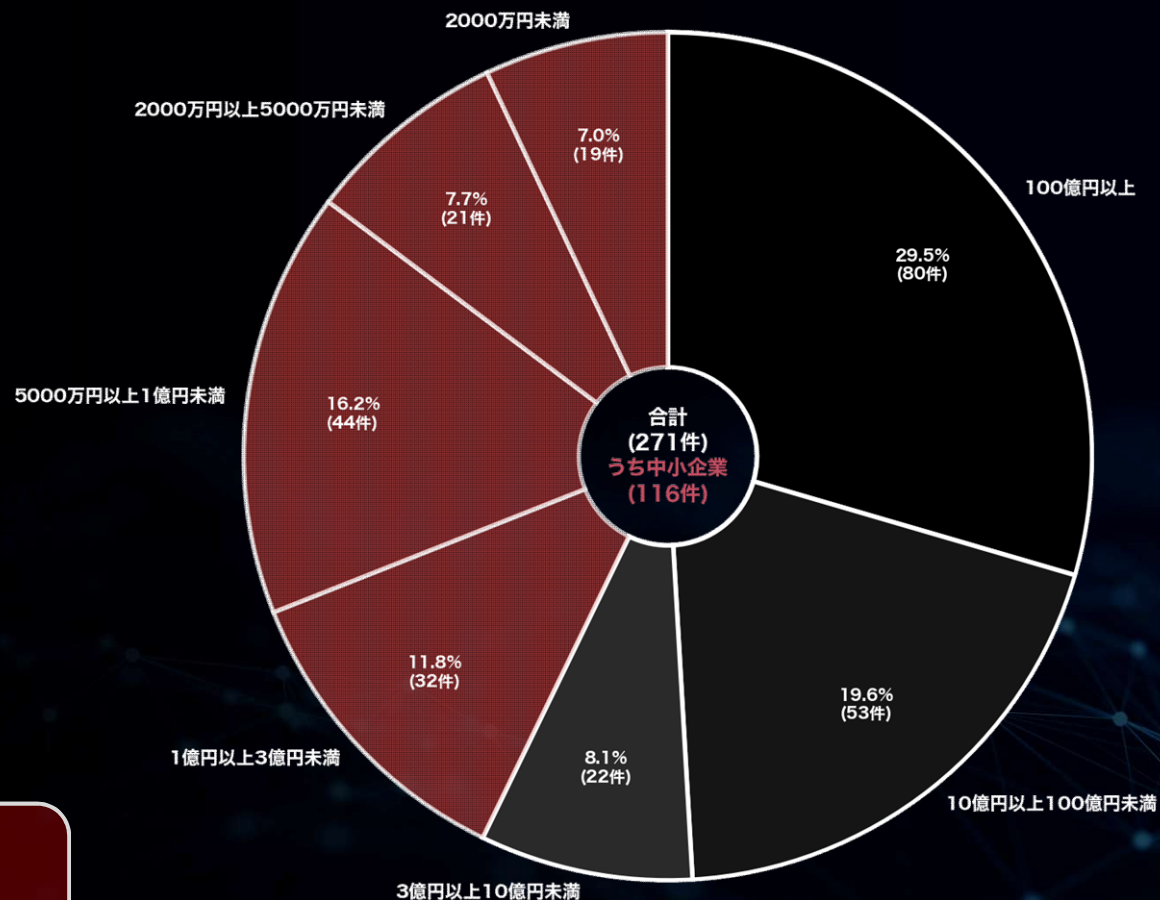
※資本金順に降順 / 資本金情報を公表していない一部の被害組織は除外

資本金	件数	割合(%)
100億円以上	80	29.5
10億円以上100億円未満	53	19.6
3億円以上10億円未満	22	8.1
1億円以上3億円未満	32	11.8
5000万円以上1億円未満	44	16.2
2000万円以上5000万円未満	21	7.7
2000万円未満	19	7.0

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116件にのぼり、全体の42.8%を占める。

これらの被害は、リークサイトへの掲載や公表から確認できたものだが、表面化していない被害も多数存在する可能性があり、実際の被害総数はさらに大きいと考えられる。

▼ランサムウェア攻撃を受けた日本関連組織の規模 (資本金)



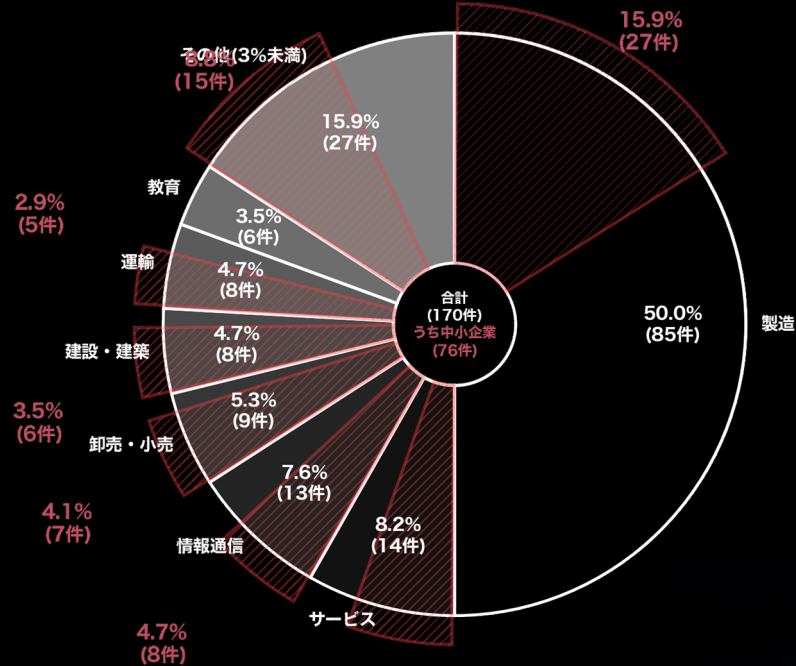
(※本ページの表／グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

公となった国内被害組織における業種割合 (国内-中小企業)

(過去1年間／2024年5月～2025年4月)

赤色は中小企業を示す

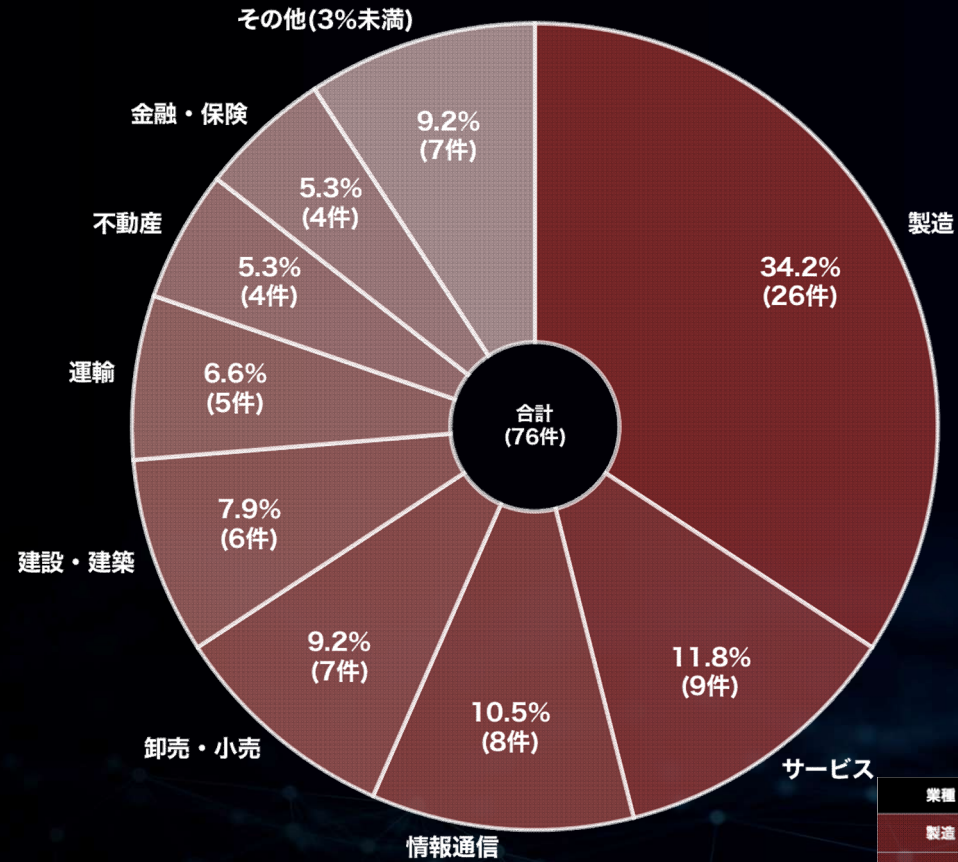
▼全体割合



※各数値の()内の数値は、資本金3億円未満の組織に対する集計結果を示す

業種	件数	割合(%)
製造	85 (27)	50.0 (15.9)
サービス	14 (9)	8.2 (5.3)
情報通信	13 (8)	7.6 (4.7)
卸売・小売	9 (7)	5.3 (4.1)
建設・建築	8 (6)	4.7 (3.5)
運輸	8 (5)	4.7 (2.9)
教育	6	3.5
その他(3%未満)	27 (15)	15.9 (8.8)

▼中小企業のための割合



業種	件数	割合(%)
製造	26	34.2
サービス	9	11.8
情報通信	8	10.5
卸売・小売	7	9.2
建設・建築	6	7.9
運輸	5	6.6
不動産	4	5.3
金融・保険	4	5.3
その他(3%未満)	7	9.2

過去1年間の業種別分析においては、中小企業のみには抜粋すると、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。

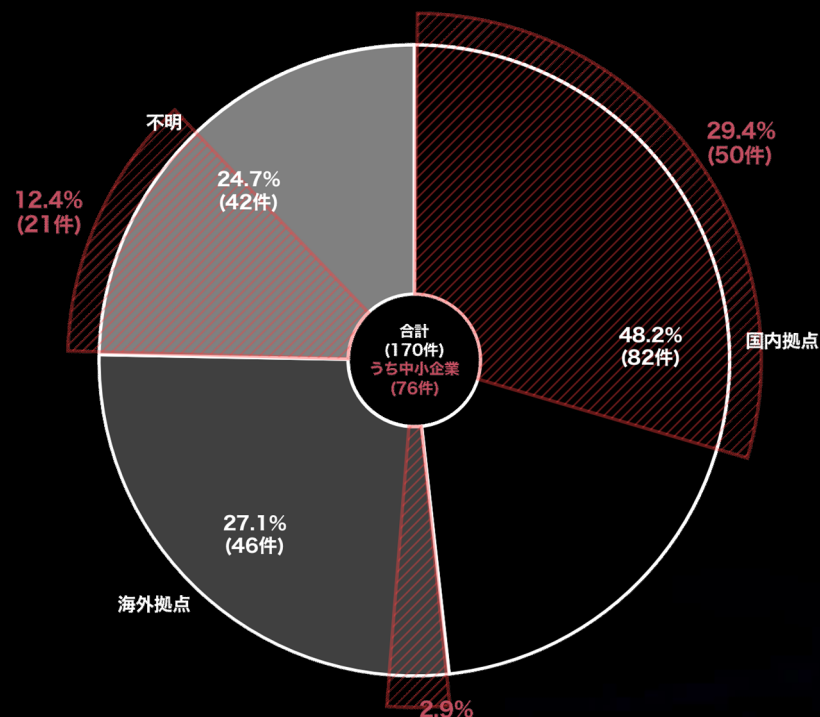
※医療や教育、行政機関など資本金が不明な一部の組織については集計から除外

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5月～2025年4月)

赤色は中小企業を示す

▼全体割合



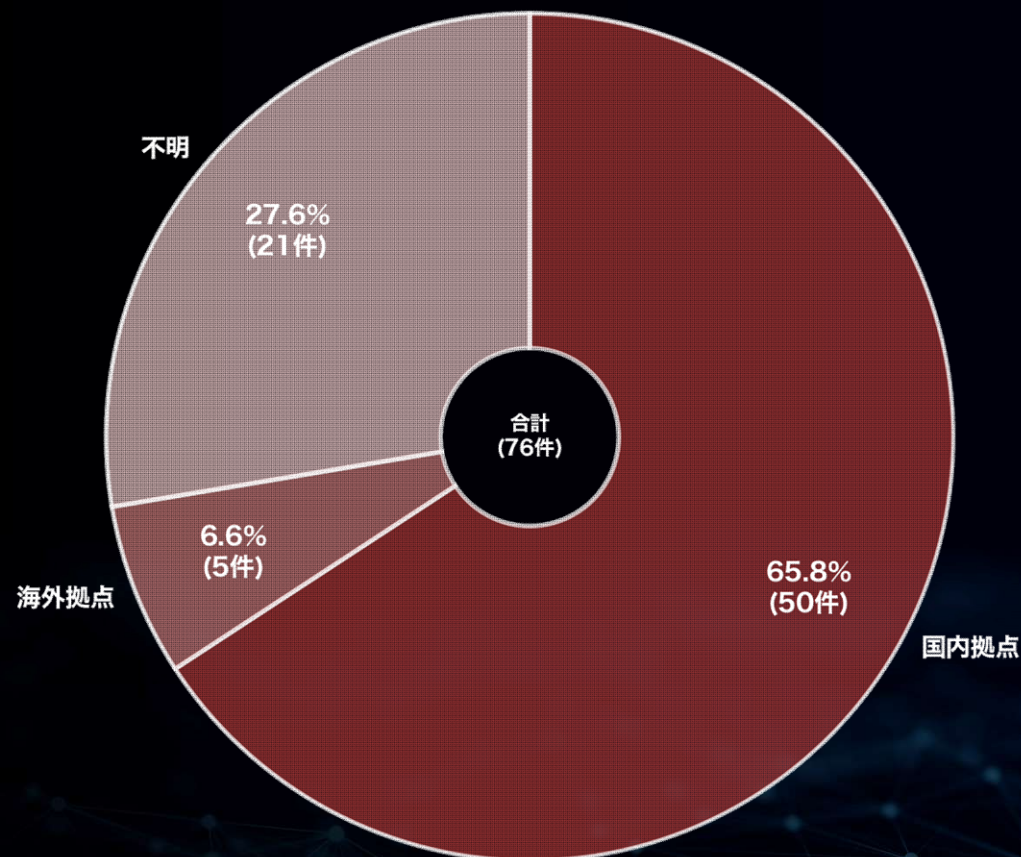
※
 「国内拠点」：公表等により、国内拠点における被害事案と判断されるケース数
 「海外拠点」：公表等により、海外拠点（支社／関係会社）における被害事案と判断されるケース数
 「不明」：上記以外、被害拠点の地域的情報が得られなかったケース数
 ※各数値の()内の数値は、資本金10億円未満の組織に対する集計結果を示す

拠点	件数 (中小企業)	割合 (%)
国内拠点	82 (50)	48.2 (29.4)
海外拠点	46 (5)	27.1 (2.9)
不明	42 (21)	24.7 (12.4)
合計	170 (76)	100 (44.7)

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

▼中小企業のための割合



拠点	件数 (中小企業)	割合 (%)
国内拠点	50	65.8
海外拠点	5	6.6
不明	21	27.6

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5月～2025年4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
2024/5	LockBit	製紙会社(海外拠点)
2024/5	(Unknown)	総合物流事業者
2024/5	Hunters International	音響関連機器メーカー(海外拠点)
2024/5	CLOP (CLOP)	大手文房具メーカー(海外拠点)
2024/5	(Unknown)	化学製品メーカー
2024/5	Ransomhub	ソフトウェア企業
2024/5	RansomHouse	建築部品メーカー
2024/5	(Unknown)	アルバム企画・制作
2024/5	(Unknown)	地方独立行政法人
2024/5	(Unknown)	不動産管理会社
2024/5	LockBit	ITサービス会社(海外拠点)
2024/5	8BASE	協同組合
2024/5	8BASE	OAサプライ用品メーカー
2024/5	8BASE	農業機械販売会社
2024/5	8BASE	税理士法人
2024/6	8BASE	電動機メーカー(海外拠点)
2024/6	8BASE	ITサービス会社
2024/6	(Unknown)	電子機器メーカー
2024/6	Phobos	総合ITサービス企業
2024/6	AKIRA	大手電機メーカー(海外拠点)
2024/6	(Unknown)	製薬会社
2024/6	(Unknown)	機械部品メーカー
2024/6	(Unknown)	化学メーカー(海外拠点)
2024/6	BlackSuit	大手出版社
2024/6	(Unknown)	総合会計・コンサルティンググループ
2024/6	(Unknown)	大手オフィス家具メーカー
2024/6	(Unknown)	通信機器販売業者
2024/6	CACTUS	アパレルメーカー
2024/6	INC Ransom	工業機械メーカー(海外拠点)

被害月	攻撃グループ	業種概要
2024/6	(Unknown)	仏具メーカー
2024/6	(Unknown)	建設コンサルタント会社
2024/6	CACTUS	内装材メーカー(海外拠点)
2024/6	8BASE	RS
2024/6	8BASE	総合建設メーカー
2024/6	LockBit	通信機器メーカー
2024/6	(Unknown)	食品メーカー
2024/6	(Unknown)	総合エンジニアリング会社
2024/6	(Unknown)	建設コンサルタント会社
2024/7	(Unknown)	商業印刷業
2024/7	Ransomhub	大手システムインテグレーター(海外拠点)
2024/7	(Unknown)	電子機器メーカー(海外拠点)
2024/7	Lockbit	レンタルサービス会社
2024/7	(Unknown)	印刷サービス会社
2024/7	(Unknown)	大手総合ディスプレイ企業
2024/7	(Unknown)	青果販売会社
2024/7	Hunters International	光学レンズメーカー
2024/7	Ransomhub	大手建設会社
2024/7	MEOOW	空調機器メーカー
2024/7	(Unknown)	無線通信機器メーカー
2024/7	CACTUS	電子部品メーカー(海外拠点)
2024/8	(Unknown)	介護サービスプロバイダー
2024/8	Everest	精密機器メーカー(海外拠点)
2024/8	(Unknown)	システムインテグレーター
2024/8	(Unknown)	ペット用品メーカー
2024/8	(Unknown)	ヘルスケア用品メーカー
2024/8	(Unknown)	化学製品商社
2024/8	(Unknown)	海運技術ソリューションプロバイダー
2024/8	(Unknown)	学校法人

被害月	攻撃グループ	業種概要
2024/8	(Unknown)	公益財団法人
2024/8	(Unknown)	保険サービスプロバイダー
2024/8	(Unknown)	電子機器メーカー
2024/8	Everest	大手化学メーカー
2024/8	RansomHub	大手自動車メーカー(海外拠点)
2024/9	RansomHub	アミューズメント機器メーカー
2024/9	Cicada3301	化学メーカー
2024/9	RansomHub	大手輸送用機器メーカー(海外拠点)
2024/9	(Unknown)	学校法人
2024/9	(Unknown)	情報通信サービス会社
2024/9	(Unknown)	物流サービス会社
2024/9	(Unknown)	物流サービス会社
2024/9	Brain Cipher	大手商社(海外拠点)
2024/9	(Unknown)	包装資材製造メーカー
2024/9	(Unknown)	食品輸入商社
2024/9	RansomHub	産業用機器メーカー
2024/9	RansomHub	産業ソリューションプロバイダー
2024/9	Medusa	情報通信サービス会社
2024/9	(Unknown)	保育サービスプロバイダー
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	MEOOW	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

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

公となった国内被害組織概要一覧 (国内-中小企業)

(過去1年間／2024年5月～2025年4月)

赤色は中小企業を示す

被害月	攻撃グループ	業種概要
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)	ソフトウェアメーカー
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
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	CLOP (CLOP)	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
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
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	リビッド品製造
2025/3	(Unknown)	不動産仲介

被害月	攻撃グループ	業種概要
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)	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)
2025/4	(Unknown)	総合エンジニアリング企業
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)	私立大学
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	Termite	光応用製品メーカー(海外拠点)

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

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

2025

4

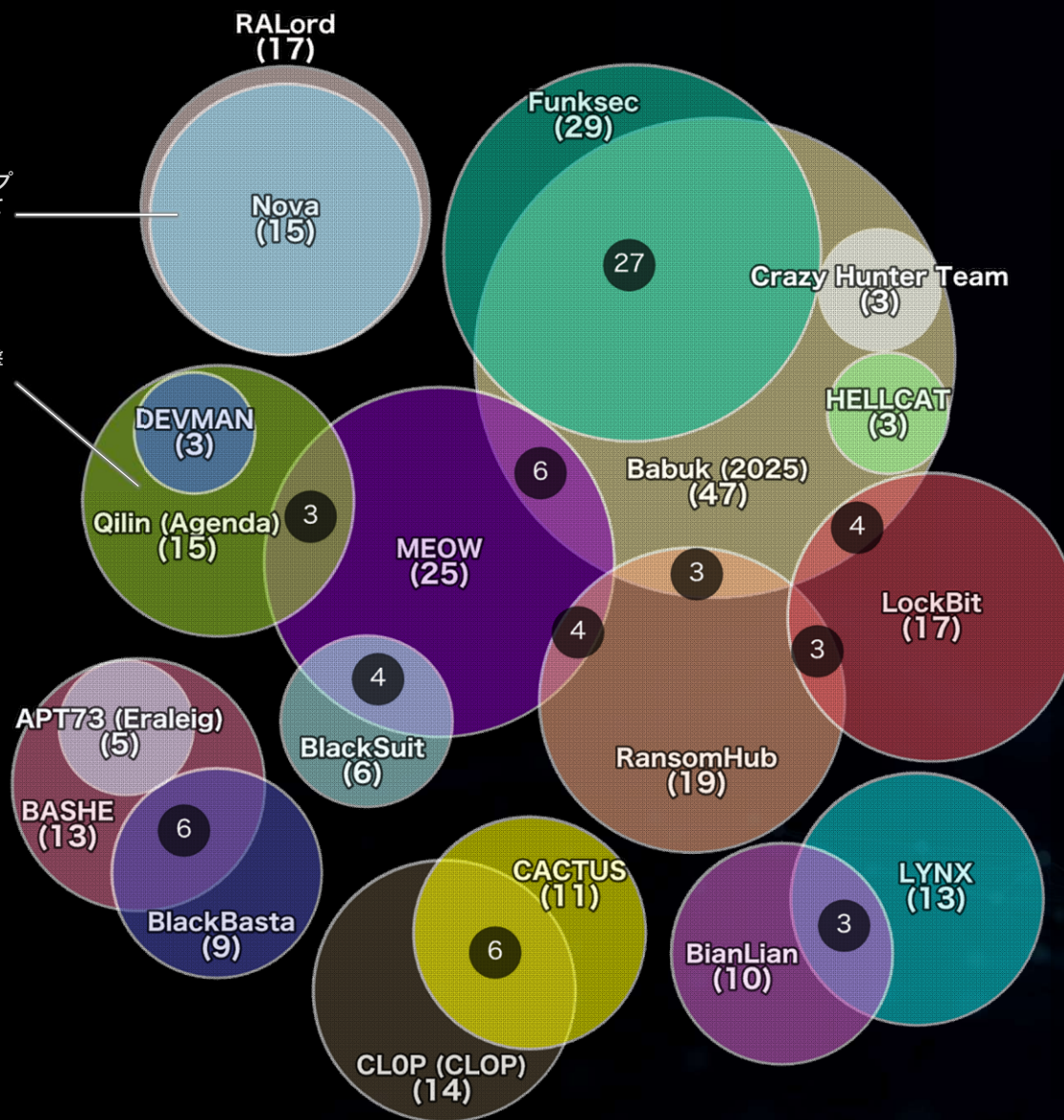
多重被害に関する分析

繰り返し暴露された事案数の集計と攻撃グループ間の関係性 (全世界)

(過去1年間／2024年5月～2025年4月) (累計174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、AlphaV (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

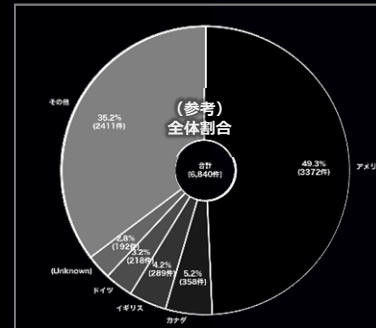
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

多重被害に遭った被害組織の傾向と分析 (全世界)

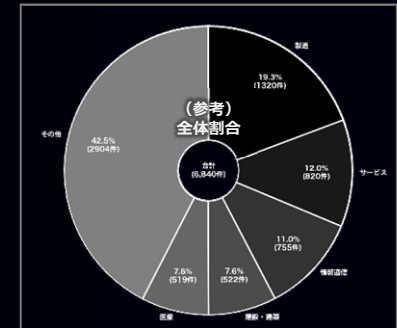
(過去1年間／2024年5月～2025年4月)

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

(参考比較) 同期間の全データにおける割合

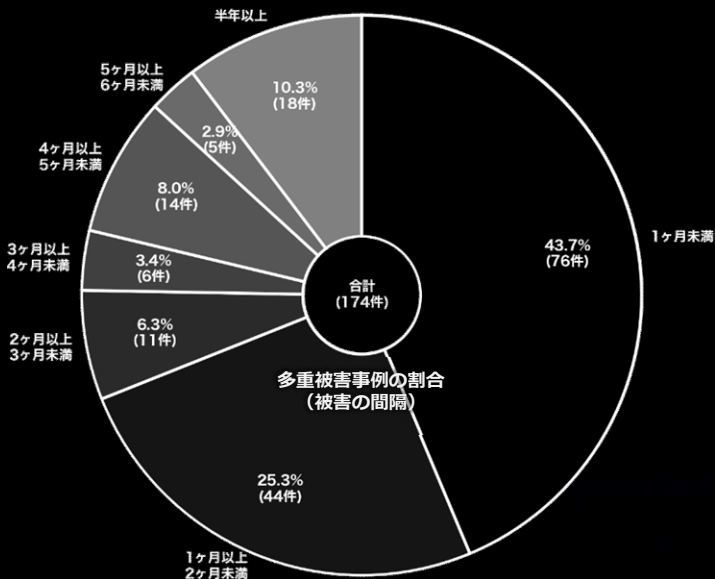


(参考比較) 同期間の全データにおける割合

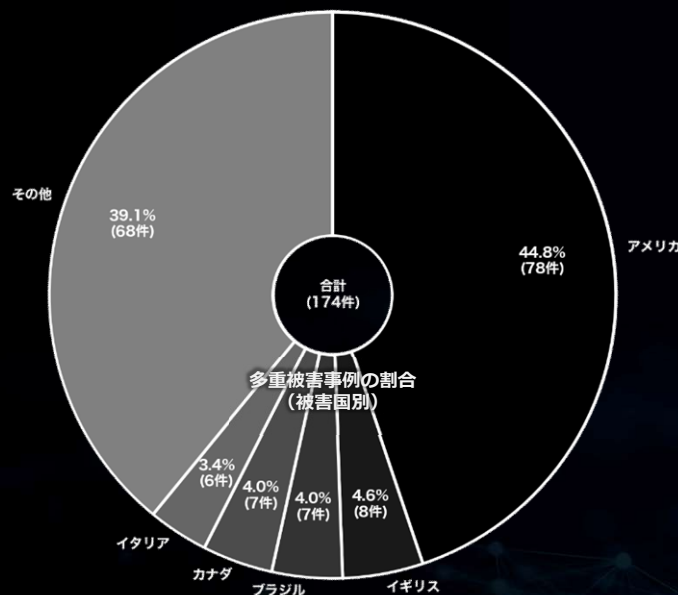


▼被害の間隔

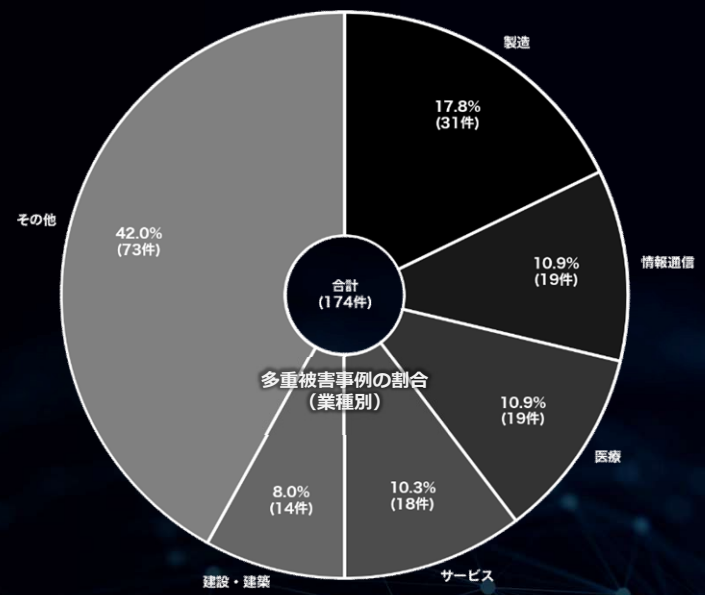
(一度目の被害から二度目の被害までの間隔)



▼被害国別



▼業種別



▶多重被害に遭った組織数の累計：174件 (全体6840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ます。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。

2025

4

業種に関する分析

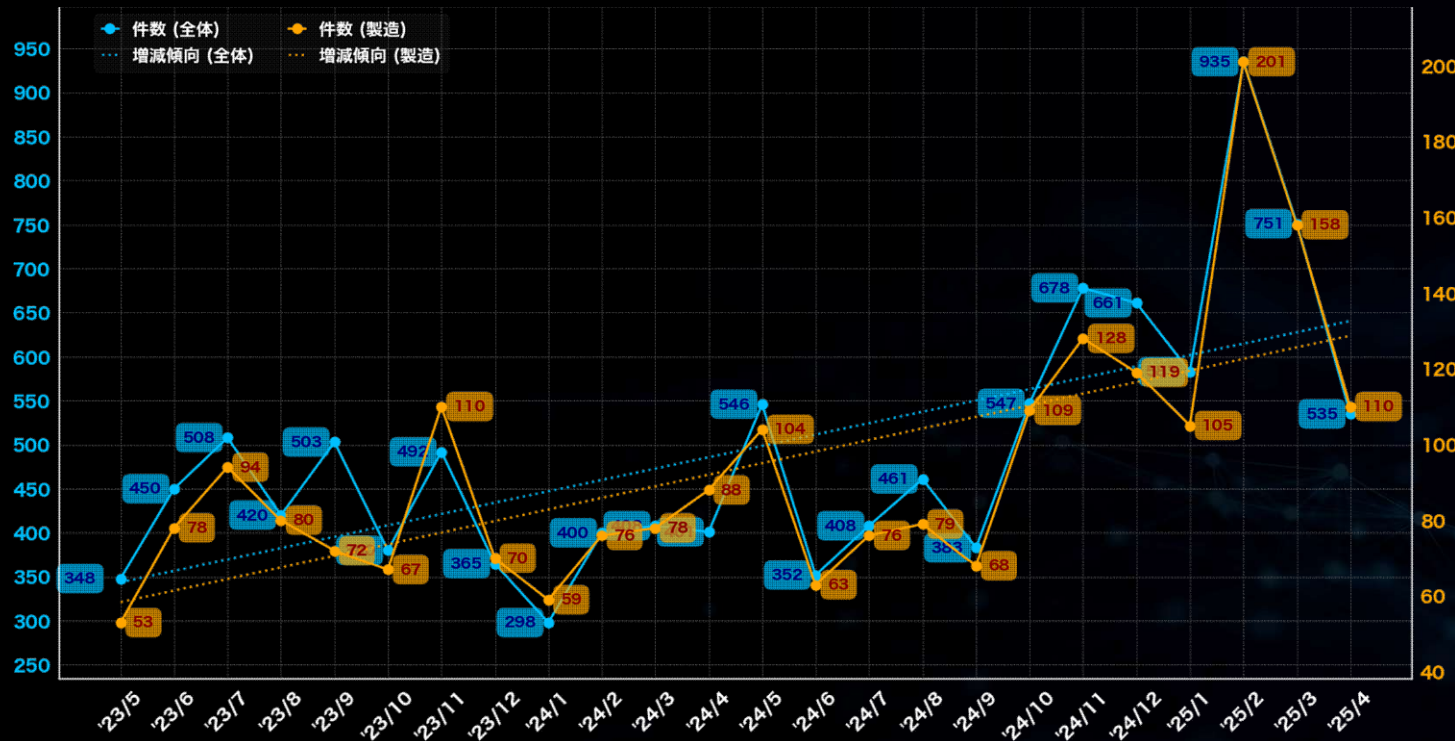
(過去2年間のリークサイト掲載上位10業種)

業種に関する分析 (全世界)

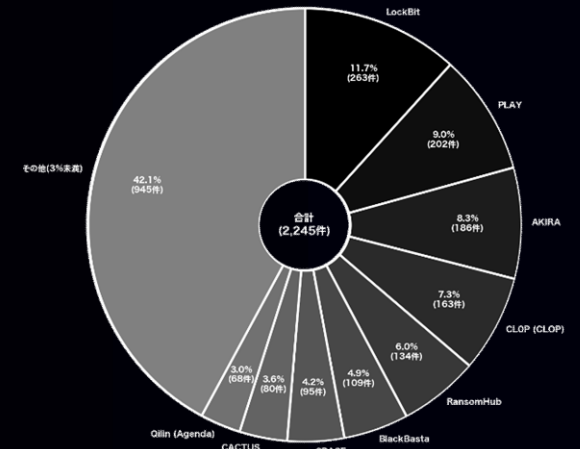
(過去2年間／2023年5月～2025年4月)

製造

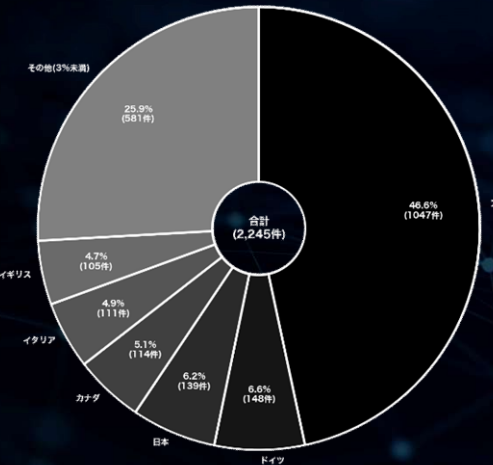
「製造」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、201件の掲載があった。一方、最も少なかった月は2023年5月で、53件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いで日本とドイツがそれぞれ約7%と約6%である。攻撃グループについては、少なくとも107のグループが関与しており、特に「LockBit」が263件のリークサイト掲載を実施している。次いで「PLAY」と「AKIRA」がそれぞれ202件と186件の掲載を行っている。製造関連の件数は全体件数に対して高い割合で推移しており、全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



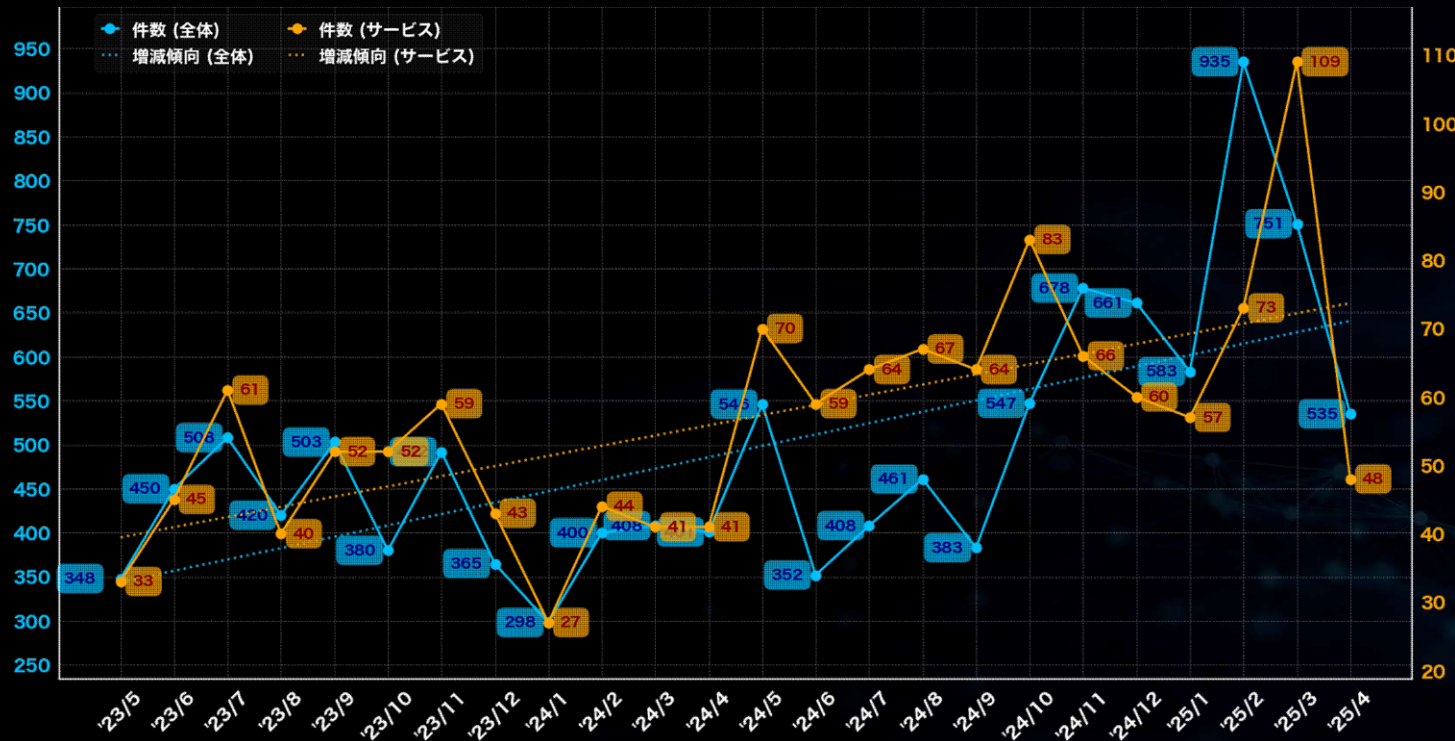
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

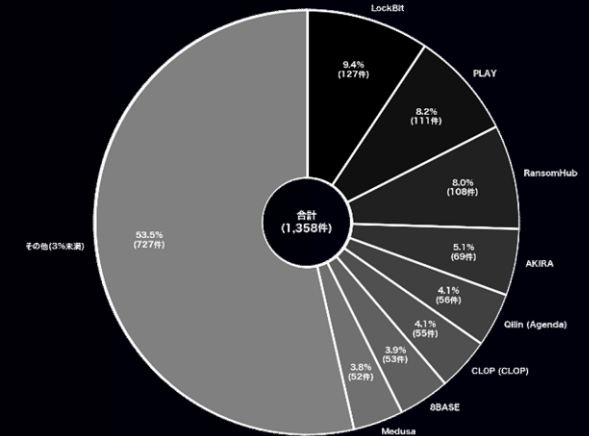
(過去2年間／2023年5月～2025年4月)

サービス

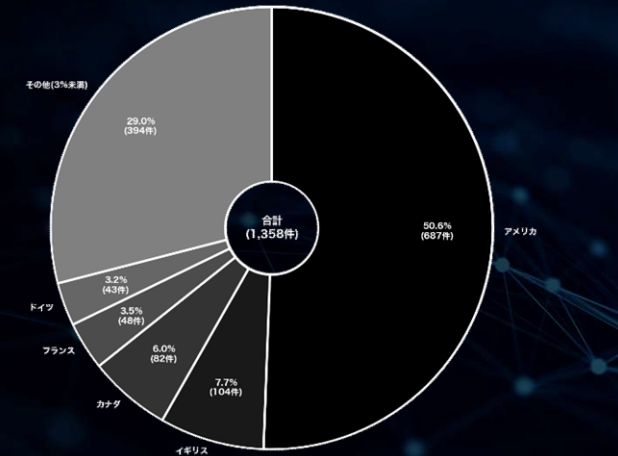
「サービス」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年3月で、109件の掲載があった。一方、最も少なかった月は2024年1月で、27件であった。被害組織の所在国の割合では、アメリカが約51%と最も多く、次いでイギリスとカナダがそれぞれ約8%と約6%である。攻撃グループについては、少なくとも96のグループが関与しており、特に「LockBit」が127件のリークサイト掲載を実施している。次いで「PLAY」と「RansomHub」とがそれぞれ108件と106件の掲載を行っている。サービス関連の件数は製造関連と同じく全体件数に対し、高い割合をキープしており、年々その割合は高まっている。



▼攻撃グループ別



▼国別



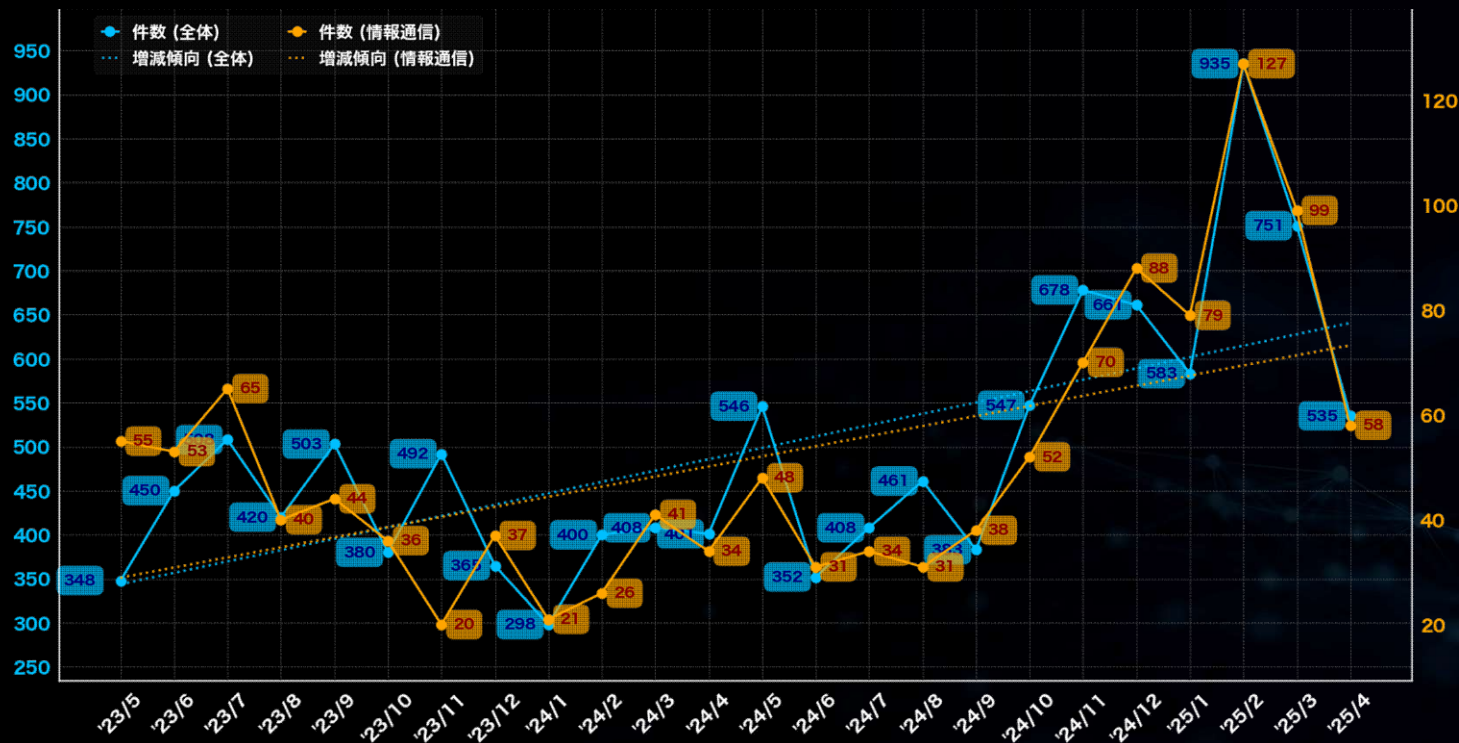
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

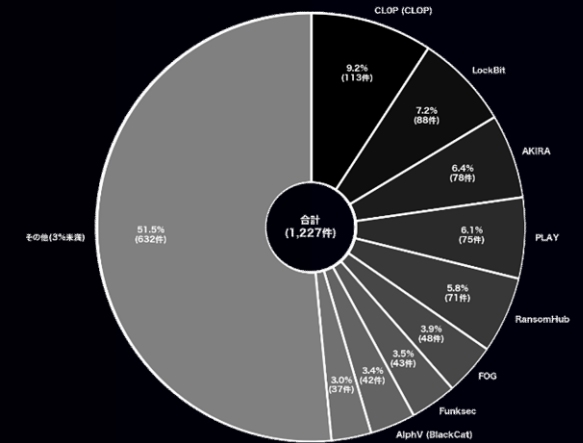
(過去2年間／2023年5月～2025年4月)

情報通信

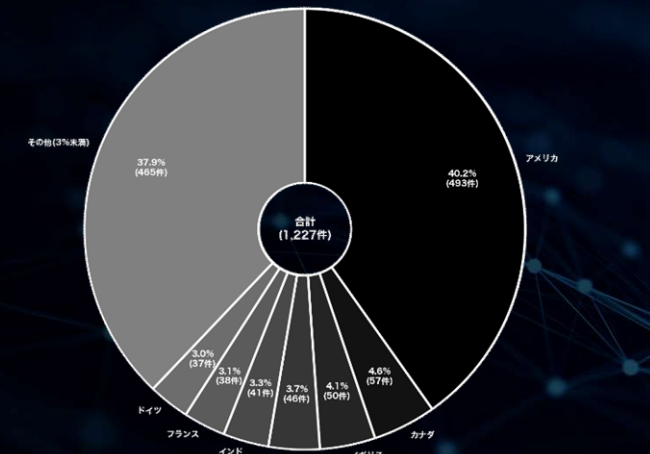
「情報通信」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、127件の掲載があった。一方、最も少なかった月は2023年11月で、20件であった。被害組織の所在国の割合では、アメリカが約40%と最も多く、次いでイギリスとカナダがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも102のグループが関与しており、特に「CLOP (CLOP)」が113件のリークサイト掲載を実施している。次いで「LockBit」と「AKIRA」がそれぞれ88件と78件の掲載を行っている。過去2年間におけるリークサイト掲載件数の上位2種である「製造」、「サービス」と比較すると緩やかではあるが、増加傾向にある。



▼攻撃グループ別



▼国別



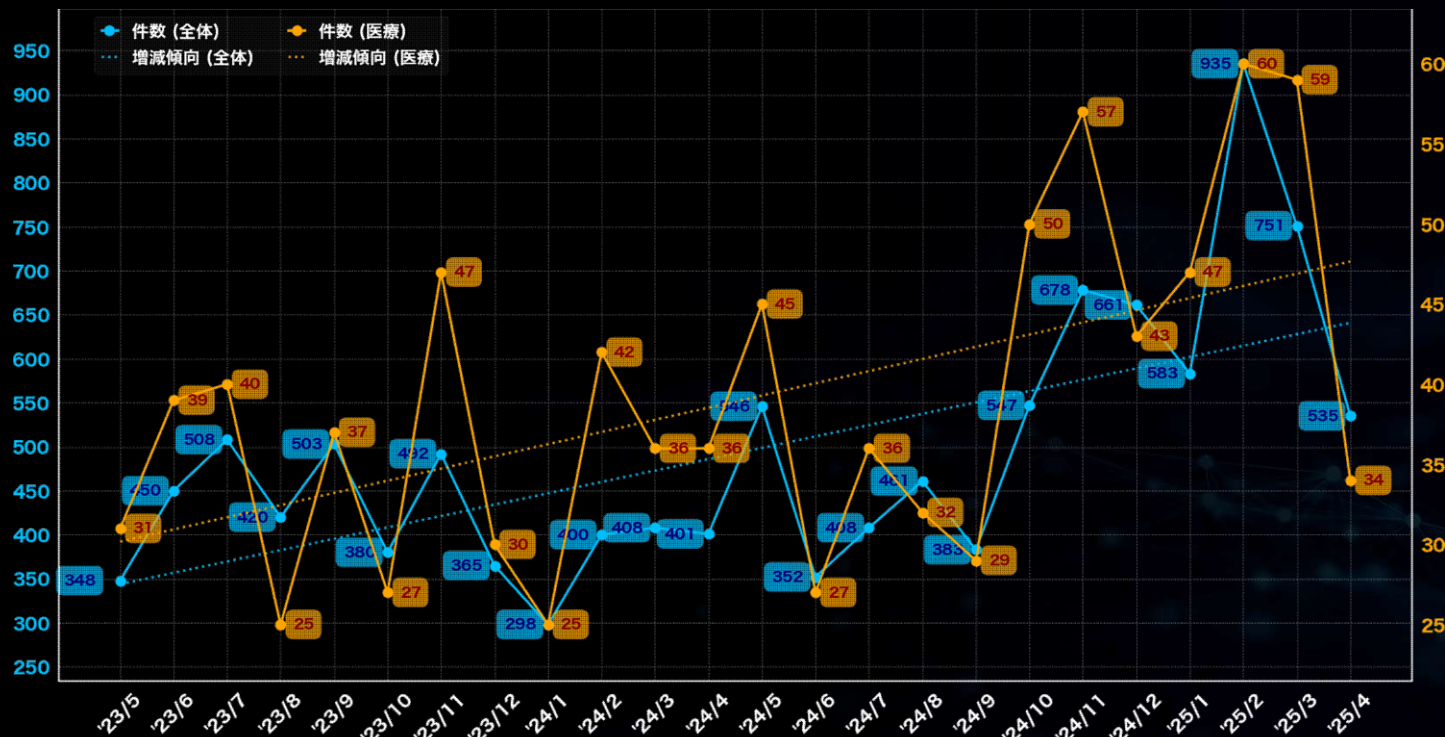
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

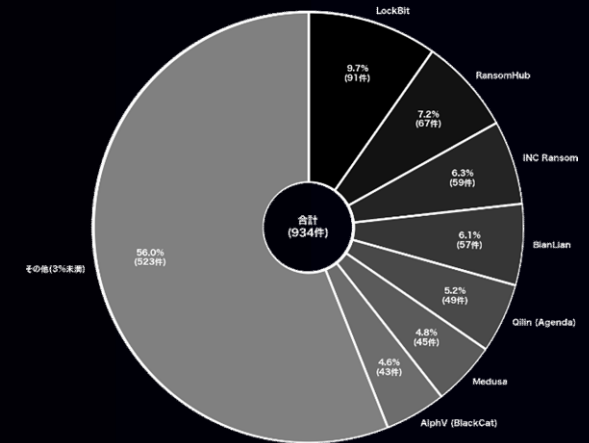
(過去2年間／2023年5月～2025年4月)

医療

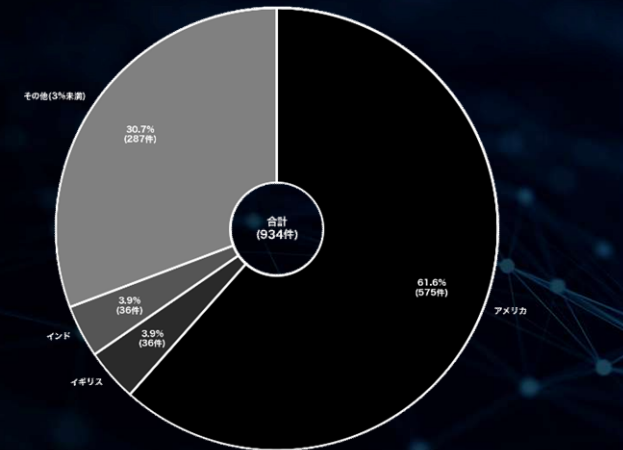
「医療」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、60件の掲載があった。一方、最も少なかった月は2023年8月および2024年1月で、25件であった。被害組織の所在国の割合では、アメリカが約62%と最も多く、次いでイギリス、インドがそれぞれ約4%である。攻撃グループについては、少なくとも91のグループが関与しており、特に「LockBit」が91件のリークサイト掲載を実施している。次いで「RansomHub」と「INC Ransom」がそれぞれ67件と59件の掲載を行っている。かつては低水準だった医療関連の被害数は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



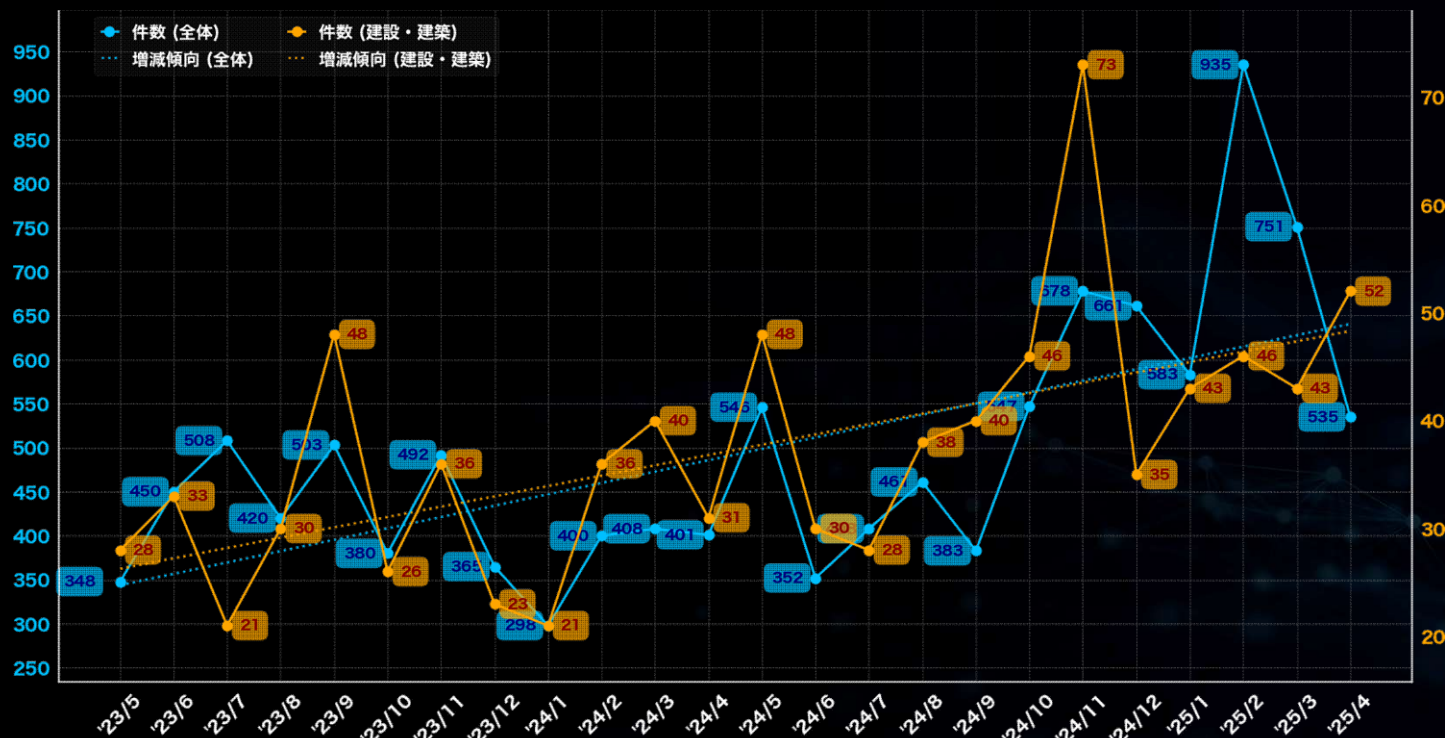
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

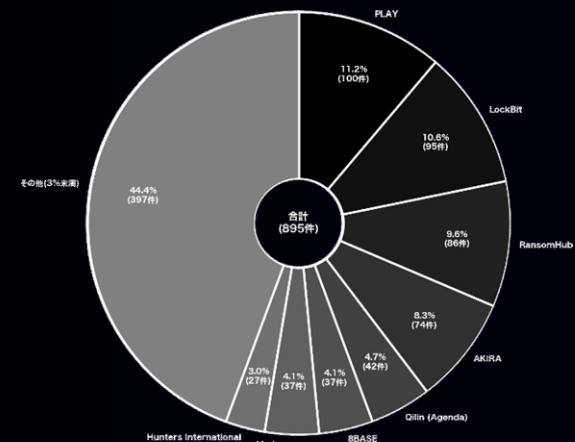
(過去2年間／2023年5月～2025年4月)

建設・建築

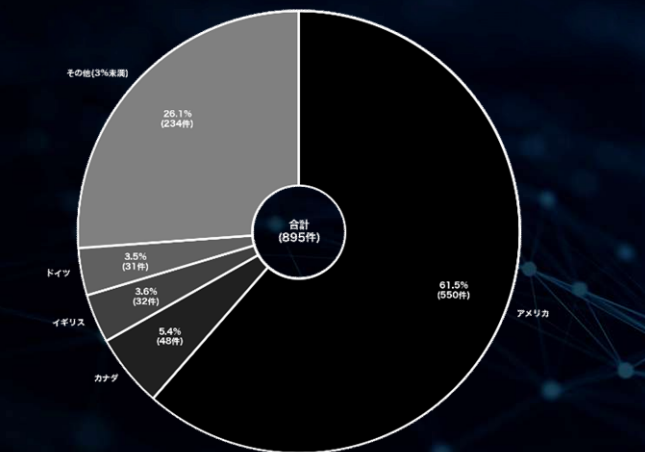
「建設・建築」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2024年11月で、73件の掲載があった。一方、最も少なかった月は2023年7月および2024年1月で、21件であった。被害組織の所在国の割合では、アメリカが約62%と最も多く、次いでカナダとイギリスがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも84のグループが関与しており、特に「PLAY」が100件のリークサイト掲載を実施している。次いで「LockBit」と「RansomHub」がそれぞれ95件と86件の掲載を行っている。製造関連などと比べると件数は少ないものの、明確な増加傾向にある。



▼攻撃グループ別



▼国別



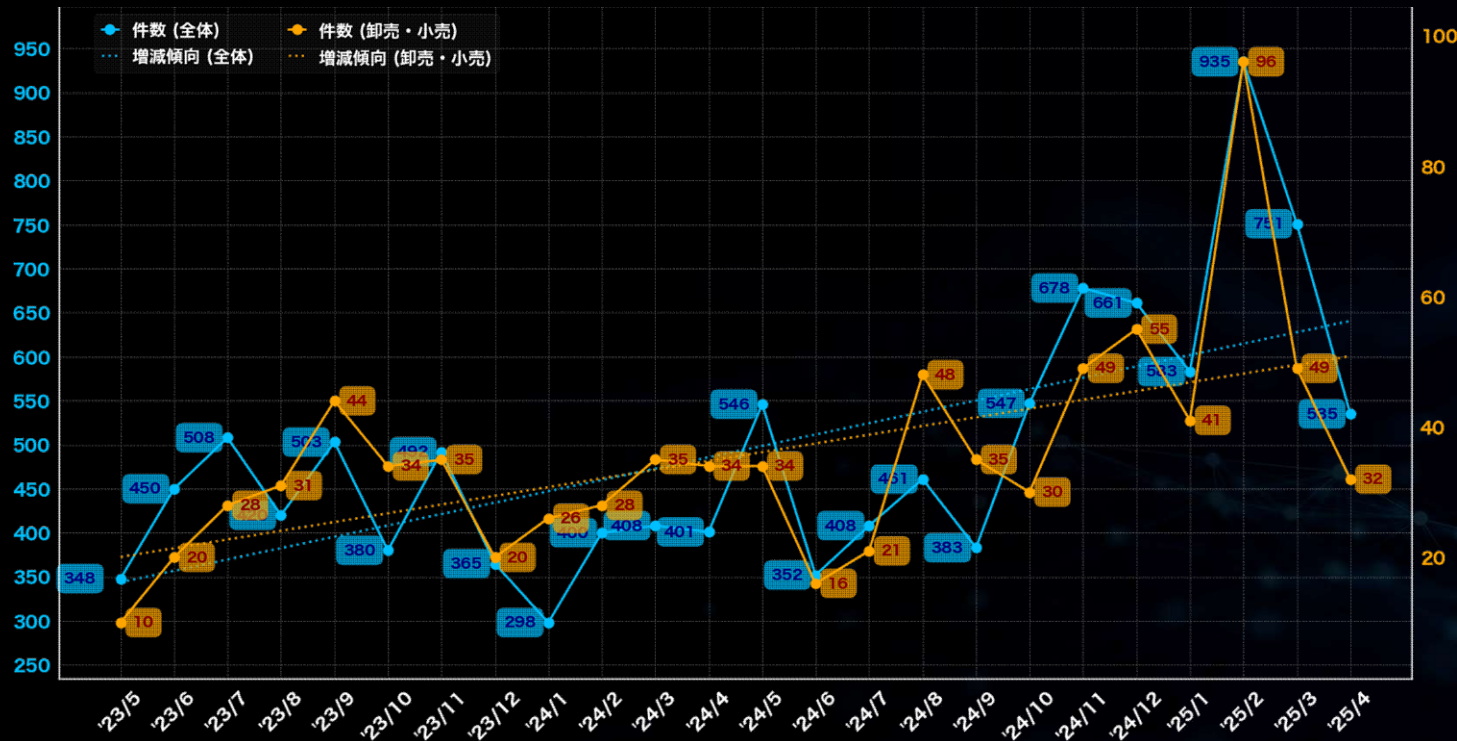
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

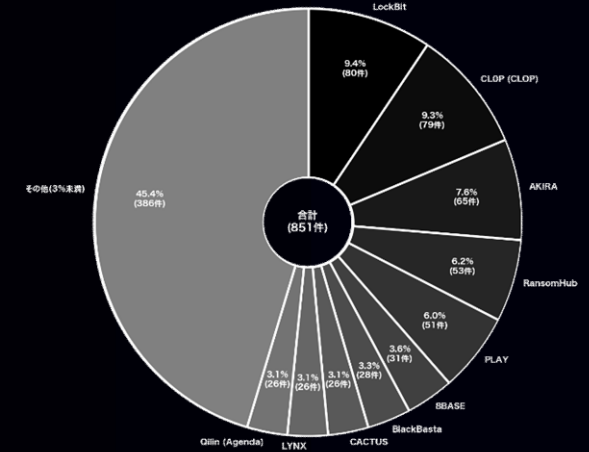
(過去2年間／2023年5月～2025年4月)

卸売・小売

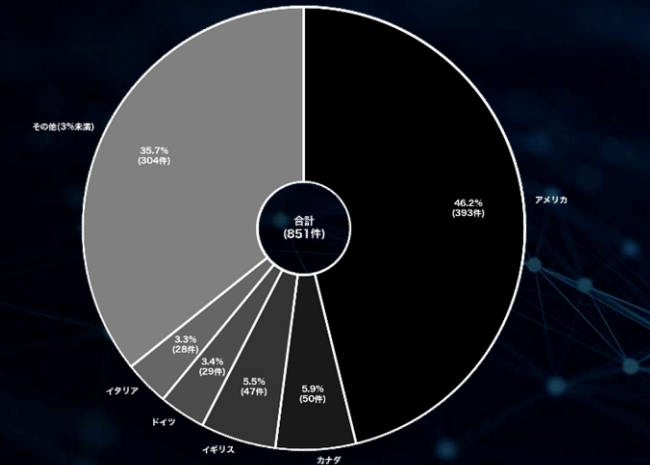
「卸売・小売」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、96件の掲載があった。一方、最も少なかった月は2023年5月で、10件であった。被害組織の所在国の割合では、アメリカが約46%と最も多く、次いでカナダとイギリスがそれぞれ約6%である。攻撃グループについては、少なくとも83のグループが関与しており、特に「LockBit」が80件のリークサイト掲載を実施している。次いで「CLOP (CLOP)」と「AKIRA」がそれぞれ79件と65件の掲載を行っている。卸売・小売関連は大きな増減の波があるものの、過去2年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



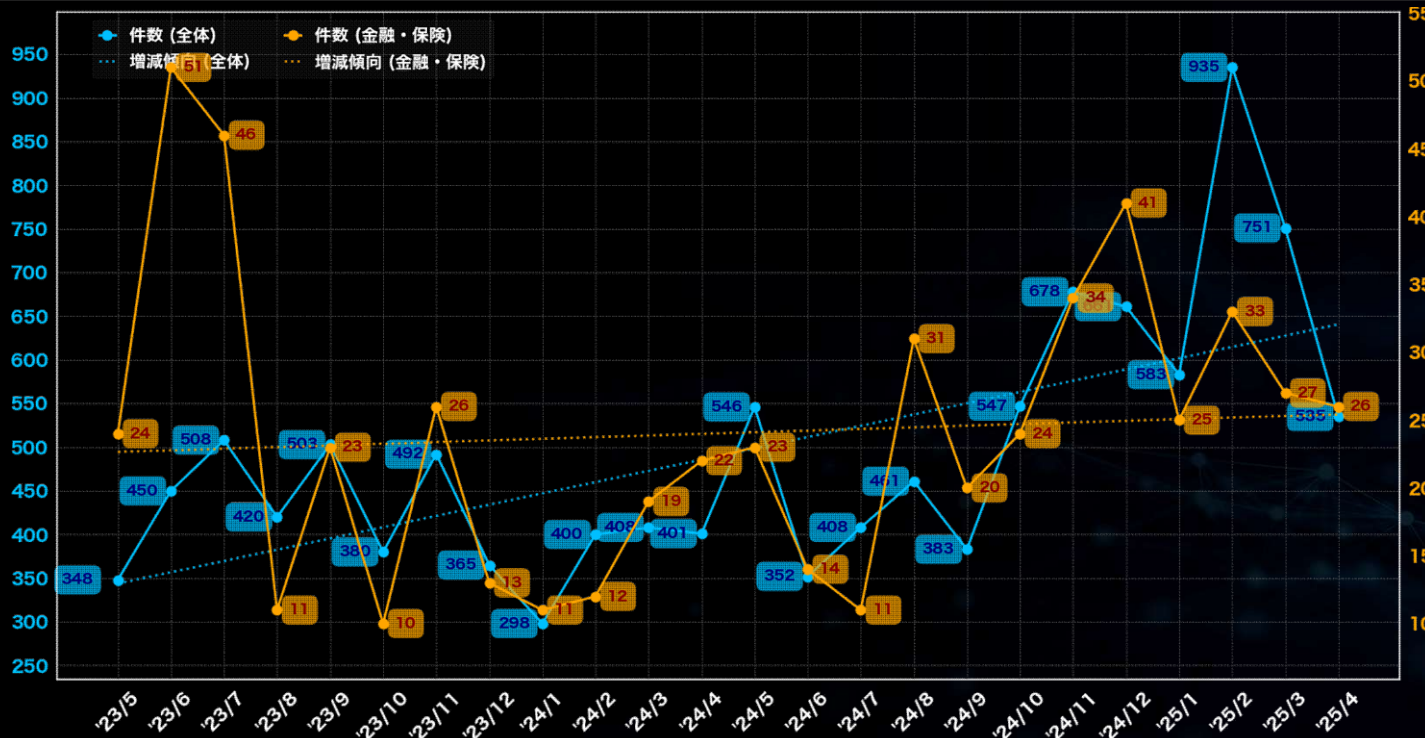
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

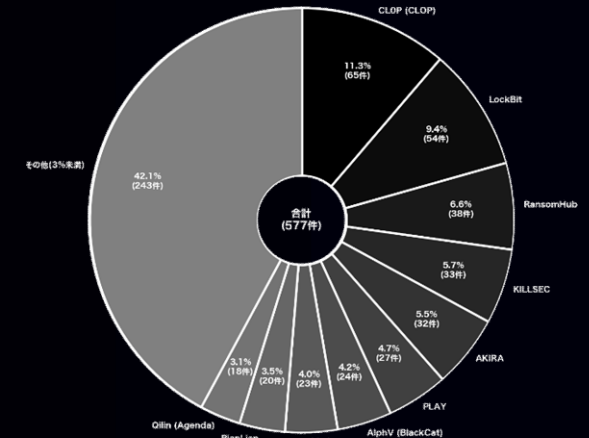
(過去2年間／2023年5月～2025年4月)

金融・保険

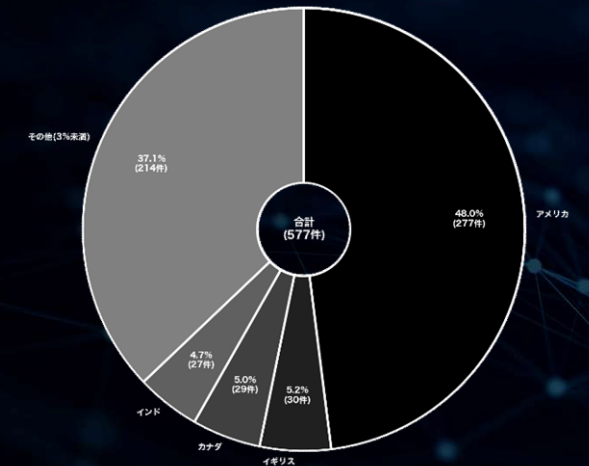
「金融・保険」業界に対するランサムウェア攻撃のリークサイト掲載件数は、最も多かった月が2023年6月で、51件の掲載があった。一方、最も少なかった月は2023年10月で、10件であった。被害組織の所在国の割合では、アメリカが約48%と最も多く、次いでイギリスとカナダがそれぞれ約5%である。攻撃グループについては、少なくとも80のグループが関与しており、特に「CL0P (CLOP)」が65件のリークサイト掲載を実施している。次いで「LockBit」と「RansomHub」がそれぞれ54件と38件の掲載を行っている。金融・保険関連は、他の業種と比較すると全体件数に対する割合が低くほぼ横ばいの推移を見せている。同業界の被害は特にCL0Pによる影響が大きく、全体推移を見てもゼロディ攻撃が目立った2023年の5月から7月にかけて被害数の増加が顕著に見られる。CL0Pはこうのようにゼロディ攻撃を多用する点に加え、そうした状況下において同業界への攻撃傾向が見られる点に、今後とも注意が必要である。



▼攻撃グループ別



▼国別



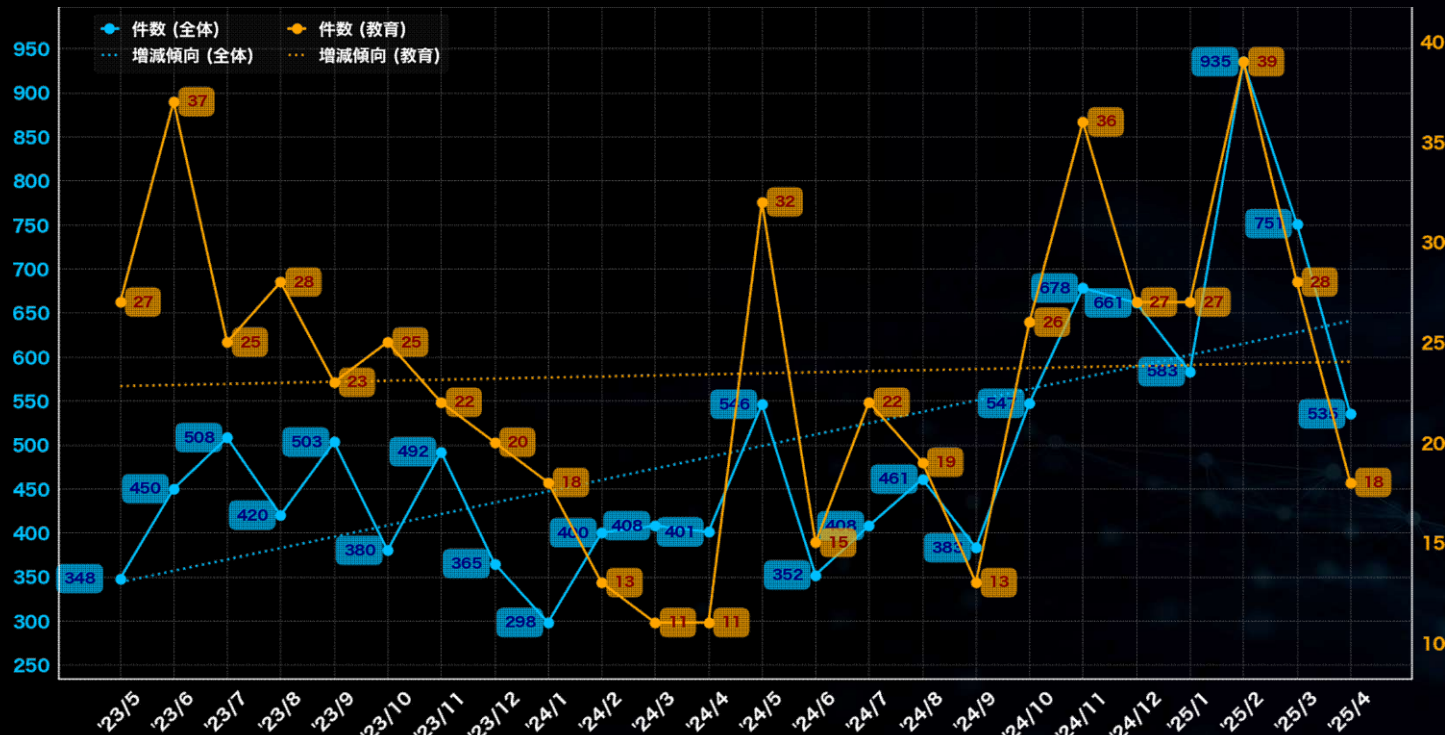
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

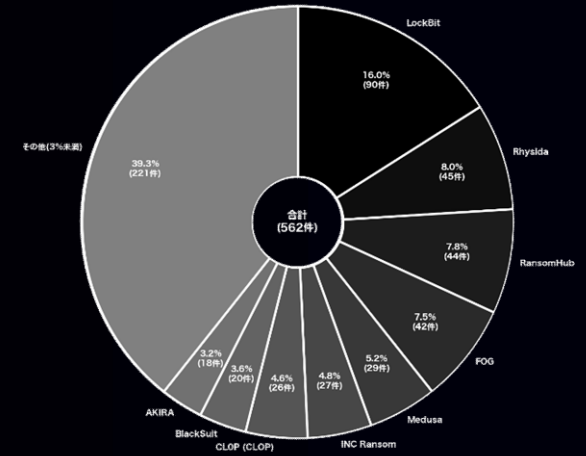
(過去2年間／2023年5月～2025年4月)

教育

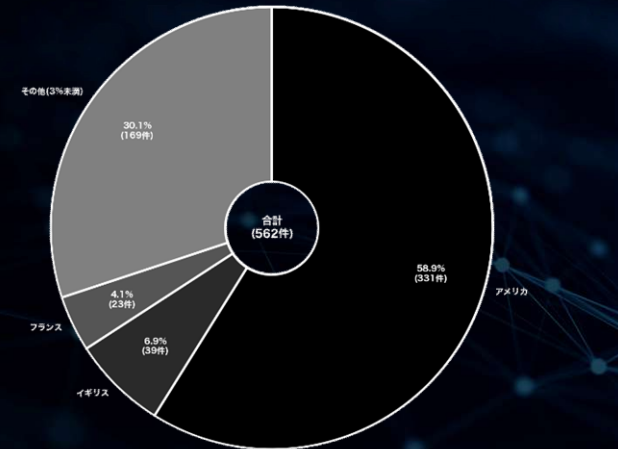
「教育」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、39件の掲載があった。一方、最も少なかった月は2024年3月と4月で、11件であった。被害組織の所在国の割合では、アメリカが約59%と最も多く、次いでイギリスとフランスがそれぞれ約7%と約4%である。攻撃グループについては、少なくとも72のグループが関与しており、特に「LockBit」が90件のリークサイト掲載を実施している。次いで「Rhysida」と「RansomHub」がそれぞれ45件と44件の掲載を行っている。教育業界は、攻撃グループ別で見ると、同業界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



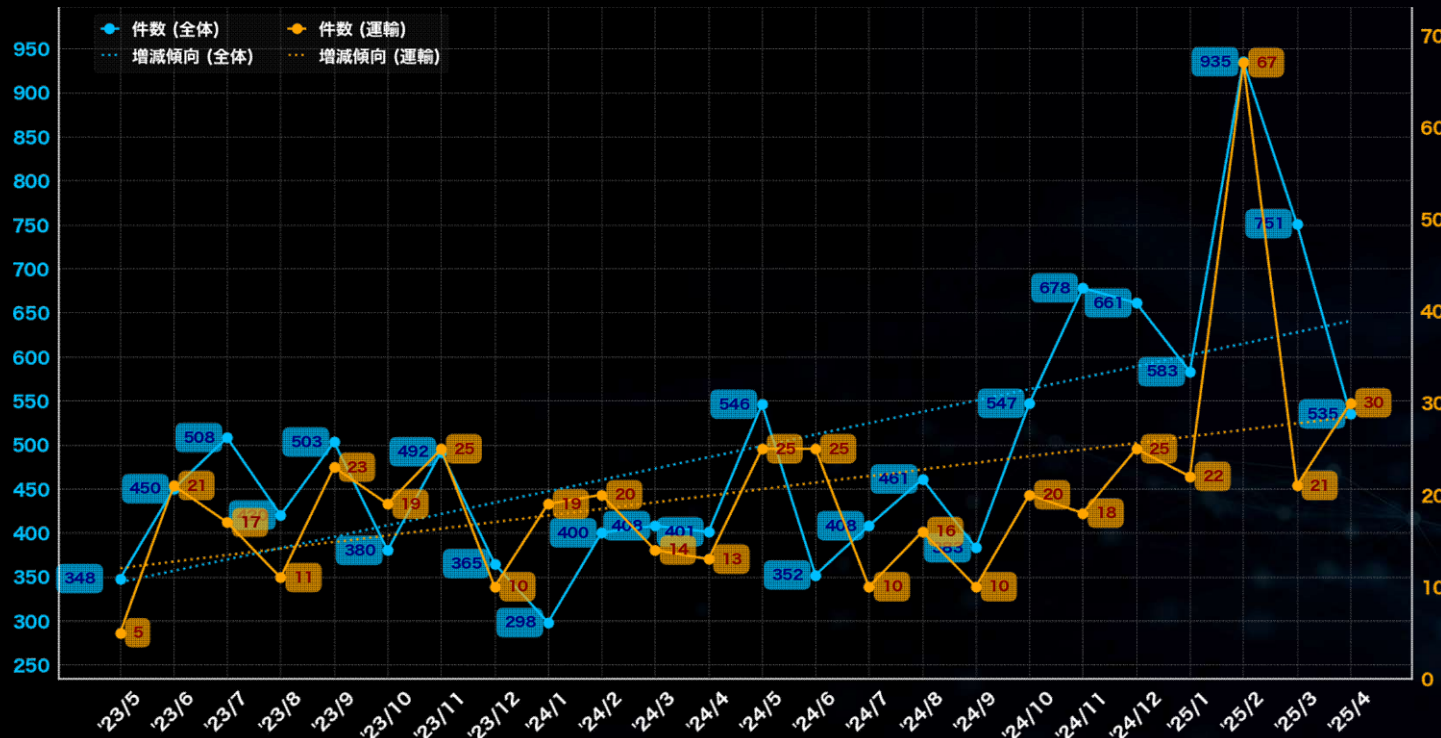
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

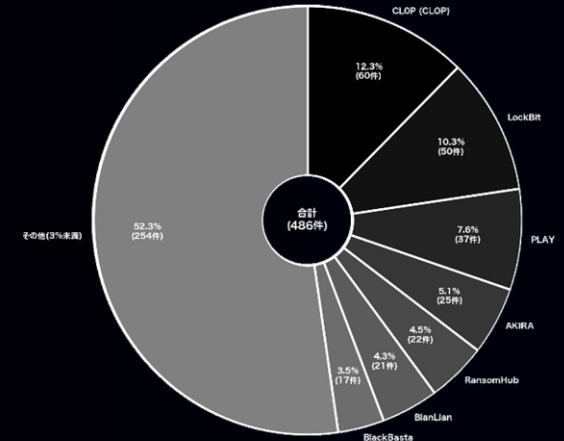
(過去2年間／2023年5月～2025年4月)

運輸

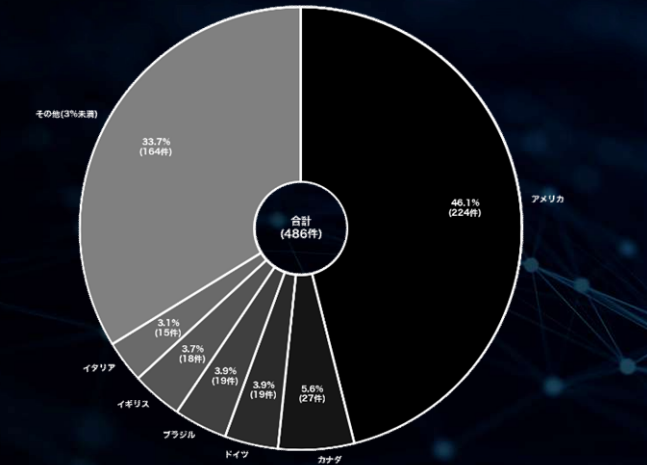
「運輸」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、67件の掲載があった。一方、最も少なかった月は2023年5月で、5件であった。被害組織の所在国の割合では、アメリカが約46%と最も多く、次いでカナダとドイツがそれぞれ約6%と約4%である。攻撃グループについては、少なくとも76のグループが関与しており、特に「CLOP (CLOP)」が60件のリークサイト掲載を実施している。次いで「LockBit」と「PLAY」がそれぞれ50件と37件の掲載を行っている。運輸関係は全体件数に対する割合こそ低く、過去2年間では著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



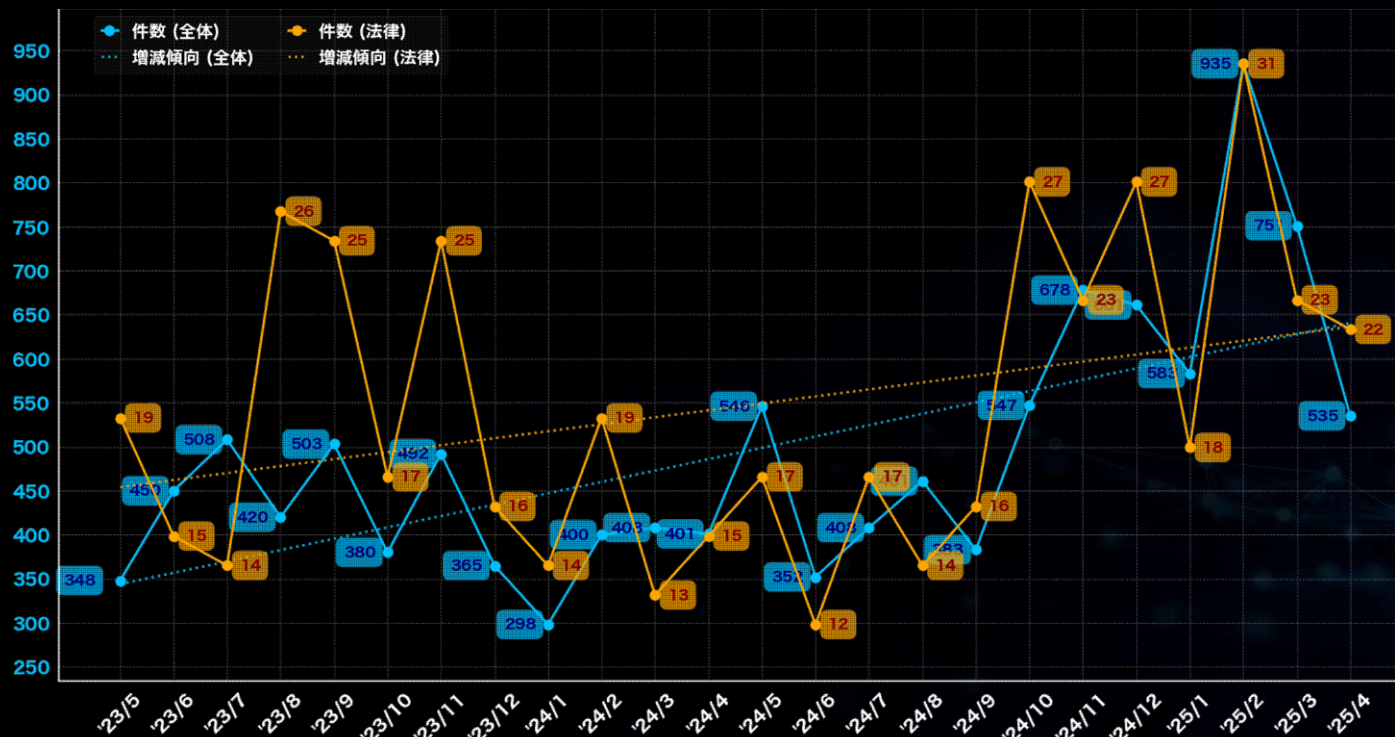
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

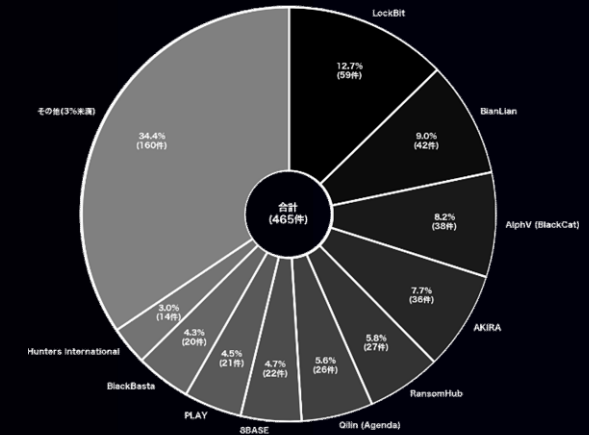
(過去2年間／2023年5月～2025年4月)

法律

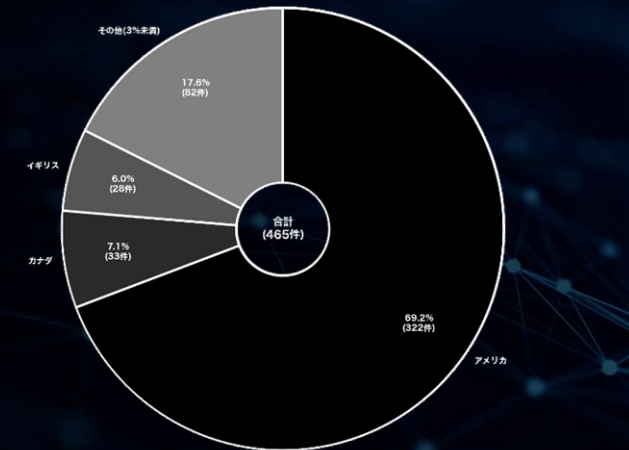
「法律」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、31件の掲載があった。一方、最も少なかった月は2024年6月で、12件であった。被害組織の所在国の割合では、アメリカが約69%と最も多く、次いでカナダとイギリスがそれぞれ約7%と約6%である。攻撃グループについては、少なくとも64のグループが関与しており、特に「LockBit」が59件のリークサイト掲載を実施している。次いで「BianLian」と「AlphV (BlackCat)」がそれぞれ42件と38件の掲載を行っている。法律関連は2023年末以降、減少傾向が見られたが、2023年7月から8月や、2024年9月から10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)

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 :

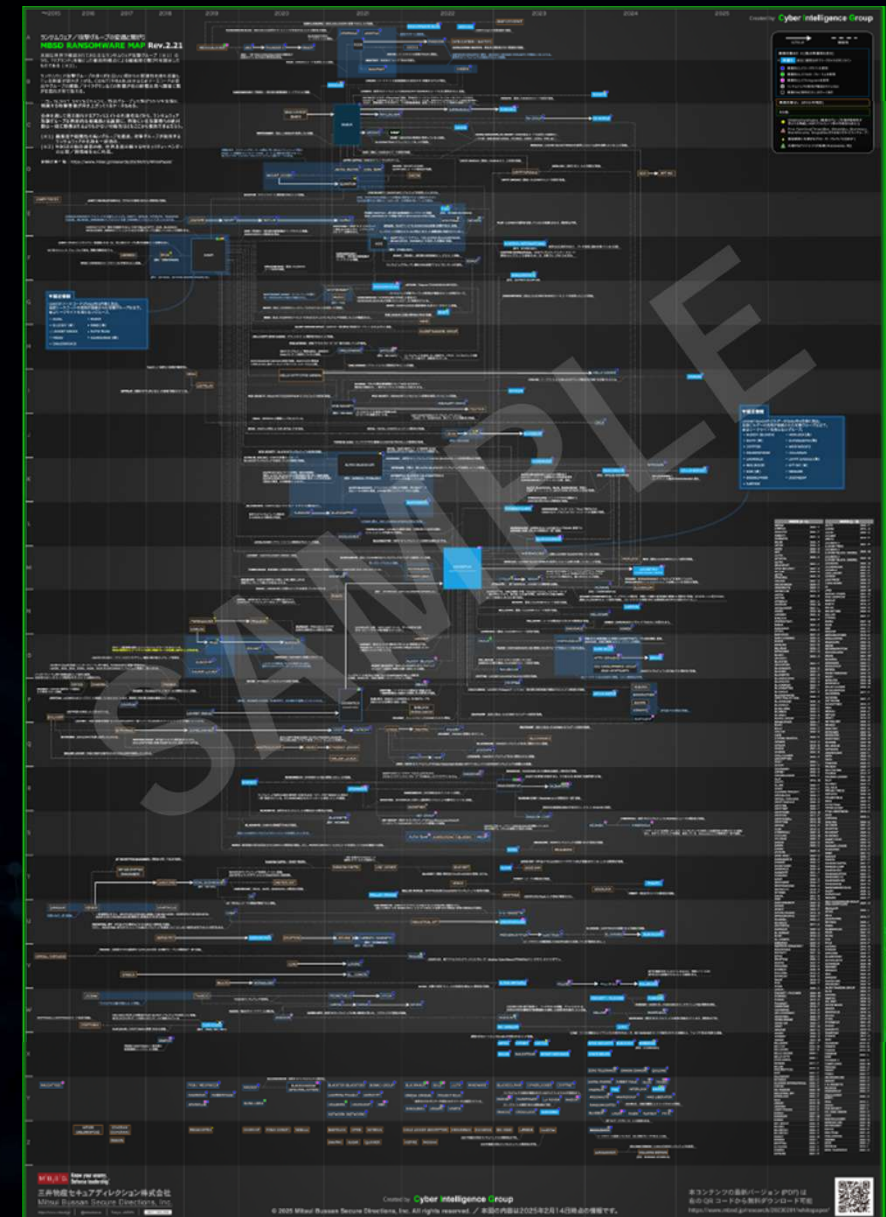
<https://www.mbsd.jp/research/20231023/blog/>

- 技術ブログ :

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

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

MBSD RANSOMWARE MAP (Rev.2)



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