

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9月号 Rev 1.00 (2025年8月分)

2025

8

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⑤～⑯）

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⑰～㉓）

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 月別統計（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㉔～㉗）

資本金別 月別統計（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㉘～㉙）

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㉚）

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 - 教育	p.53
業種に関する分析 - 法律	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

8

今月のハイライト

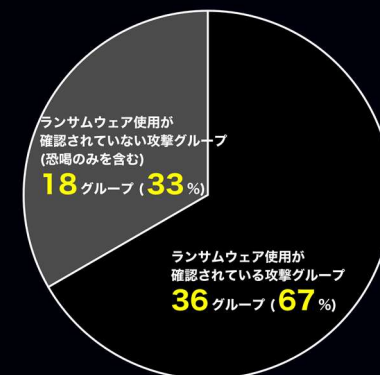
● ランサムウェア攻撃手法の変化

サイバー攻撃の手法に新たな傾向が現れている。ランサムウェア攻撃では、データの暗号化と身代金要求が主流であるが、近年は暗号化を伴わない（ランサムウェアを使用しない）恐喝手法を採用する攻撃グループを複数確認している。

ランサムウェアの使用が認められない攻撃グループの割合は、2025年8月には33%（右図）となり、2024年8月の19%から1年間で約1.7倍に増加している。

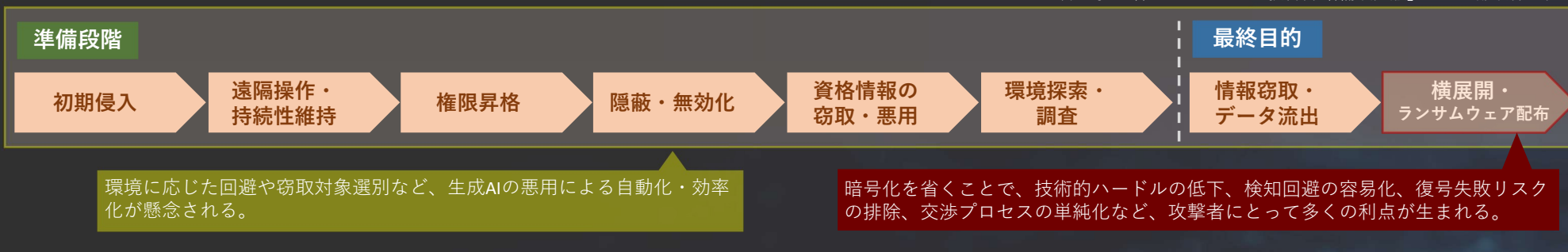
8月に出現した新興グループ「PEAR」は“Pure Extraction And Ransom”を掲げ、暗号化を伴わない恐喝を明確に宣言している。また、CLOP（CLOP）やWorld Leaks（旧Hunters Internationalとされる）といった既存グループも同様の手法を採用している。

暗号化を伴う従来の攻撃では、情報窃取ののちにランサムウェアを配布し、暗号化を行っていた（下図）。一方、データ窃取に特化した手法では、暗号化に関わる工程を省略できる。



ランサムウェア攻撃の段階と今後の懸念 / 目立つ変化

吉川孝志 著「マルウェアの教科書 増補改訂版」より一部抜粋・転用



同様に攻撃過程における効率化や省力化の観点では、生成AIの悪用も今後の懸念事項である。2025年8月には研究者によるPoC段階だが、AI駆動型ランサムウェア「PromptLock」※1が確認され、生成AIの攻撃転用が現実的な脅威となりつつある。実際にClaude Codeを悪用したランサムウェア攻撃も報告されている※2。Anthropicによると、攻撃者は窃取データの分析や脅迫文の生成などに利用していた。

我々の調査「Behind Black Basta」※3でも、Black Bastaが生成AIやディープフェイク技術をいち早く採用していたことを確認。攻撃者は常に最新技術を取り入れており、防御側も技術進化への迅速な対応と追従が求められる。

※1: <https://www.eset.com/jp/about/newsroom/press-releases/2025/eset-discovers-promptlock-the-first-ai-powered-ransomware-jp/>

※2: <https://www-cdn.anthropic.com/b2a76c6f6992465c09a6f2fce282f6c0cea8c200.pdf>

※3: <https://www.mbsd.jp/report/>

ランサムウェア関連記事 | 今月のピックアップ

【2025年度 夏休みにおける情報セキュリティに関する注意喚起】（独立行政法人 情報処理推進機構(IPA)：2025/08/01)

夏休み期間中に管理者不在などでインシデント対応が遅れ被害が拡大するリスクを踏まえ、情報セキュリティ対策の徹底をIPAが注意喚起。

<https://www.ipa.go.jp/security/anshin/heads-up/alert20250801.html>

【1,000 万円以上 5,000 万円未満が最多 ～ ランサムウェア感染被害金額】（ScanNetSecurity：2025/08/06）

JNSA調査によると、2024年までの国内のサイバー攻撃被害は中小企業が最多。ランサムウェア被害額の増加傾向も確認された。

<https://scan.netsecurity.ne.jp/article/2025/08/06/53378.html>

【SSL-VPN機能が有効化されたSonicWall製ファイアウォールGen 7以降を標的とする脅威活動について】（JPCERT/CC：2025/08/07）

SonicWall Gen 7以降のSSL-VPN機能を狙う攻撃が確認され、脆弱性悪用による国内被害拡大が懸念されている。攻撃グループ「AKIRA」も悪用の可能性。

<https://www.jpccert.or.jp/newsflash/2025080701.html>

【8つのランサムウェアグループが新しいEDR無効化ツールを使用】（BleepingComputer：2025/08/07）

8つのランサムウェアグループが新たなEDR無効化ツールを使用。正規ファイルを装い、主要なセキュリティ製品を停止し攻撃成功率を高めていることが確認された。

<https://www.bleepingcomputer.com/news/security/new-edr-killer-tool-used-by-eight-different-ransomware-groups/>

【米司法省がBlackSuit（Royal）ランサムウェアへの大規模な摘発を発表】（United States Department of Justice：2025/08/11）

米司法省はBlackSuit（Royal）ランサムウェアグループのインフラ摘発を発表し、複数のサーバやドメイン及び約109万ドル相当の仮想通貨を押収。

<https://www.justice.gov/opa/pr/justice-department-announces-coordinated-disruption-actions-against-blacksuit-royal>

【米司法省、280万ドル超の仮想通貨と現金などを押収】（United States Department of Justice：2025/08/14）

米司法省は、ランサムウェア「Zeppelin」に関与した個人から仮想通貨約280万ドルと現金、車両などを押収したと発表。

<https://www.justice.gov/opa/pr/justice-department-announces-seizure-over-28-million-cryptocurrency-cash-and-other-assets>

【Europol、Qilinランサムウェアの5万ドル懸賞金は偽物と確認】（BleepingComputer：2025/08/21）

Europolは、Qilinランサムウェアの管理者2名に関する情報提供に5万ドルの報奨金を提供すると主張したTelegramチャンネルが偽物であることを確認した。

<https://www.bleepingcomputer.com/news/security/europol-confirms-that-qilin-ransomware-reward-is-fake/>

【AIの不正利用の検知と対策（2025年8月）】（Anthropic：2025/08/28）

Anthropicは、AIがランサムウェア攻撃への悪用を含め、恐喝・偽装就労・マルウェア作成といったサイバー犯罪の自動化・高度化に使われている実態を報告。

<https://www.anthropic.com/news/detecting-counteracting-misuse-aug-2025>

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) : 261^(※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 : 54

● 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)	BOTLOCK	DEVMAN	Hunters International	Mindware	Ragnar Locker	Silent
8BASE	Brain Cipher	DEVMAN 2.0	ICEFIRE	Mogilevich [fraud]	Ragnarok	Sinobi
Abyss	BULLY	Dire Wolf	IMN Crew	MOISHA	RA GROUP	SKIRA TEAM
AKIRA	Business Data Leaks	Dispossessor[Databroker]	INC Ransom	Money Message	RALord	SLUG
AKO	CACTUS	Donex	Insane	Monti	Rancoz	Snatch
Alpha (MYDATA)	● Cephalus	Donut Leaks	INTERLOCK	Morpheus	RansomBay	Solidbit
AlphV (BlackCat)	CHAOS (2025)	DoppelPaymer	J GROUP	Mount Locker	Ransom Cartel	Space Bears
Anubis	CHEERS	dotAdmin	KAIROS	N3tw0rm (NetWorm)	Ransom Corp	Sparta
Apos Security	ChileLocker (Arcrypter)	DragonForce	Karakurt	N4UGHTYSEC (NAUGHTYSEC)	RANSOMCORTX	Spook
APT73 (Eraleig)	CHORT	DragonRansomware	Karma	Nefilim	Ransomed.vc	STORMOUS
ARCUS MEDIA	Cicada3301	DUNGHILL	Kawa4096	Nevada	Ransom EXX	Sugar
Argonauts	CiphBit	eCh0raix (eChoraix)	KILLSEC	NightSky	RansomHouse	Suncrypt
Arkana	CipherLocker	EL Cometa	Knight	NightSpire	RansomHub	SynACK
ArvinClub	CLOP (CLOP)	EL DORADO	Kraken (HelloKitty)	NITROGEN	Ransomware Blog	TeamXXX
Astro (Astra)	Cloak	EMBARGO	LAMBDA	NoEscape	Ranzy	Termite
AtomSilo	Conti	Endurance	La Piovra	Nokoyawa	RA WORLD	ThreeAM (3AM)
Avaddon	Cooming Project	Entropy	LAPSUS\$	NONAME (VF0KX)	Raznatovic	TRIGONA
AvosLocker	Crazy Hunter Team	Everest	LeakedData (Silent Ransom Group)	NONAME [2023年確認]	RedAlert (N13V)	TRINITY
Axxes	CROSSLOCK	FOG	● LEAKNET	Nova	Red Ransomware Group (Red CryptoApp)	TRISEC
AzzaSec	CryptBB	Frag	LILITH	NULLBULGE	Relic	Underground
Babuk	CRYPTNET	FSOCIETY / FLOCKER	Linkc	Onyx	Revil (Sodinokibi)	UnSafe
Babuk (2025)	CRYPTO24	FSTeam	LockBit	Orca	Rhysida	Valencia
BASHE	CryptOn	Funksec	Lorenz	Pandora	Risen	VanHelsing
BEAST	Cuba	GD LockerSec	LostTrust	Pay2Key	ROOK	VanirGroup
BERT	Cyclops	GLOBAL	LV	Payload.bin	Royal	Vice Society
BianLian	D4RK4RMY	Grief	LYNX	Payouts King	Rransom	V IS VENDETTA
BL00DY (BLOODY)	DAGON	Groove	MADCAT	● PEAR	RunSomeWares	VSOP
Bl4ckt0r (BlackTor)	DAIXIN	Gunra	MAD LIBERATOR	PLAY	Sabbath (54bb47h)	WALocker
Black Basta	dAn0n (danon)	HANDARA [Hacktivist]	MALAS	PLAYBOY	SAFEPAY	Warlock
BlackByte	Dark Angels	Haron	MalekTeam	Prometheus	SARCOMA	WEREWOLVES
BlackDolphin	DARKBIT	HELLCAT	Mallox	PRYX	SATAN LOCK	Weythro
BlackLock	DARKPOWER	Helldown	Mamona RIP	PUTIN TEAM	SATANLOCK V2	WORLD LEAKS
BlackMatter	DarkRace	HelloGookie	MBC	Pysa / Mespinoza	Secp0	x001xs
● Black Nevas	DarkRypt	Hitler (AGL0BGVYCG)	Medusa	Qilin (Agenda)	Securotrop	XING Team
Blackout	Darkside	Hive	MEOW	QIULONG	SenSayQ	Yanluowang
BlackSuit	Dark Vault	HolyGhost	Metaencryptor	Quantum	shaoleaks	Zeon
BLUEBOX	DataCarry	Hotarus	Midax	RABBIT HOLE	SIEGEDSEC	Zero Tolerance
BLUESKY	● Desolator					

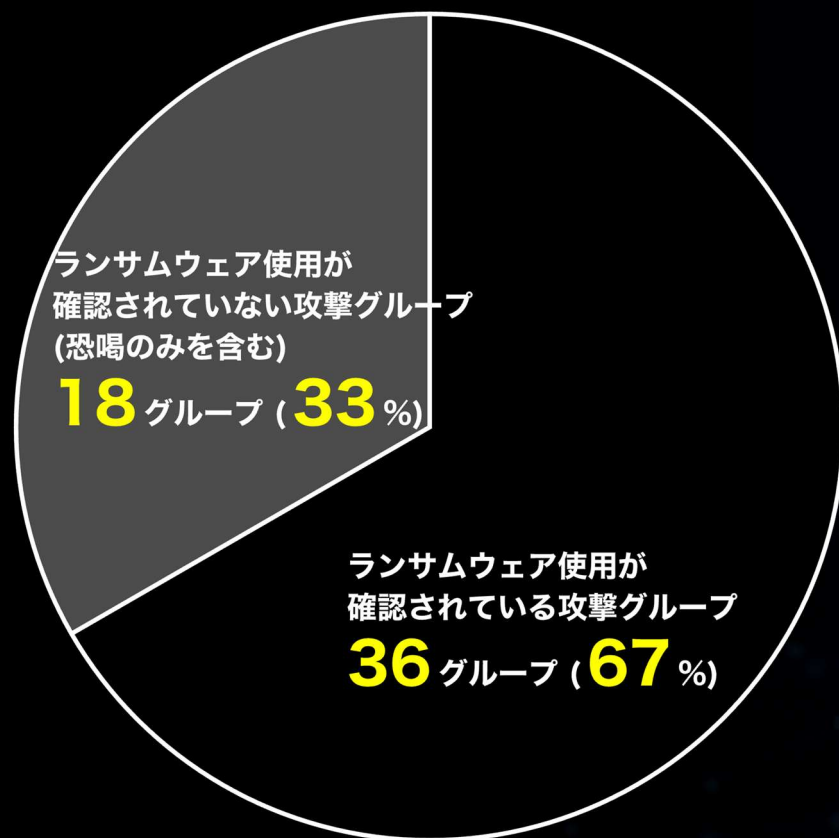
※1) レポート公開月に出現した攻撃グループは次月号に反映

※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 **8**月)

(※当月にリークサイト掲載を確認した攻撃グループ全**54**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8月に活動中である事が確認された全54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

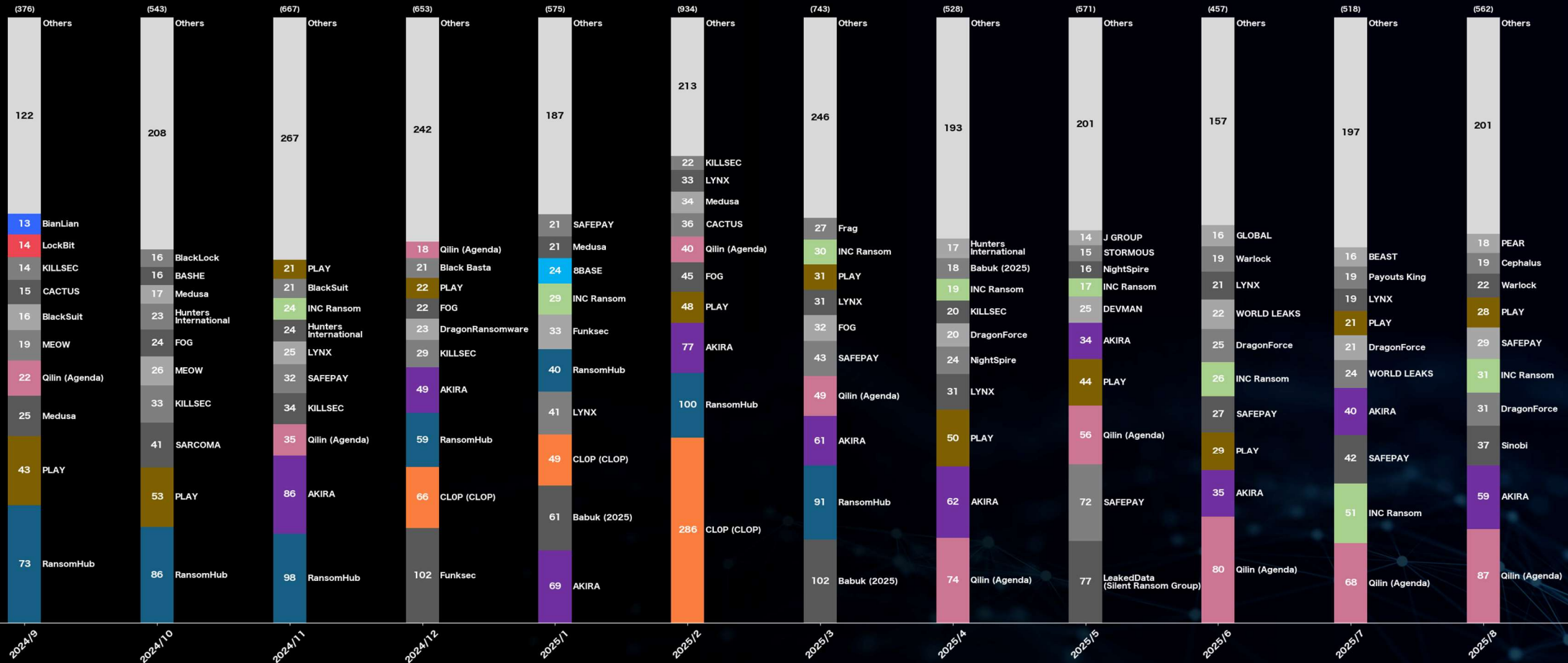
(全世界)

2025

8

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9月～2025年8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

8

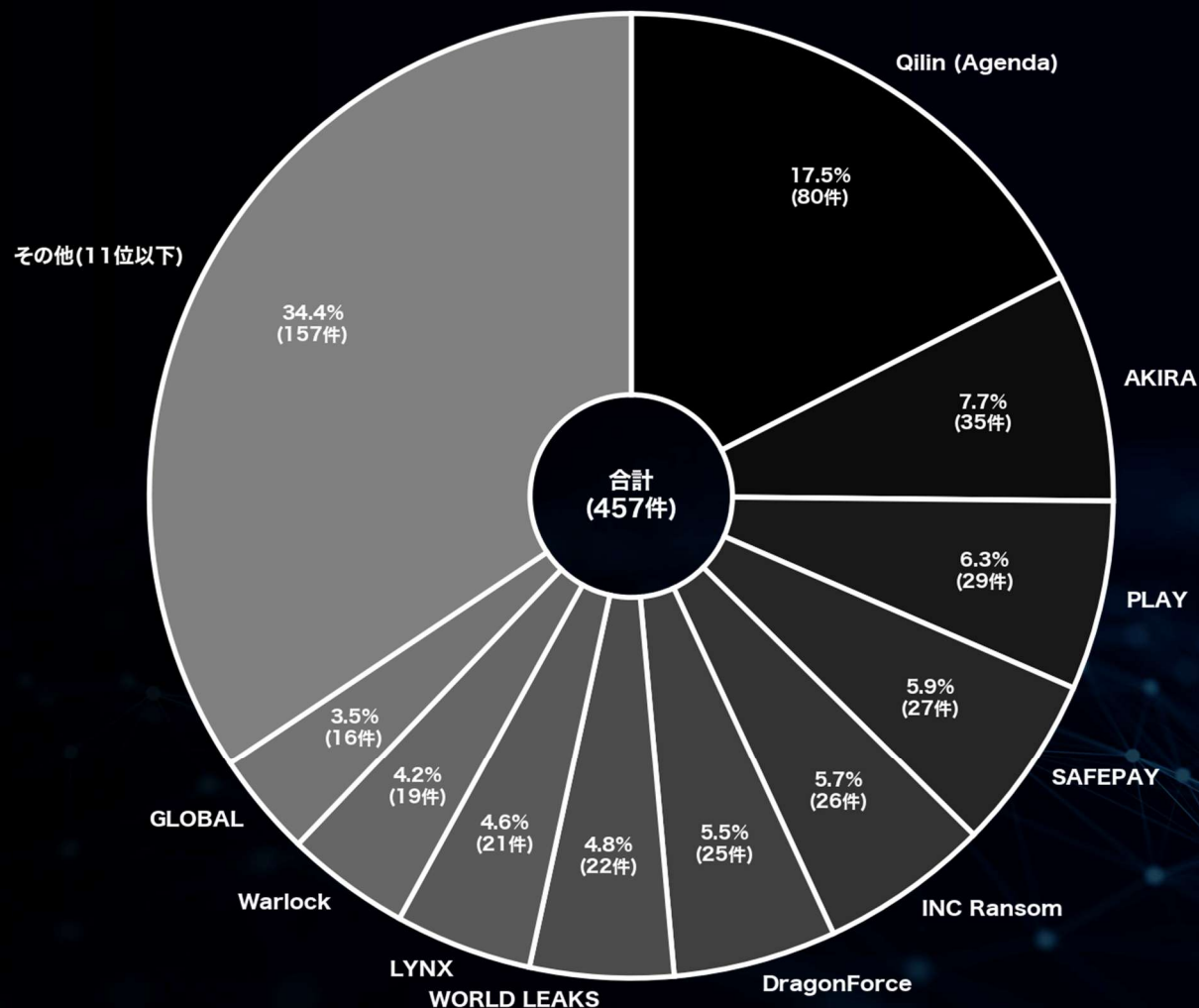
月別内訳 攻撃グループ TOP10 (全世界)

(2025年 6 月)

※件数順に降順／同件数のものが含まれる場合は名前順でTOP10までを記載

攻撃グループ名	件数	割合(%)	前月比(件数)
Qilin (Agenda)	80	17.5	+ 24
AKIRA	35	7.7	+ 1
PLAY	29	6.3	- 15
SAFEPAY	27	5.9	- 45
INC Ransom	26	5.7	+ 9
DragonForce	25	5.5	+ 23
WORLD LEAKS	22	4.8	+ 13
LYNX	21	4.6	+ 10
Warlock	19	4.2	+ 19
GLOBAL	16	3.5	+ 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)



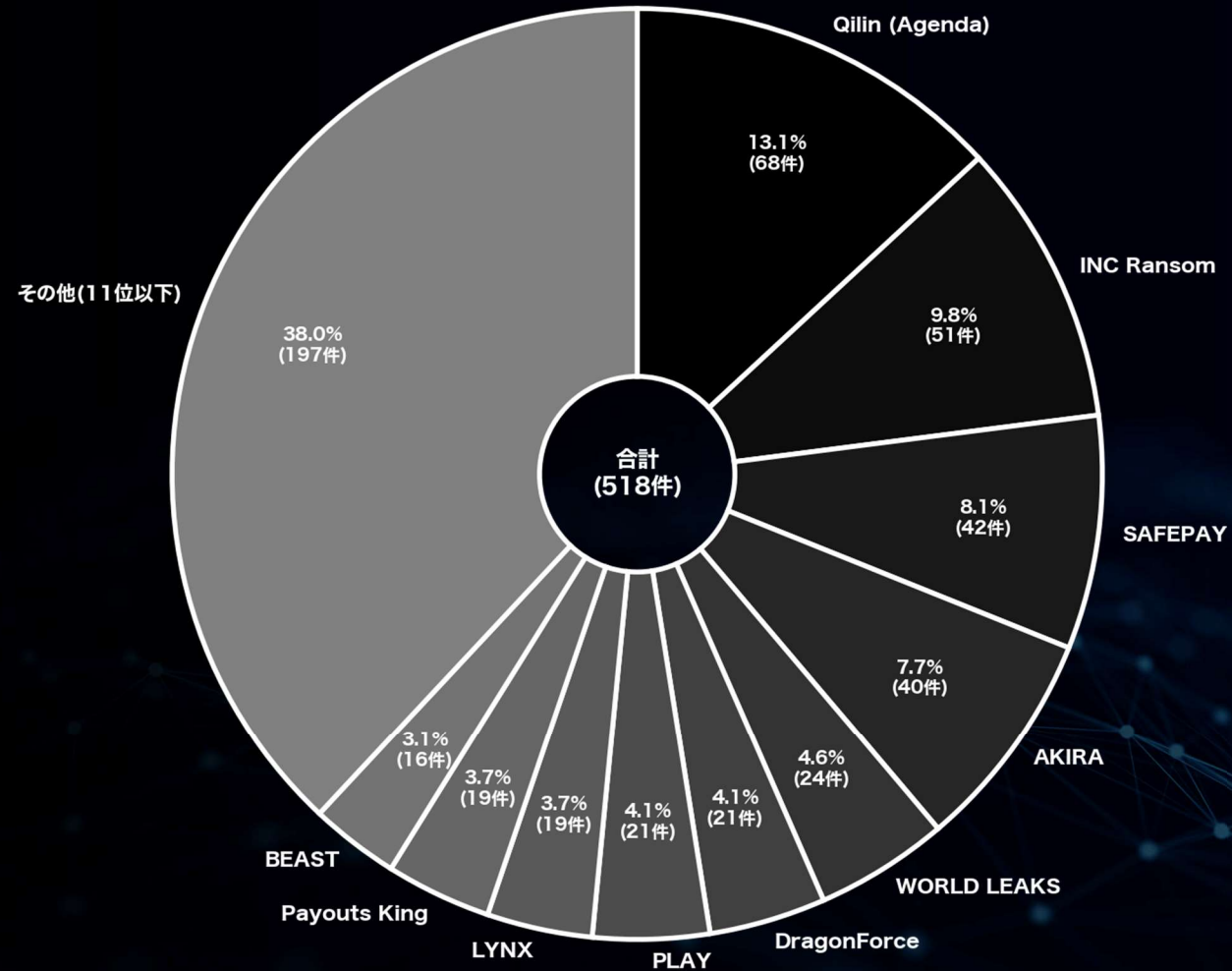
月別内訳 攻撃グループ TOP10 (全世界)

(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)



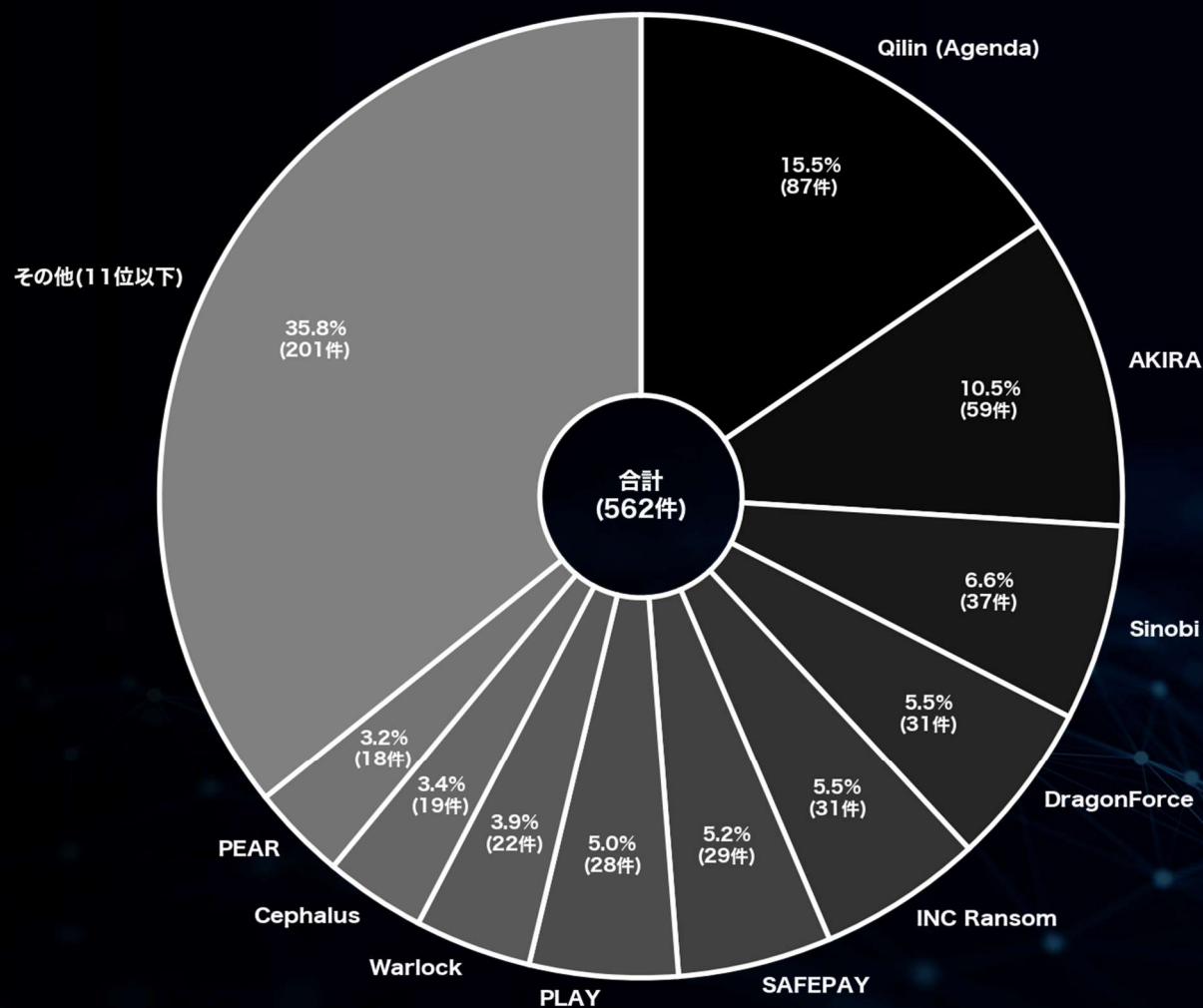
月別内訳 攻撃グループ TOP10 (全世界)

(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)



被害国 月別統計

(全世界) (過去3ヶ月分)

2025

8

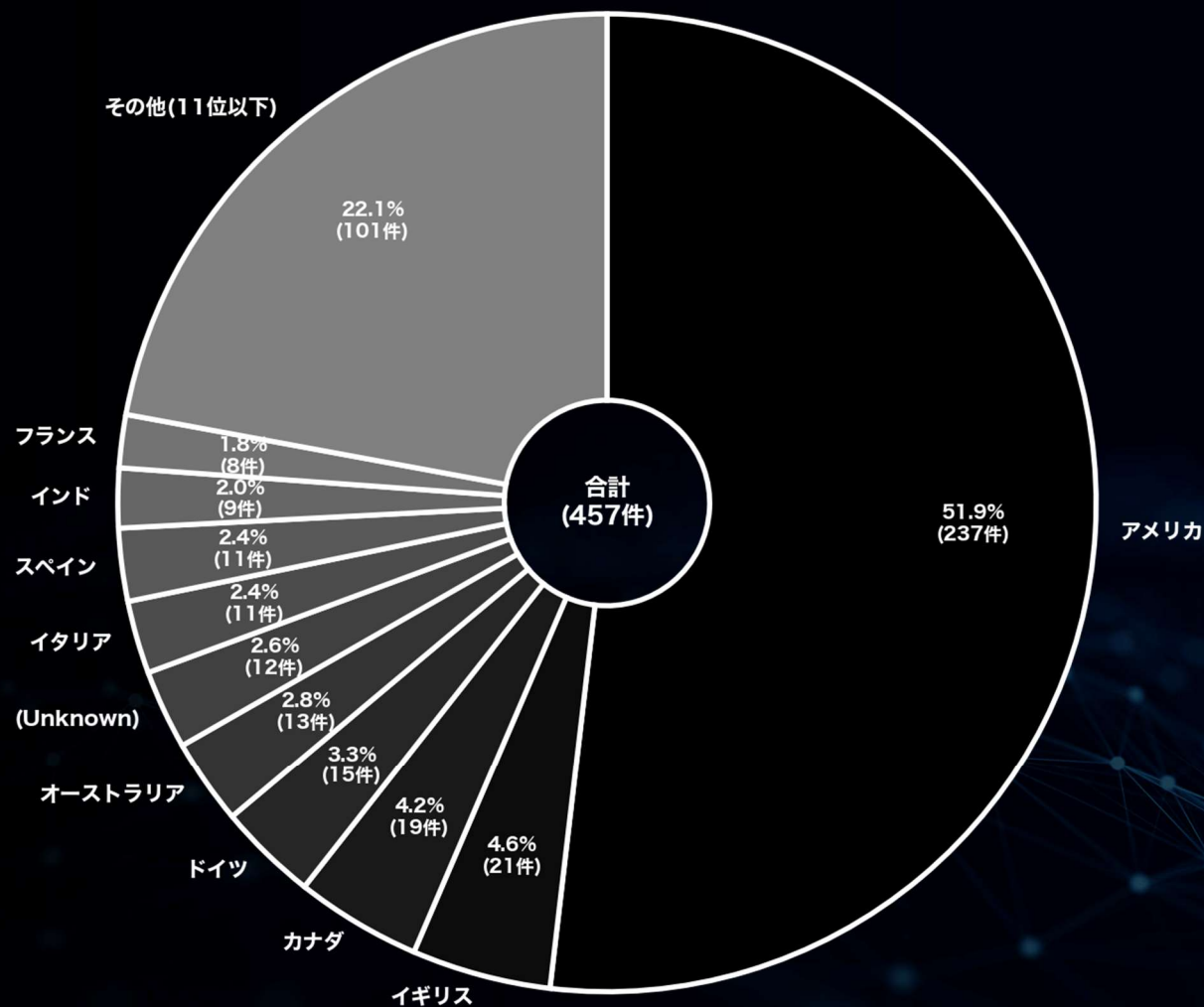
月別内訳 被害国TOP10 (全世界)

(2025年 6 月)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
アメリカ	237	51.9	- 56
イギリス	21	4.6	+ 5
カナダ	19	4.2	- 10
ドイツ	15	3.3	- 17
オーストラリア	13	2.8	+ 7
(Unknown)	12	2.6	+ 1
イタリア	11	2.4	+ 1
スペイン	11	2.4	- 8
インド	9	2.0	+ 6
フランス	8	1.8	± 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)



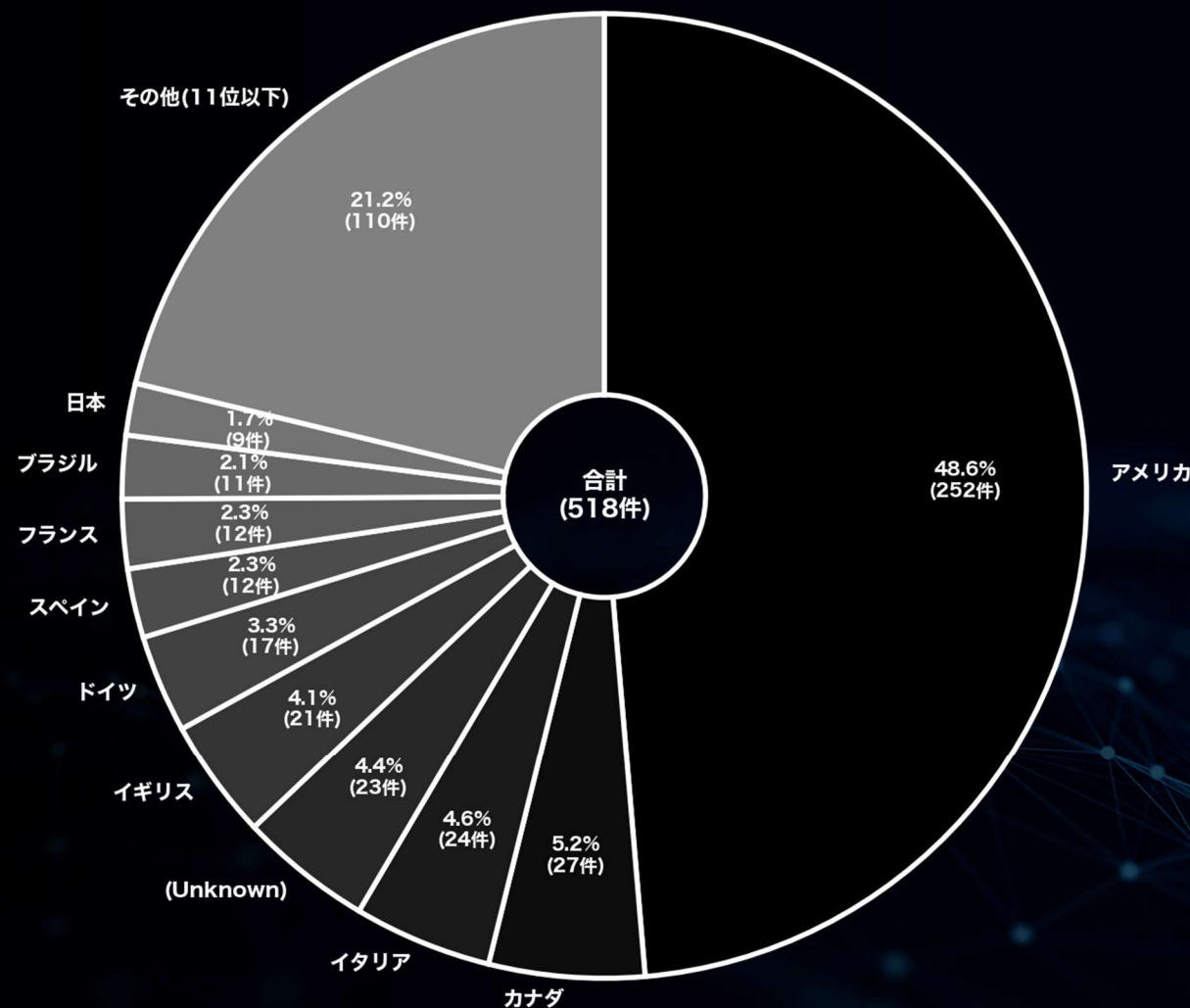
月別内訳 被害国TOP10 (全世界)

(2025年 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)



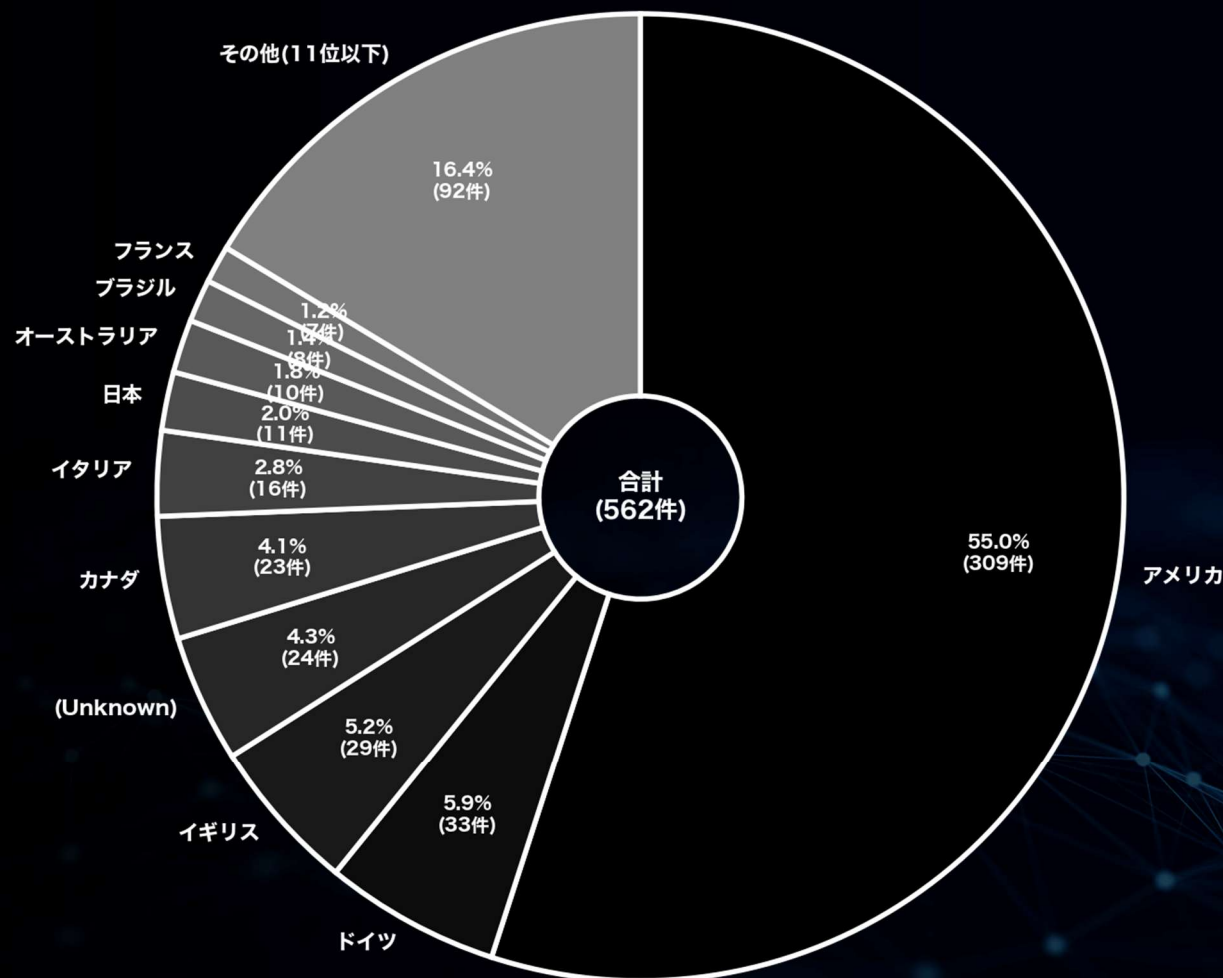
月別内訳 被害国TOP10 (全世界)

(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)



被害国 月別統計

(アジア) (過去3ヶ月分)

2025

8

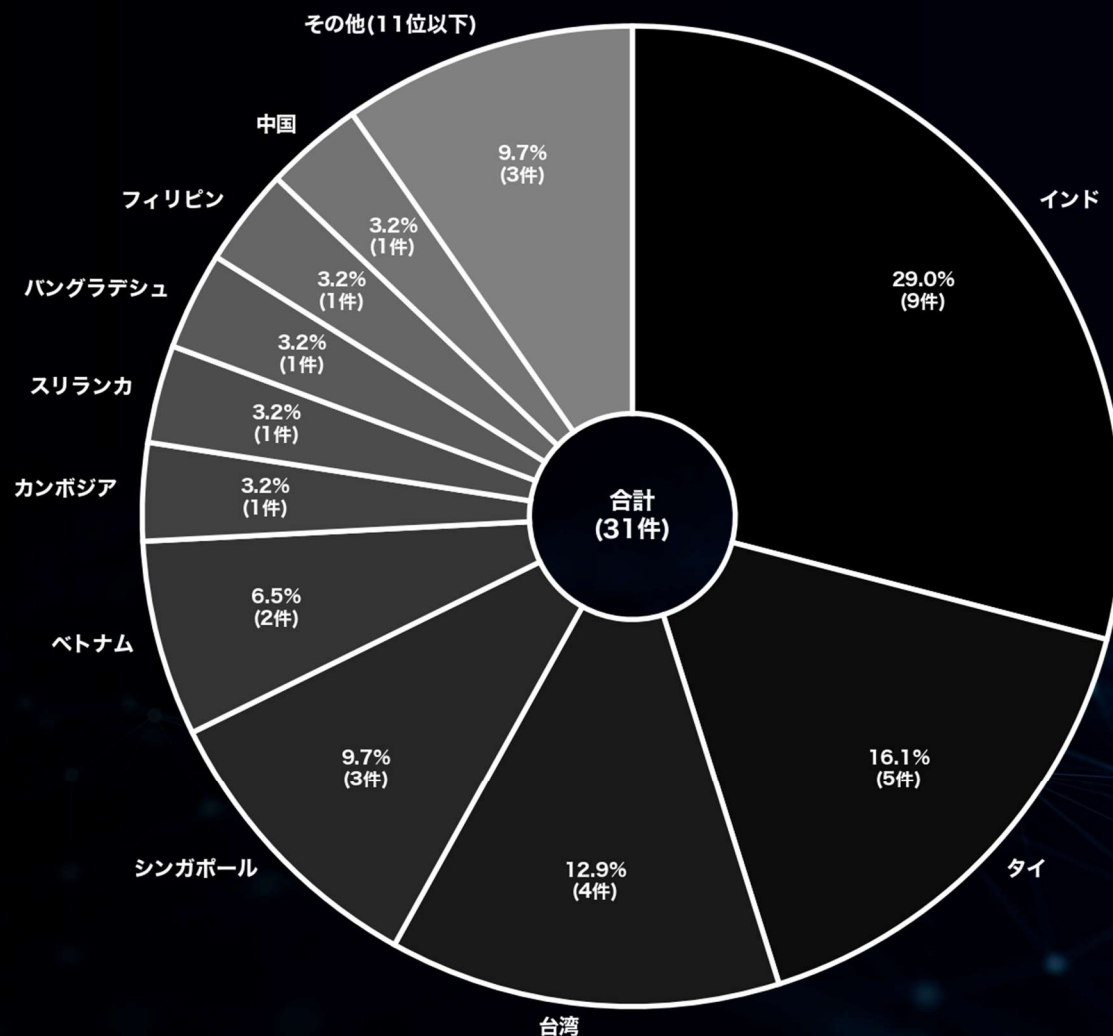
月別内訳 被害国TOP10 (アジア)

(2025年 6 月)

※件数順に降順/同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
インド	9	29.0	+ 6
タイ	5	16.1	+ 1
台湾	4	12.9	+ 1
シンガポール	3	9.7	- 7
ベトナム	2	6.5	± 0
カンボジア	1	3.2	+ 1
スリランカ	1	3.2	± 0
バングラデシュ	1	3.2	+ 1
フィリピン	1	3.2	- 3
中国	1	3.2	- 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)



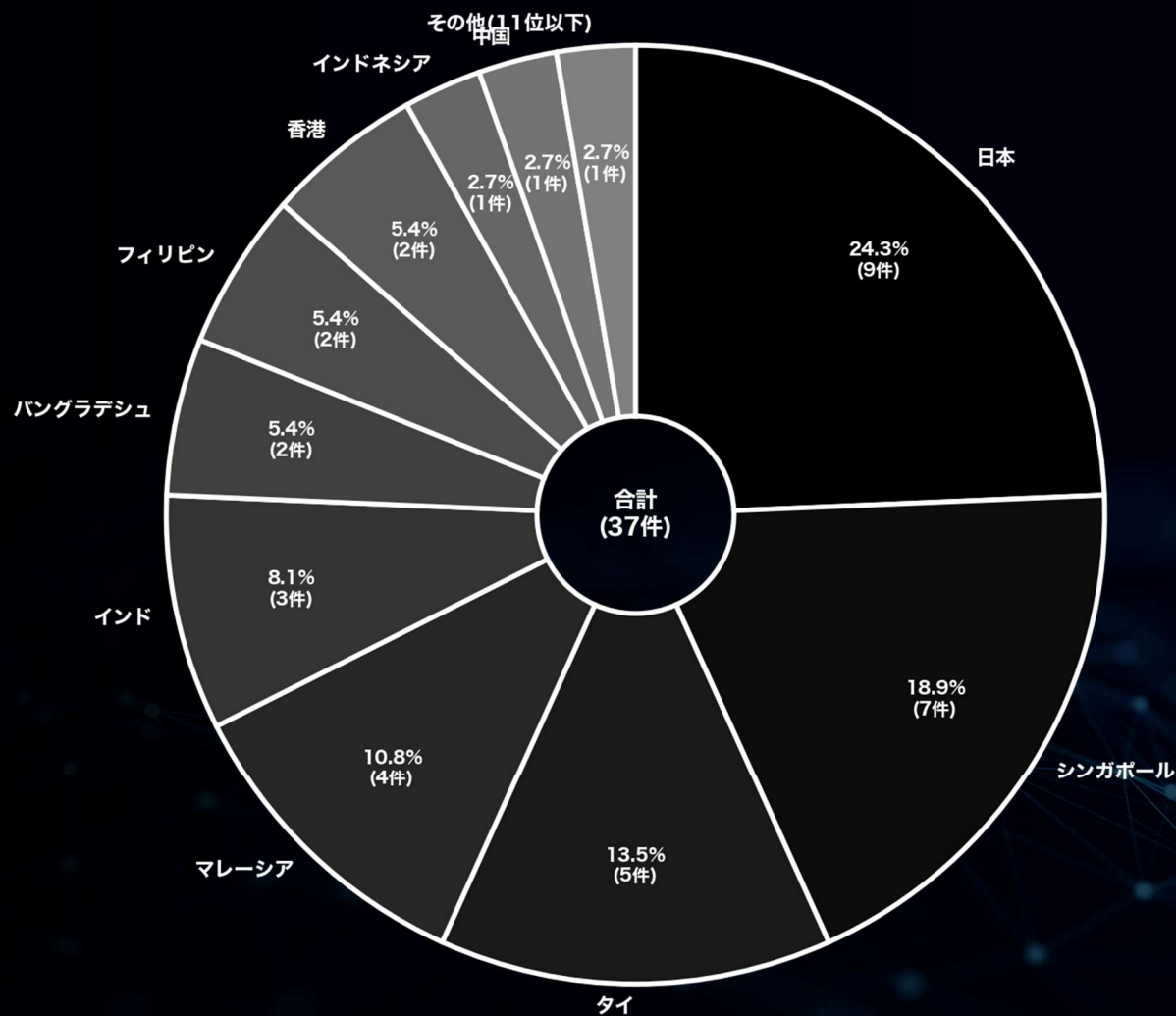
月別内訳 被害国TOP10 (アジア)

(2025年 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)



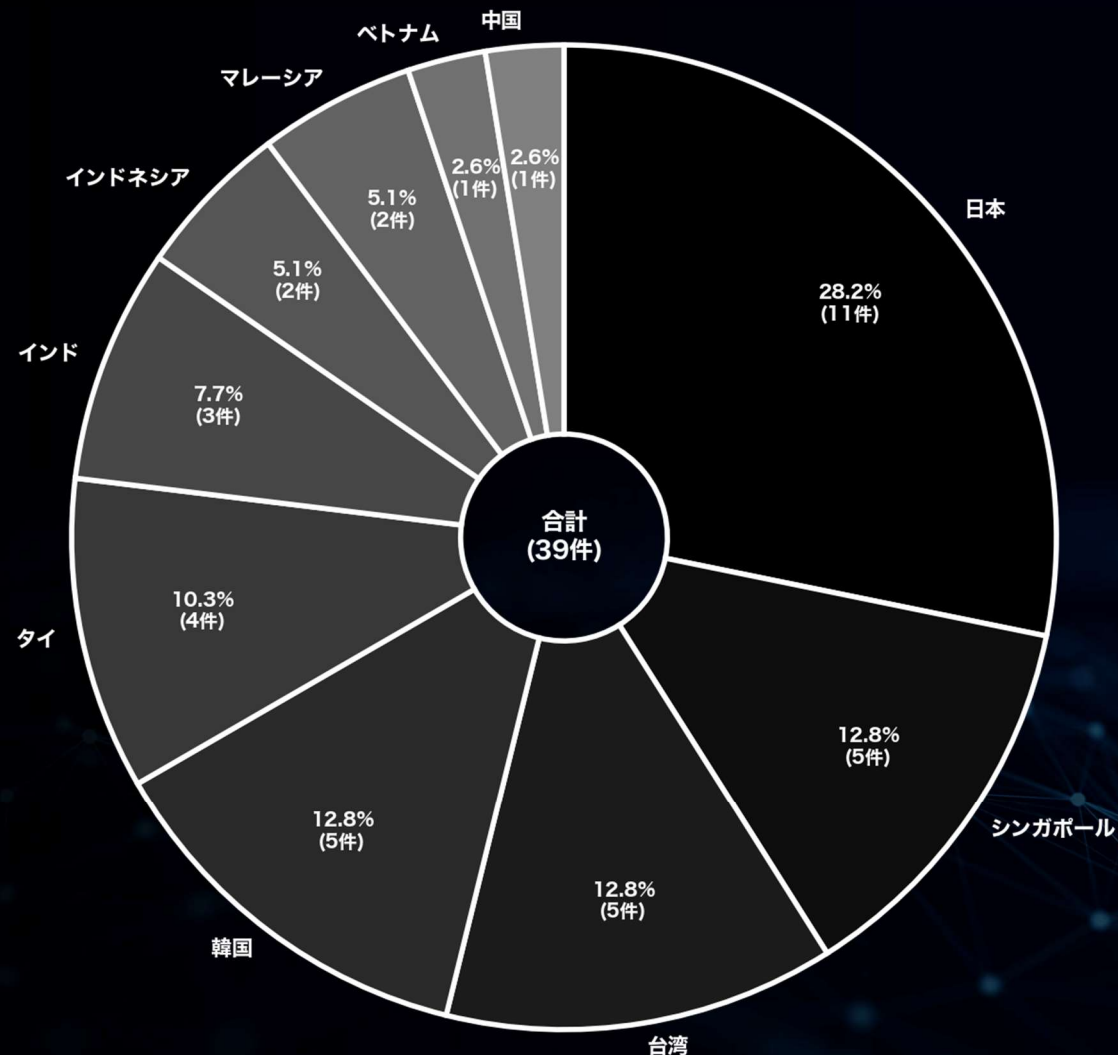
月別内訳 被害国TOP10 (アジア)

(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)



業種 月別統計

(全世界) (過去3ヶ月分)

2025

8

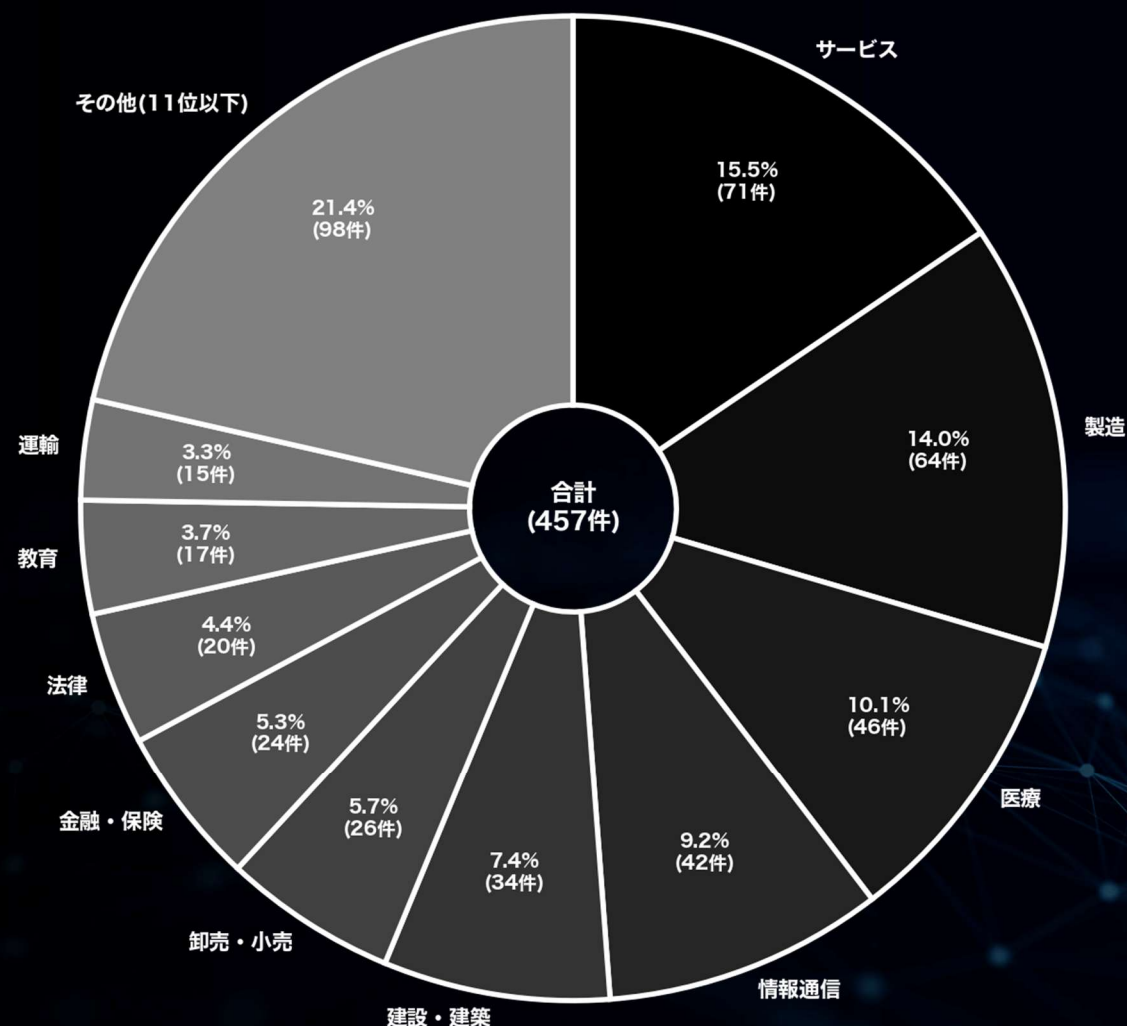
月別内訳 業種 TOP10 (全世界)

(2025年 6 月)

※件数順に降順／同件数のものが含まれる場合は名前順でTOP10までを記載

業種	件数	割合(%)	前月比(件数)
サービス	71	15.5	+ 18
製造	64	14.0	- 28
医療	46	10.1	+ 14
情報通信	42	9.2	- 4
建設・建築	34	7.4	- 20
卸売・小売	26	5.7	- 1
金融・保険	24	5.3	- 28
法律	20	4.4	- 38
教育	17	3.7	- 4
運輸	15	3.3	- 5

▼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)



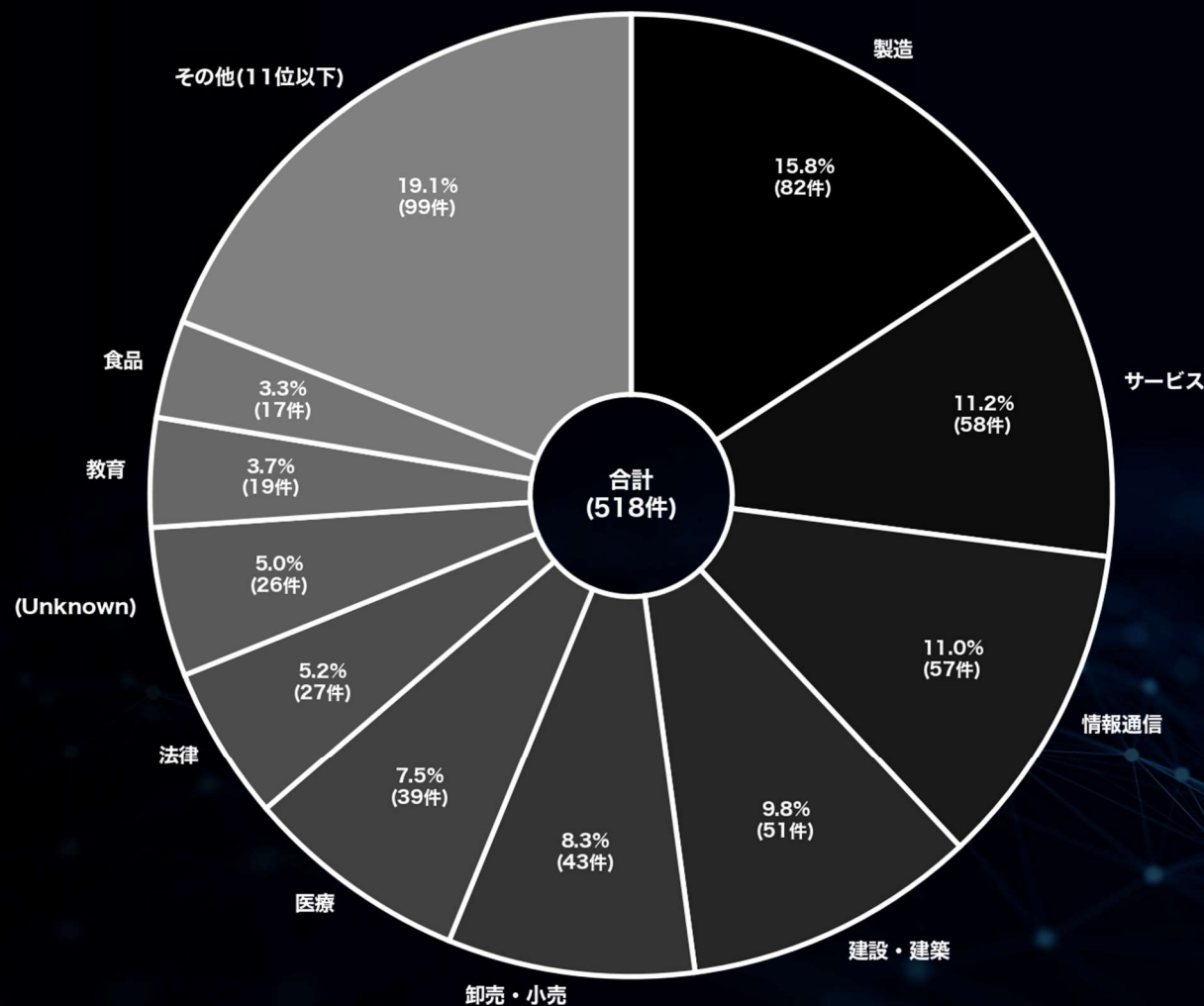
月別内訳 業種 TOP10 (全世界)

(2025年 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)



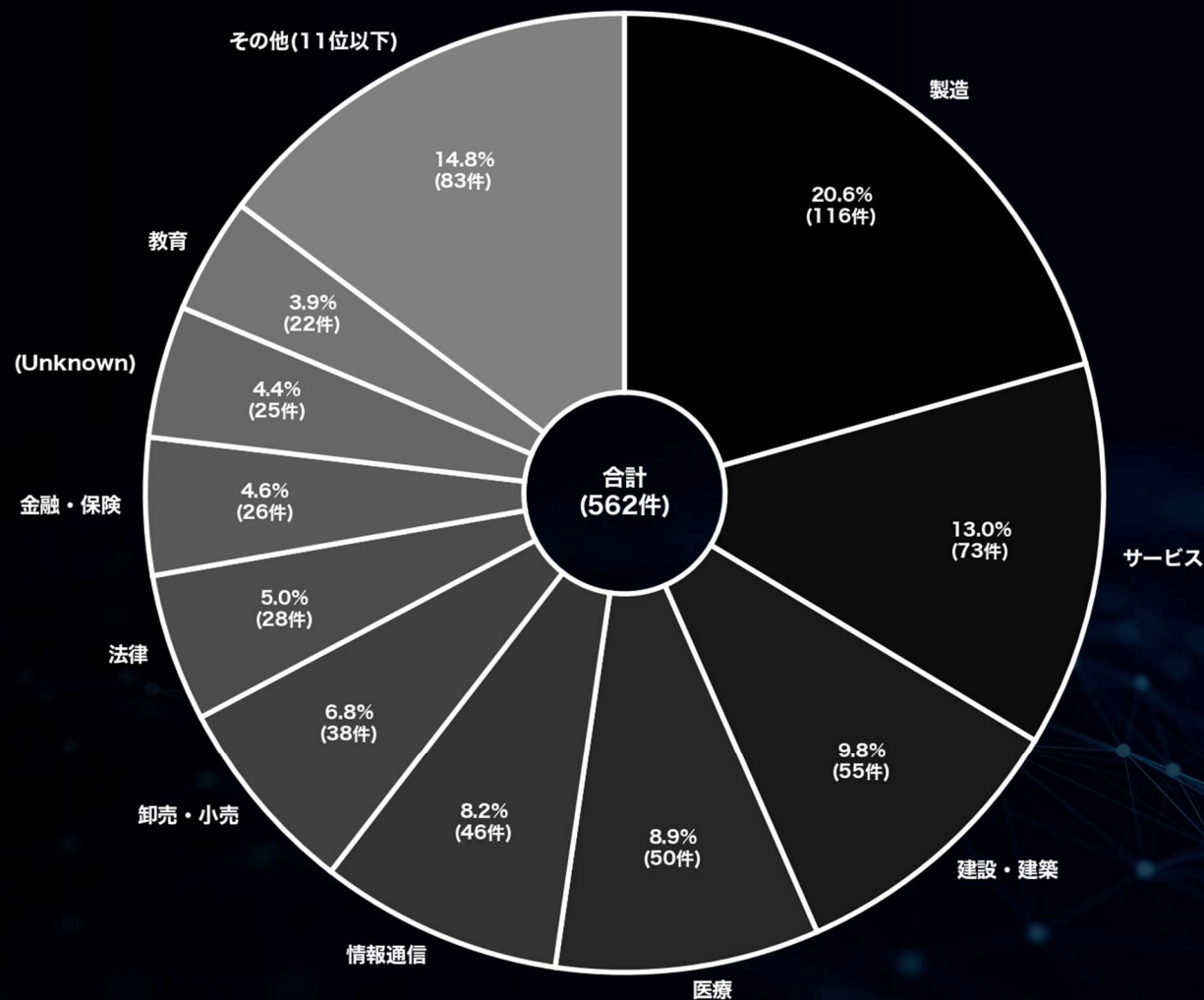
月別内訳 業種 TOP10 (全世界)

(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)



被害数の推移に関する統計

(全世界及び国内)

2025

8

被害数の推移 (全世界及び国内)

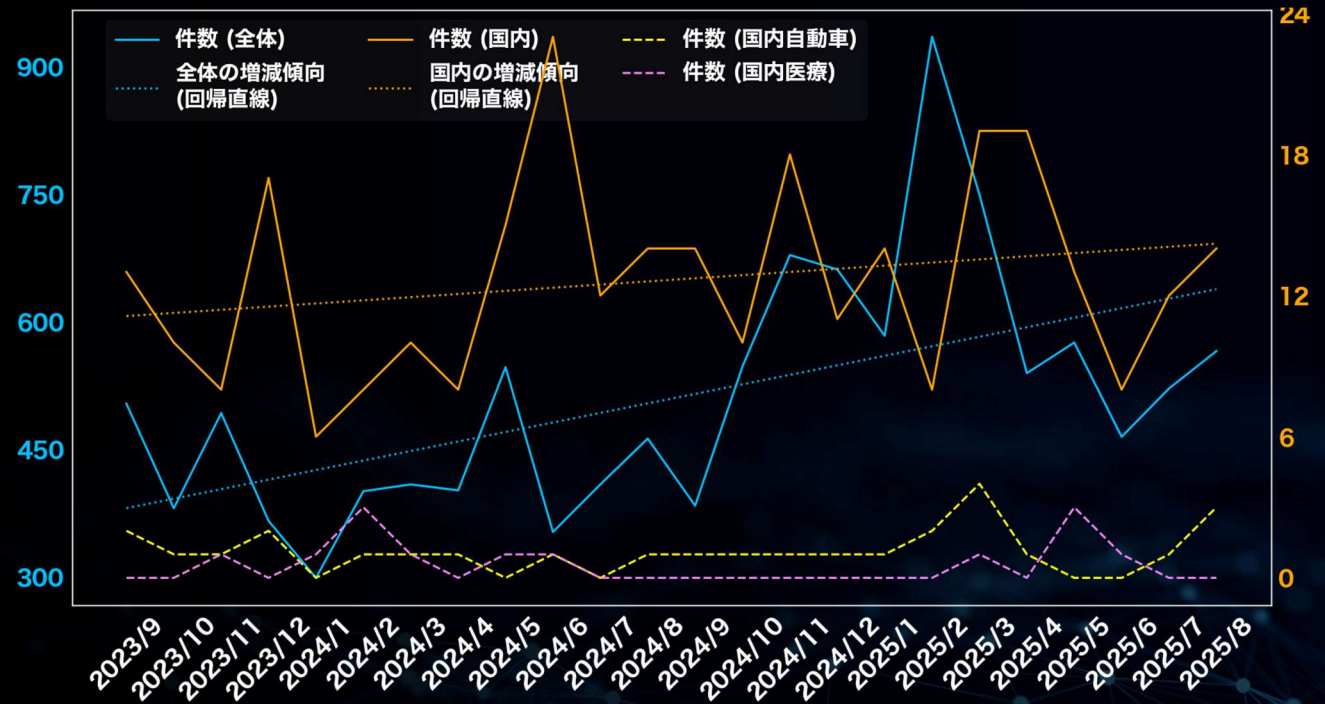
(過去2年間／2023年9月～2025年8月)

※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)
2023/9	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	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	539	19	1	0
2025/5	575	13	0	3
2025/6	464	8	0	1
2025/7	521	12	1	0
2025/8	565	14	3	0
合計	12215	304	27	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 月別統計

(国内)

2025

8

月別内訳 資本金別 (国内)

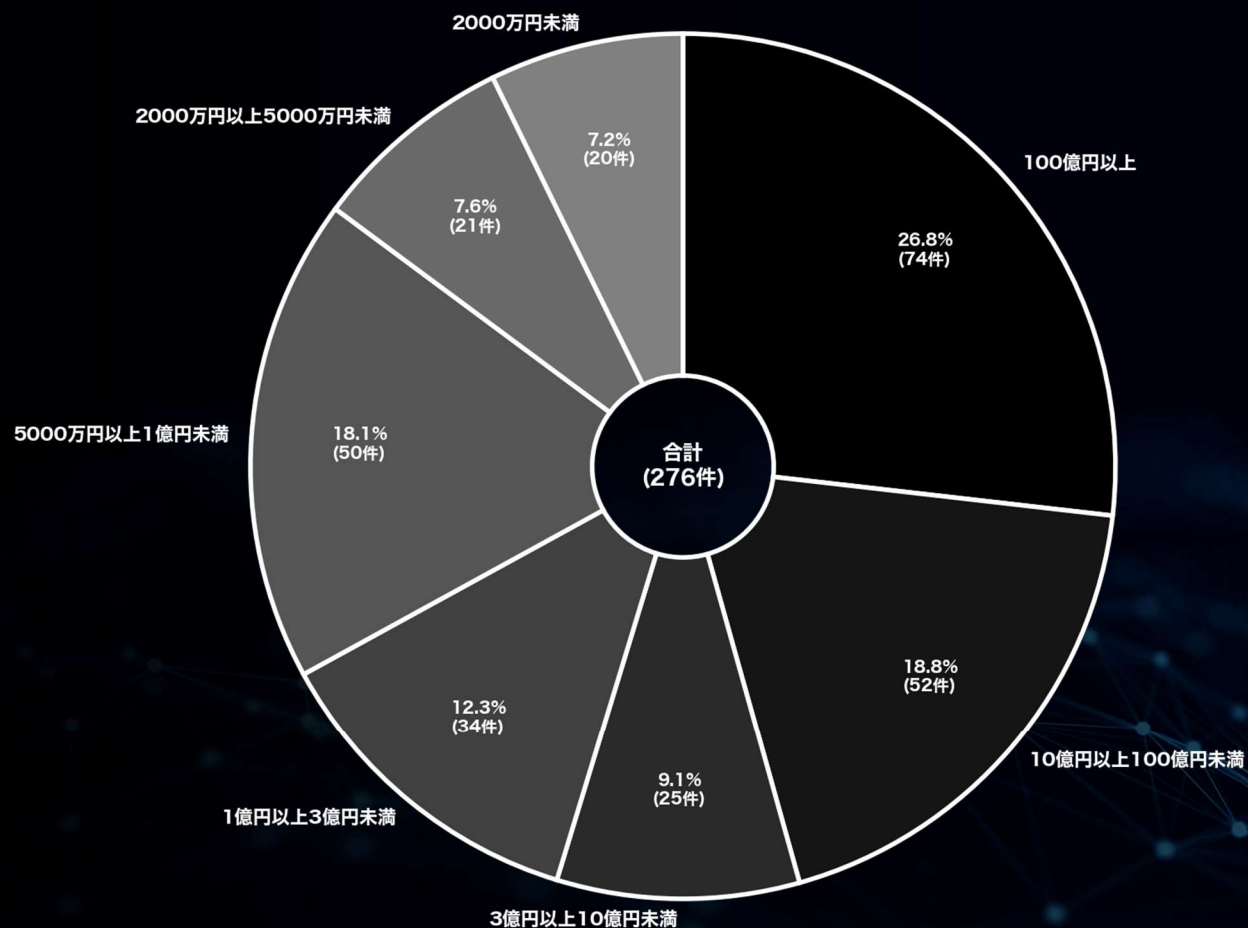
(過去2年間／2023年9月～2025年8月)

※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	26.8
10億円以上100億円未満	52	18.8
3億円以上10億円未満	25	9.1
1億円以上3億円未満	34	12.3
5000万円以上1億円未満	50	18.1
2000万円以上5000万円未満	21	7.6
2000万円未満	20	7.2

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)

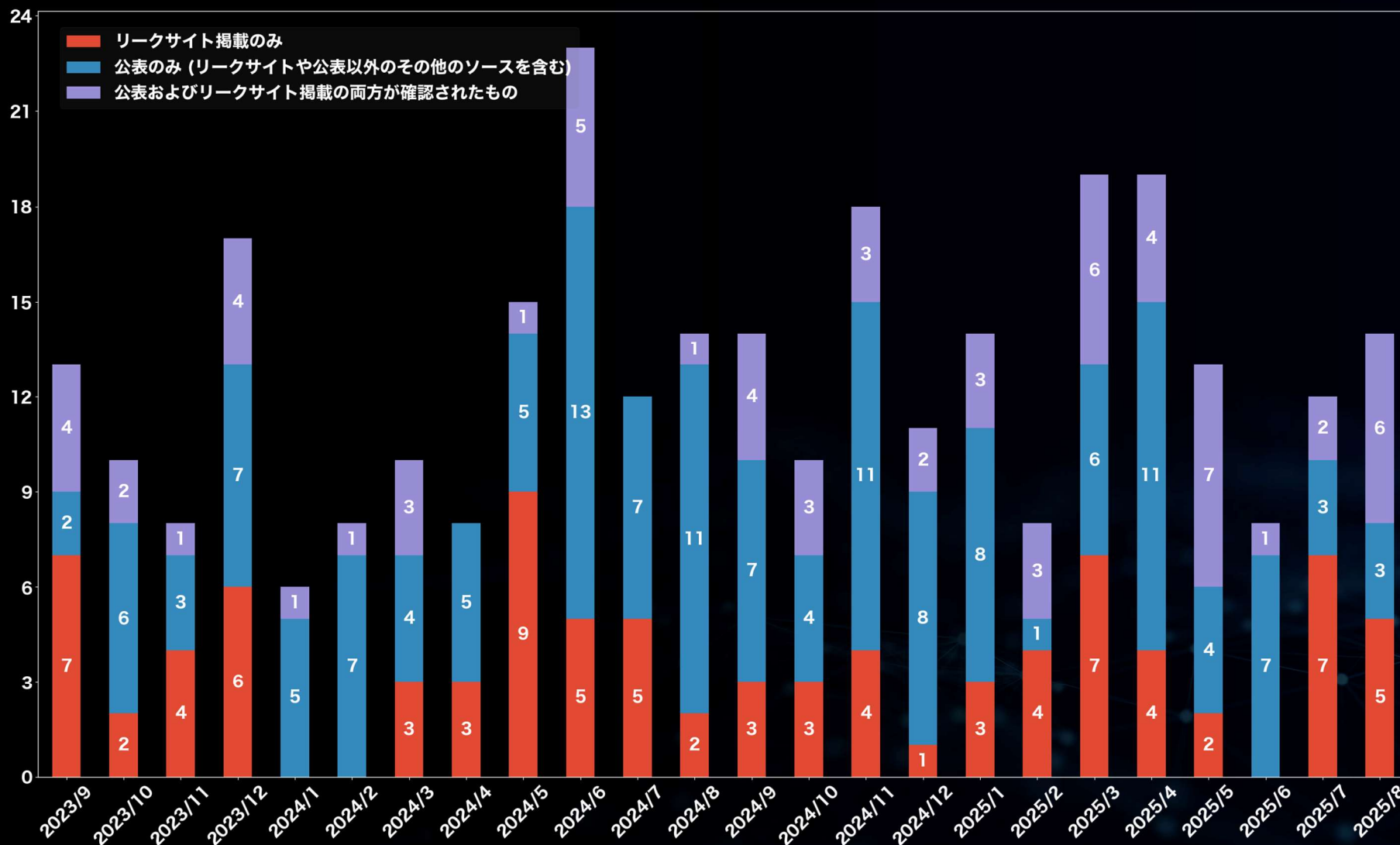
2025

8

公表割合 月別内訳 (国内)

(過去2年間／2023年9月～2025年8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

8

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9月～2025年8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
2024/9	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
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

被害月	攻撃グループ	業種概要
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	MEOOW	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)
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

被害月	攻撃グループ	業種概要
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
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)

(※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9月～2025年8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	Night Spire	ポンテ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

被害月	攻撃グループ	業種概要
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	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

被害月	攻撃グループ	業種概要
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	ハ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)

(※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)

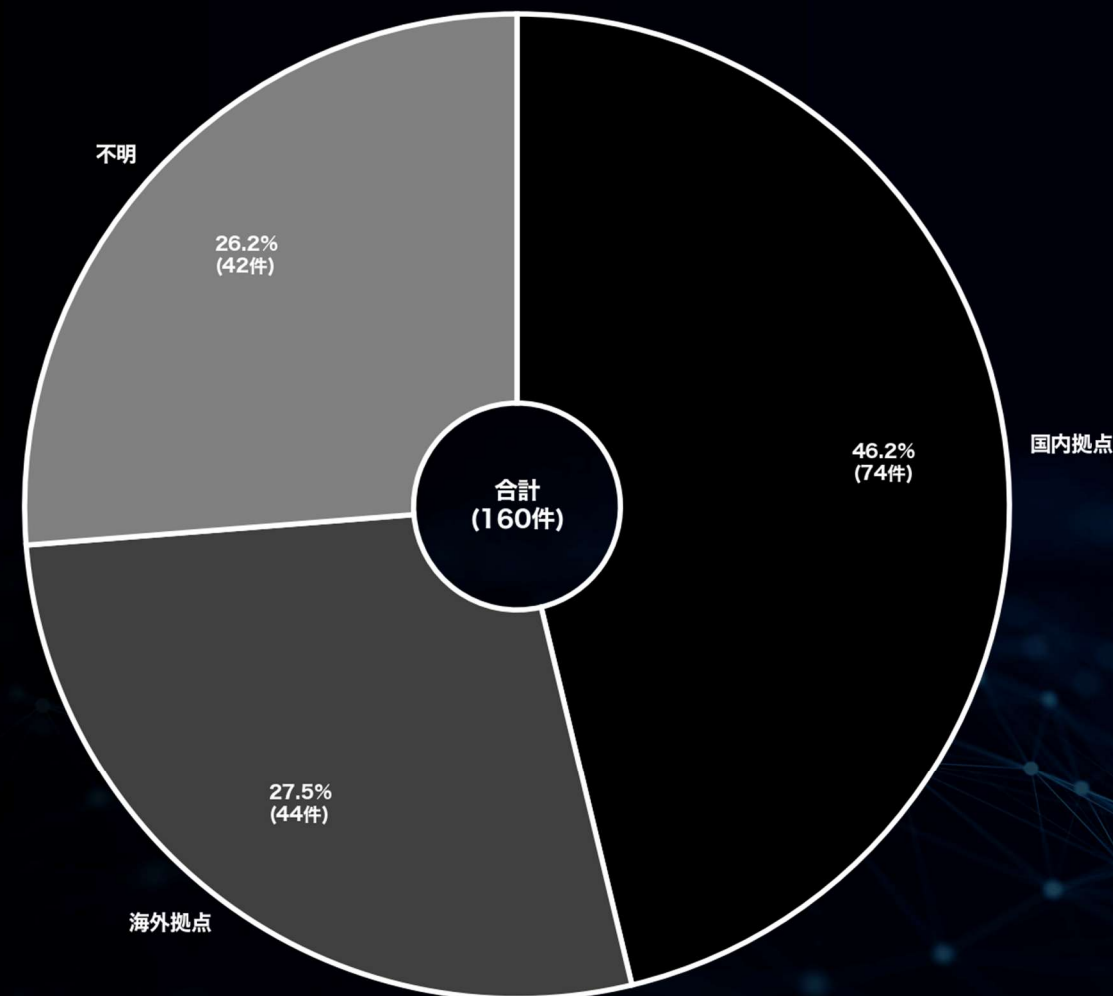
(過去1年間／2024年9月～2025年8月)

(※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	74	46.2
海外拠点	44	27.5
不明	42	26.2



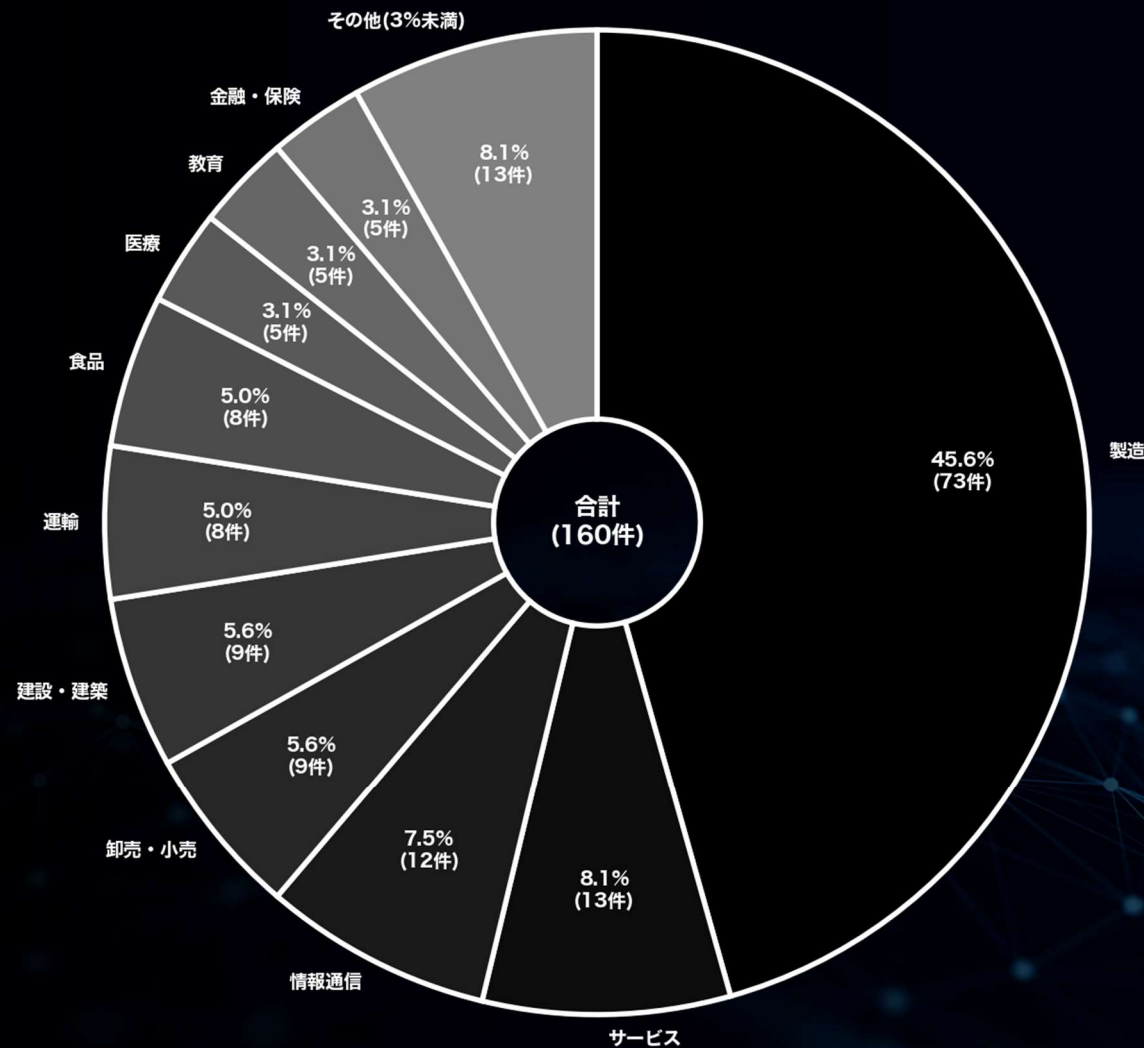
(※本ページの表／グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

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9月～2025年8月)

業種	件数	割合(%)
製造	73	45.6
サービス	13	8.1
情報通信	12	7.5
卸売・小売	9	5.6
建設・建築	9	5.6
運輸	8	5.0
食品	8	5.0
医療	5	3.1
教育	5	3.1
金融・保険	5	3.1
その他(3%未満)	13	8.1

▼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

8

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9月～2025年8月）

赤色は中小企業を示す

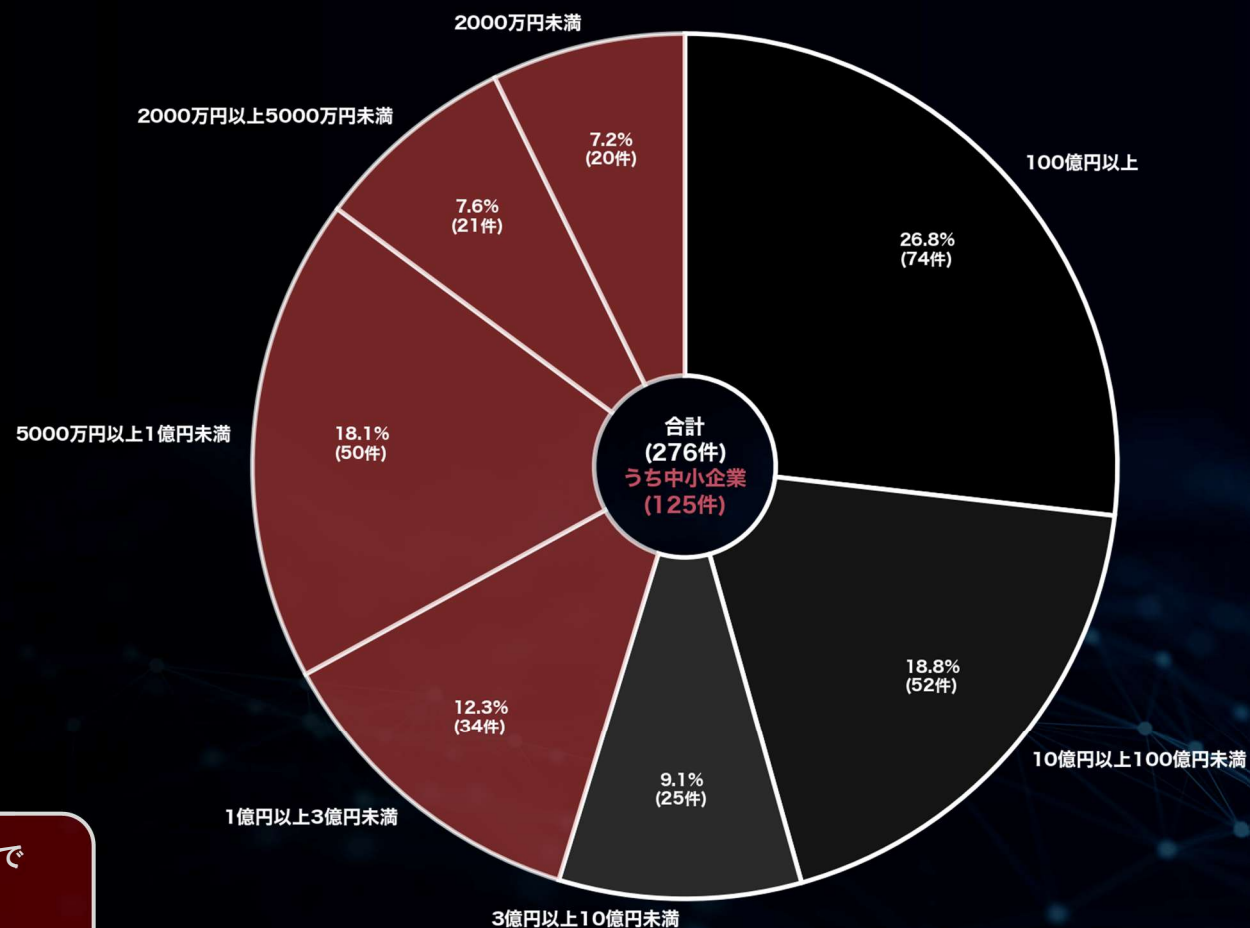
※資本金順に降順 / 資本金情報を公表していない一部の被害組織は除外

資本金	件数	割合(%)
100億円以上	74	26.8
10億円以上100億円未満	52	18.8
3億円以上10億円未満	25	9.1
1億円以上3億円未満	34	12.3
5000万円以上1億円未満	50	18.1
2000万円以上5000万円未満	21	7.6
2000万円未満	20	7.2

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125件にのぼり、全体の45.3%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）



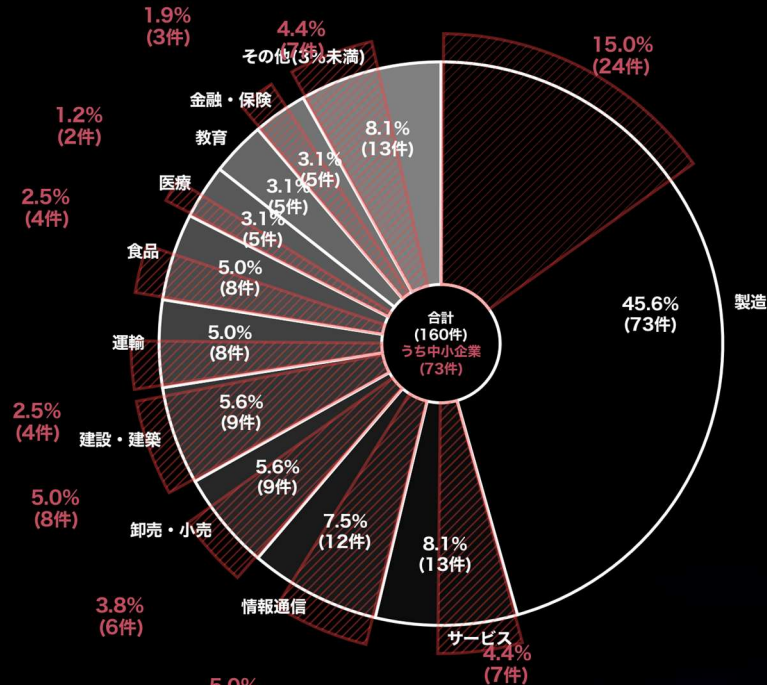
（※本ページの表／グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している）

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9月～2025年8月)

赤色は中小企業を示す

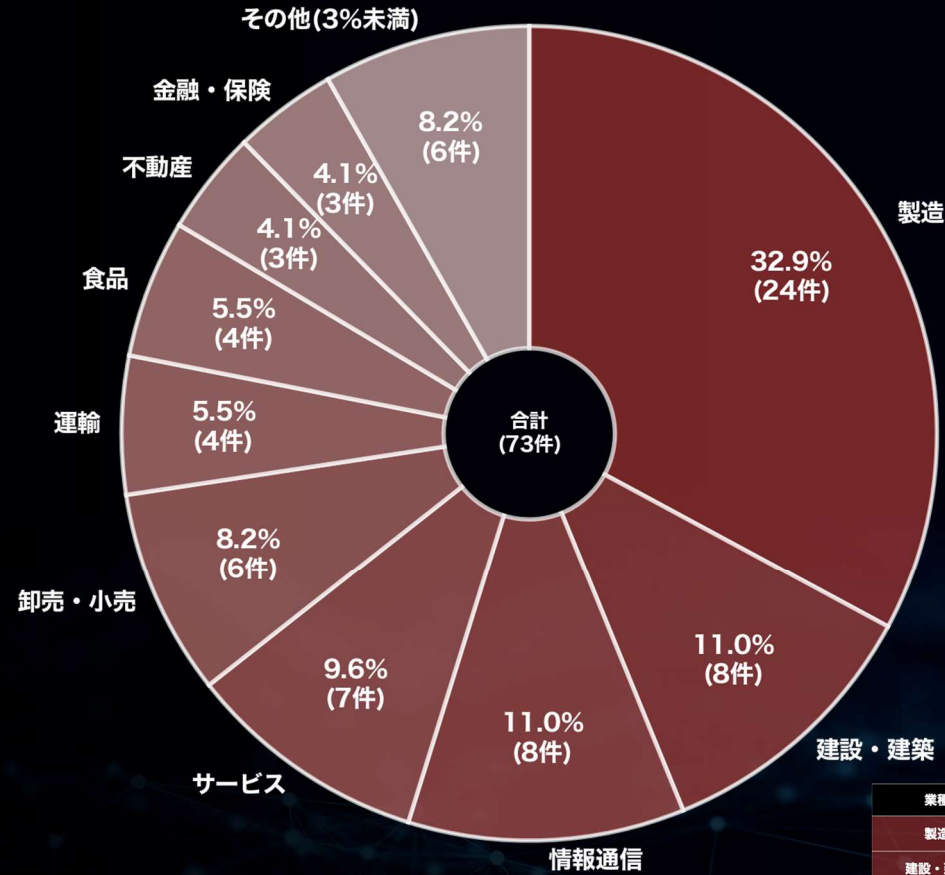
▼全体割合



※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	73 (24)	45.6 (15.0)
サービス	13 (7)	8.1 (4.4)
情報通信	12 (8)	7.5 (5.0)
卸売・小売	9 (6)	5.6 (3.8)
建設・建築	9 (8)	5.6 (5.0)
運輸	8 (4)	5.0 (2.5)
食品	8 (4)	5.0 (2.5)
医療	5 (2)	3.1 (1.2)
教育	5	3.1
金融・保険	5 (3)	3.1 (1.9)
その他(3%未満)	13 (7)	8.1 (4.4)

▼中小企業のための割合



業種	件数	割合(%)
製造	24	32.9
建設・建築	8	11.0
情報通信	8	11.0
サービス	7	9.6
卸売・小売	6	8.2
運輸	4	5.5
食品	4	5.5
不動産	3	4.1
金融・保険	3	4.1
その他(3%未満)	6	8.2

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

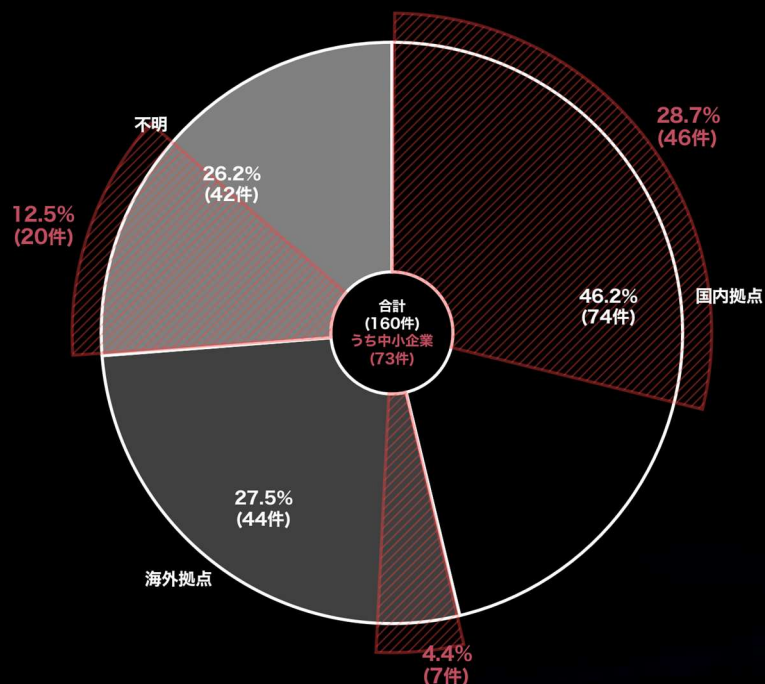
(※本ページの表/グラフの各値は、日本にフォーカスする関係上、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も加味し集計している)

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9月～2025年8月)

赤色は中小企業を示す

▼全体割合



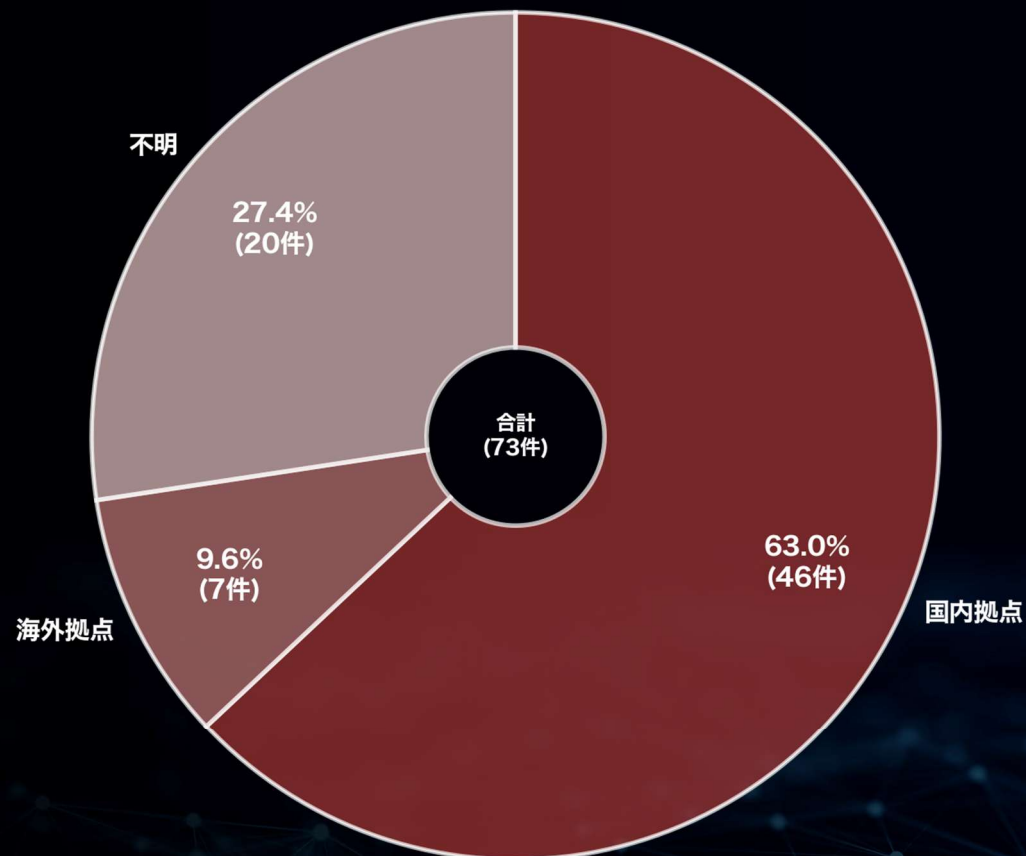
※
 「国内拠点」：公表等により、国内拠点における被害事案と判断されるケース数
 「海外拠点」：公表等により、海外拠点（支社／関係会社）における被害事案と判断されるケース数
 「不明」：上記以外、被害拠点の地域的情報が得られなかったケース数
 ※各数値の()内の数値は、資本金10億円未満の組織に対する集計結果を示す

拠点	件数 (中小企業)	割合 (%)
国内拠点	74 (46)	46.2 (28.7)
海外拠点	44 (7)	27.5 (4.4)
不明	42 (20)	26.2 (12.5)
合計	160 (73)	100 (45.6)

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	46	63.0
海外拠点	7	9.6
不明	20	27.4

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9月～2025年8月)

赤色は中小企業を示す

被害月	攻撃グループ	業種概要
2024/9	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
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

被害月	攻撃グループ	業種概要
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	MEOOW	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	産業機械メーカー
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

被害月	攻撃グループ	業種概要
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
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)

※ (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9月～2025年8月)

赤色は中小企業を示す

被害月	攻撃グループ	業種概要
2025/3	Night Spire	ポンテ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)
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

被害月	攻撃グループ	業種概要
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	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

被害月	攻撃グループ	業種概要
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	ハ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)

※ (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

8

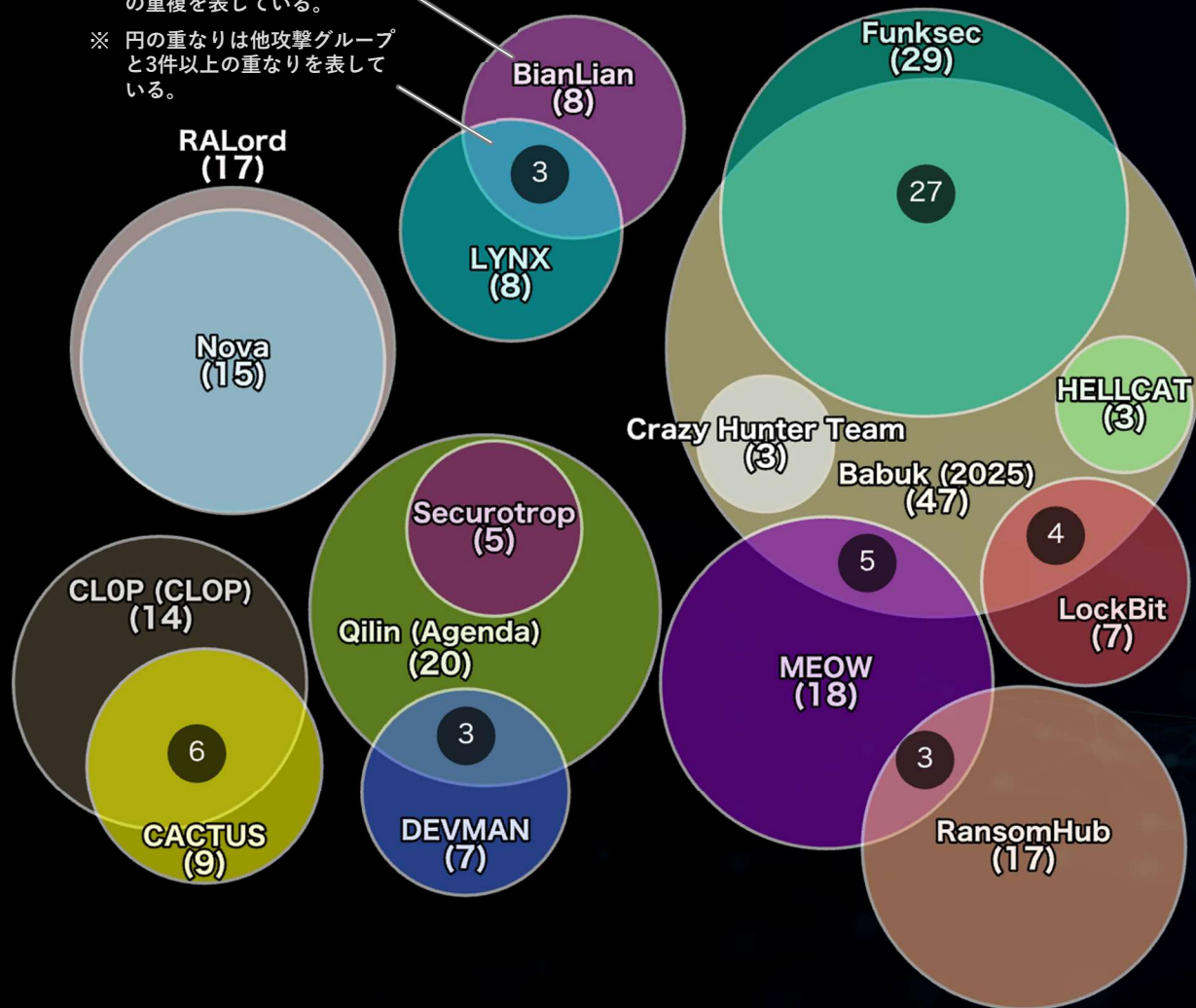
多重被害に関する分析

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9月～2025年8月) (累計164件) ※多重被害に遭った組織数の累計

※ 重ならない部分は他攻撃グループと3件未満の事案の重複を表している。

※ 円の重なりは他攻撃グループと3件以上の重なりを表している。



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

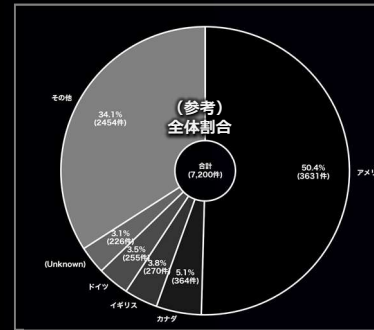
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

多重被害に遭った被害組織の傾向と分析 (全世界)

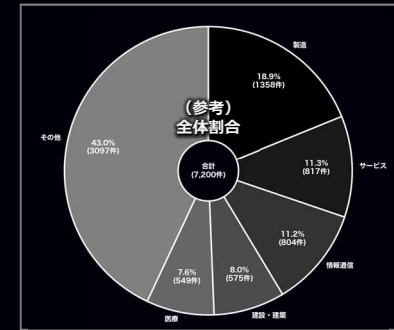
(過去1年間／2024年9月～2025年8月)

※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

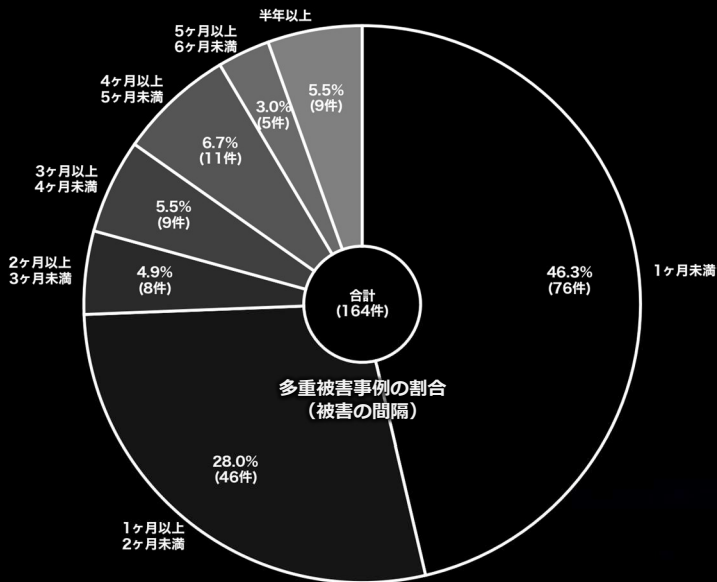


(参考比較) 同期間の全データにおける割合

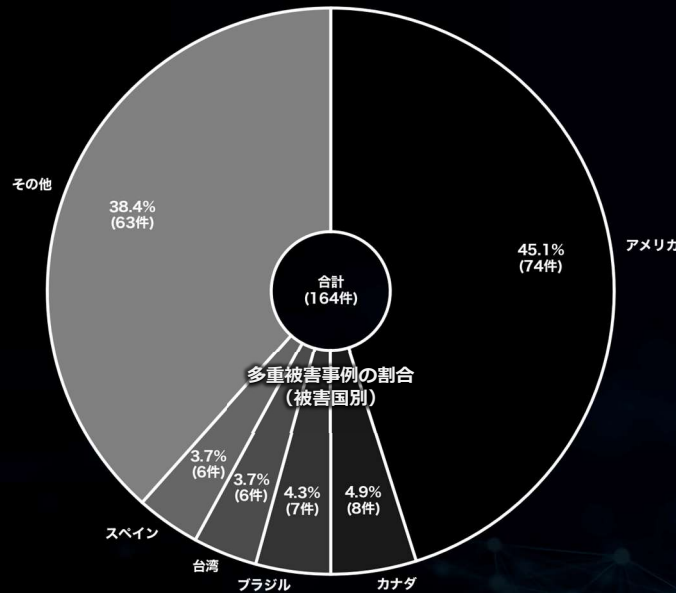


▼被害の間隔

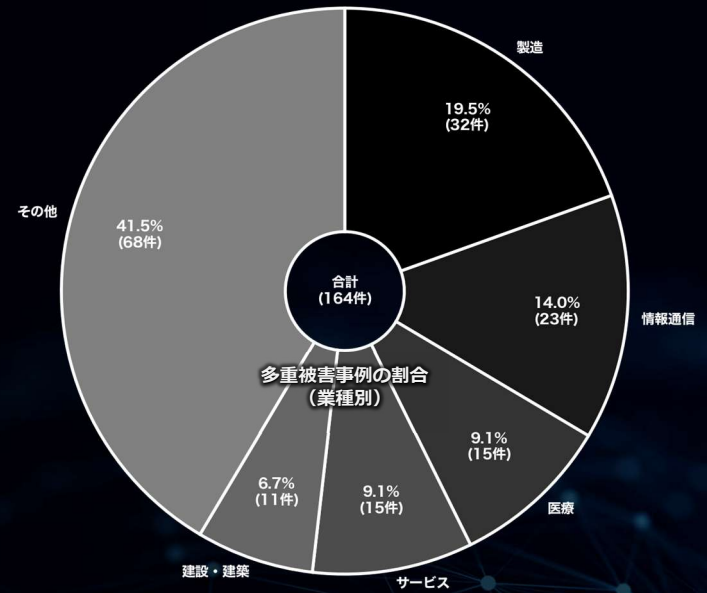
(一度目の被害から二度目の被害までの間隔)



▼被害国別



▼業種別



▶多重被害に遭った組織数の累計：164件 (全体7200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。

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

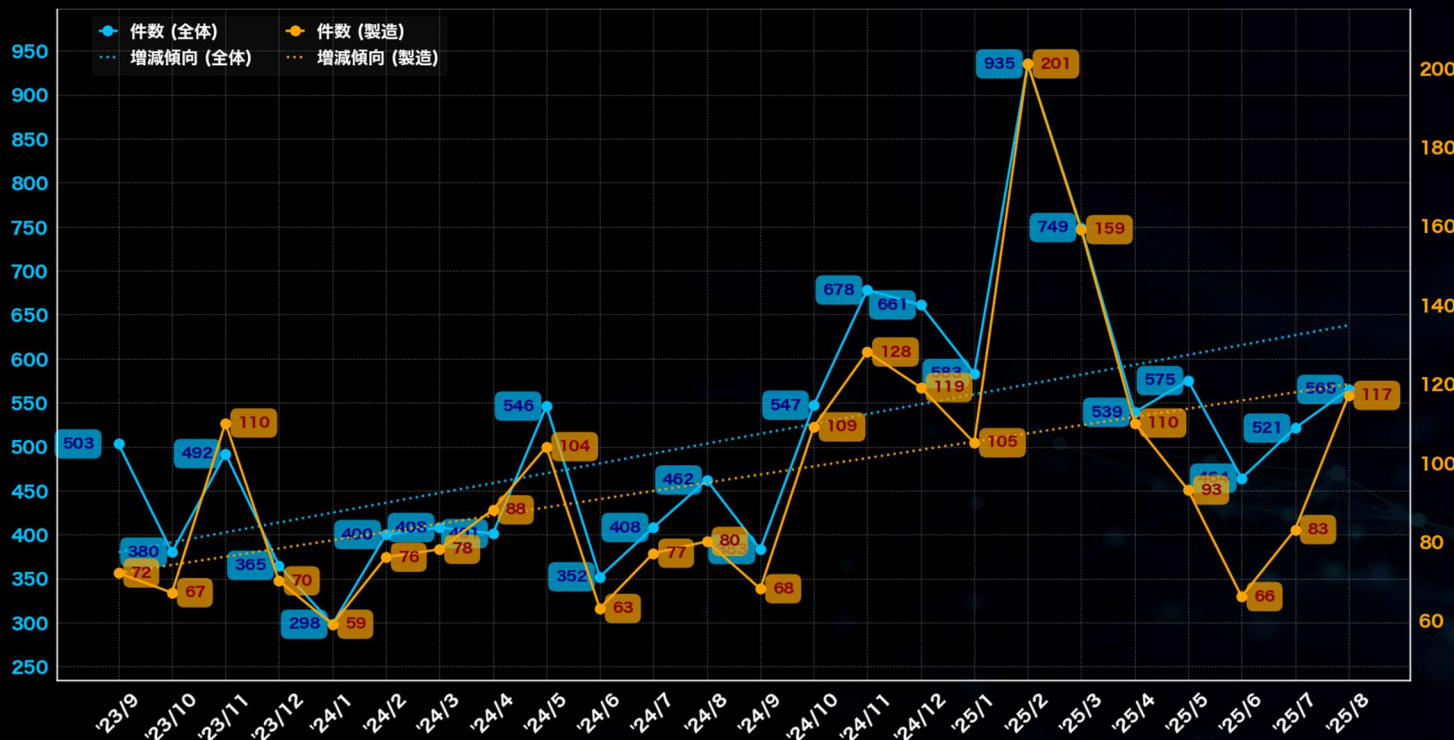
8

業種に関する分析 (全世界)

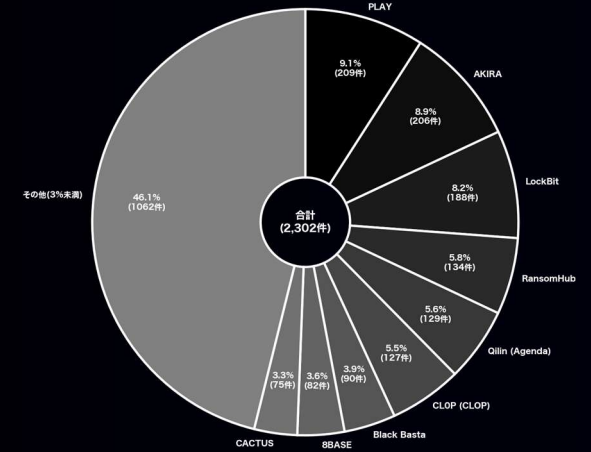
(過去2年間／2023年9月～2025年8月)

製造

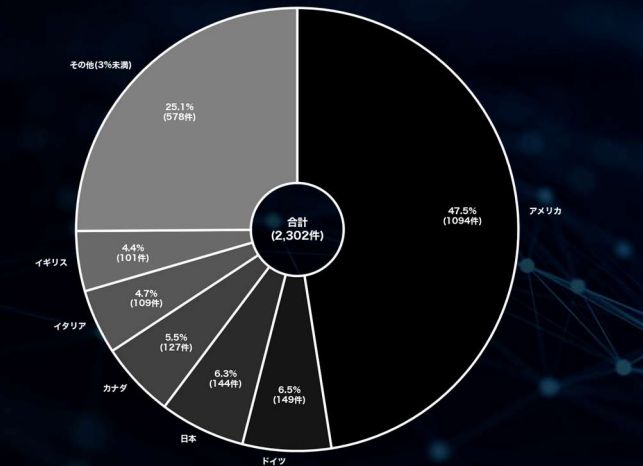
「製造」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、201件の掲載があった。一方、最も少なかった月は2024年1月で、59件であった。被害組織の所在国の割合では、アメリカが約48%と最も多く、次いでドイツと日本がそれぞれ約7%と約6%である。攻撃グループについては、少なくとも125のグループが関与しており、特に「PLAY」が209件のリークサイト掲載を実施している。次いで「AKIRA」と「LockBit」がそれぞれ206件と188件の掲載を行っている。製造関連の件数は全体件数に対して高い割合で推移しており、全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



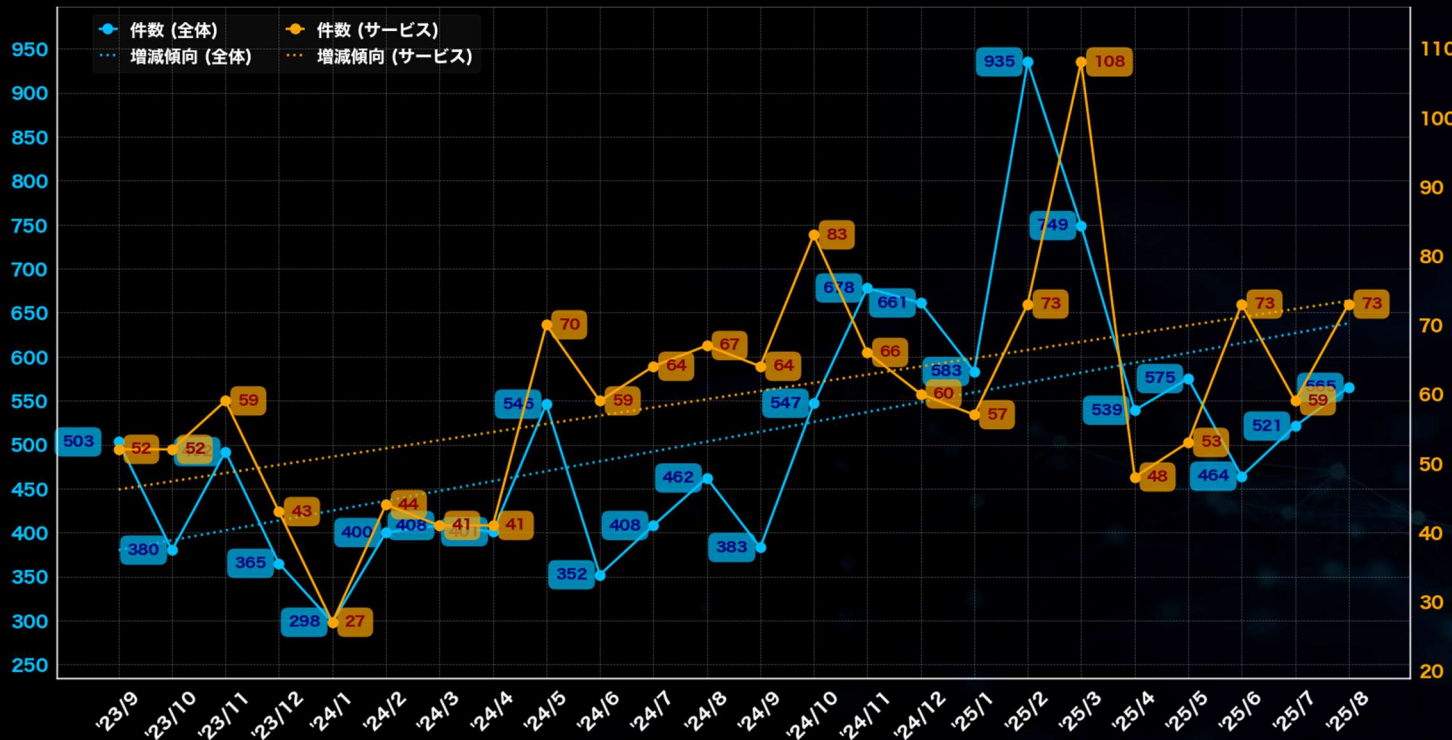
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

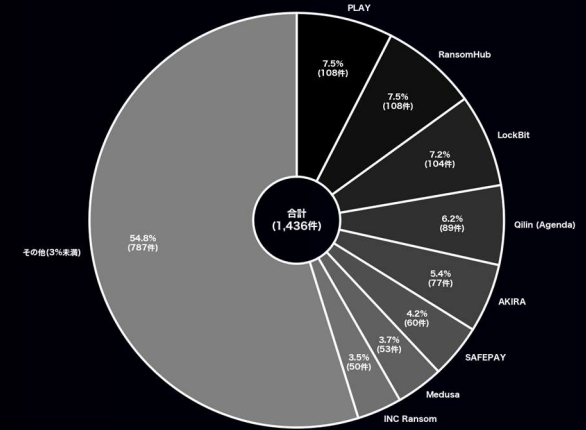
(過去2年間／2023年9月～2025年8月)

サービス

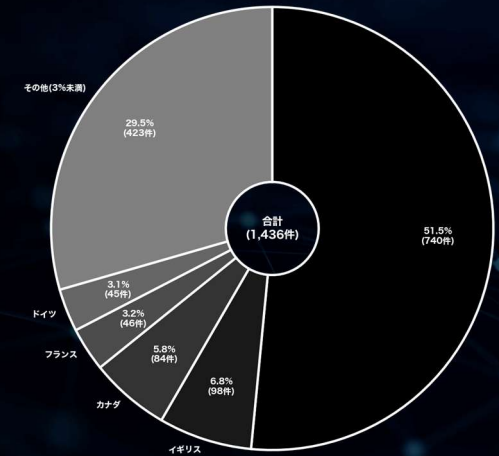
「サービス」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年3月で、108件の掲載があった。一方、最も少なかった月は2024年1月で、27件であった。被害組織の所在国の割合では、アメリカが約52%と最も多く、次いでイギリスとカナダがそれぞれ約7%と約6%である。攻撃グループについては、少なくとも116のグループが関与しており、特に「PLAY」が108件のリークサイト掲載を実施している。次いで「RansomHub」と「LockBit」がそれぞれ104件と104件の掲載を行っている。サービス関連の件数は製造関連と同じく全体件数に対し、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



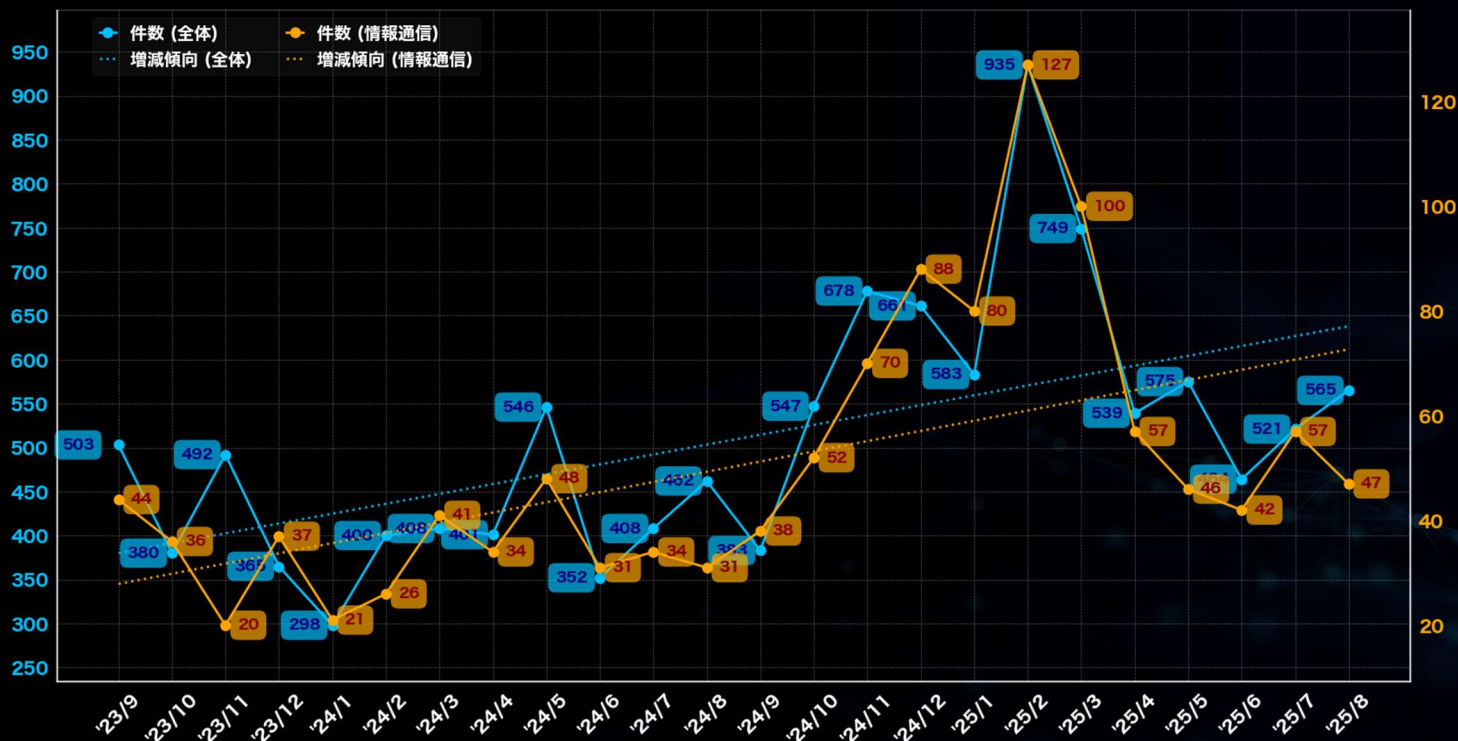
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

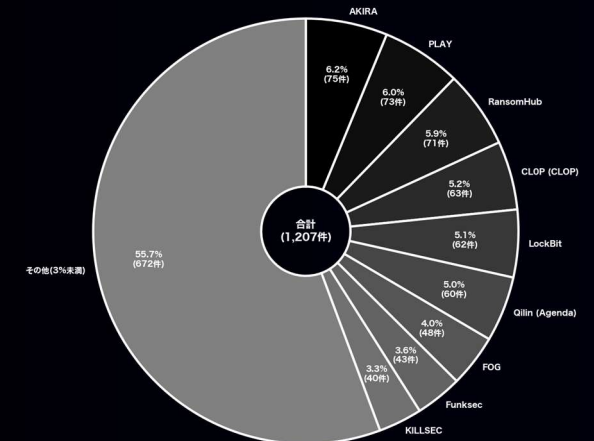
(過去2年間／2023年9月～2025年8月)

情報通信

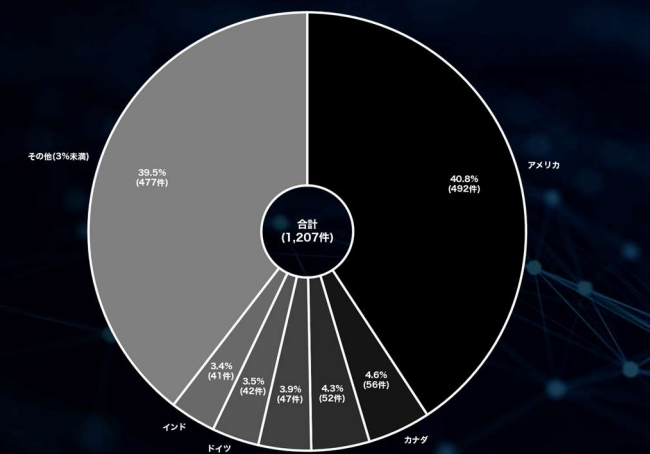
「情報通信」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、127件の掲載があった。一方、最も少なかった月は2023年11月で、20件であった。被害組織の所在国の割合では、アメリカが約41%と最も多く、次いでカナダとイギリスがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも119のグループが関与しており、特に「AKIRA」が75件のリークサイト掲載を実施している。次いで「RansomHub」と「PLAY」がそれぞれ73件と71件の掲載を行っている。過去2年間におけるリークサイト掲載件数は明確な増加傾向にある。



▼攻撃グループ別



▼国別



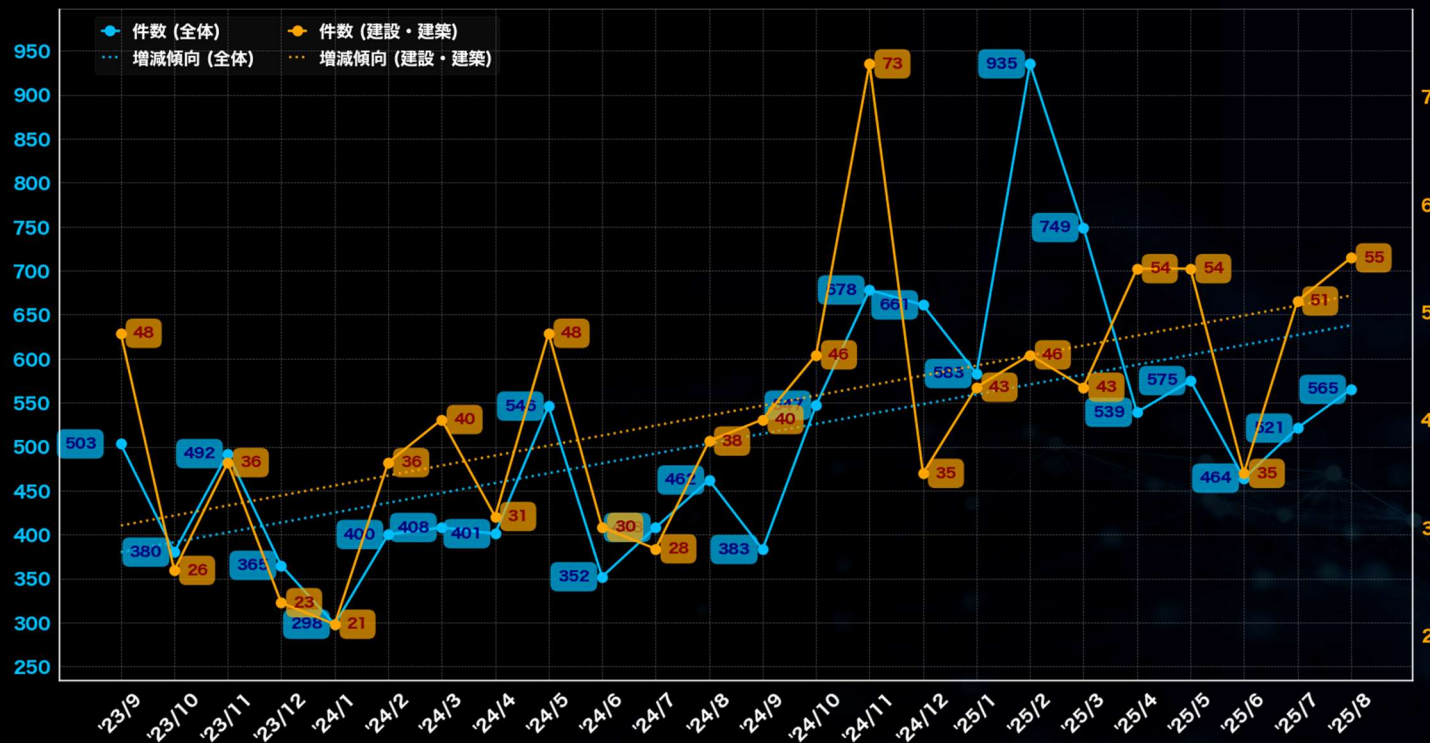
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

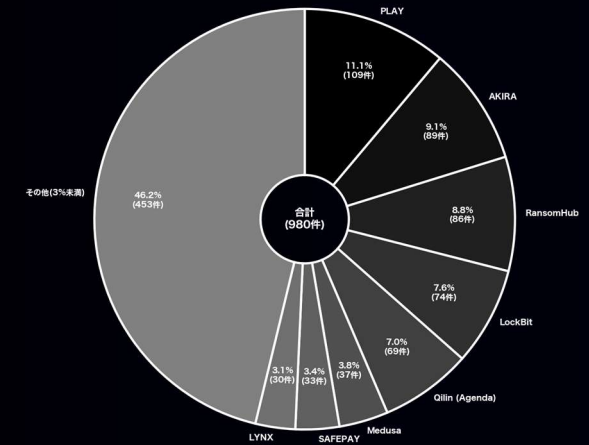
(過去2年間／2023年9月～2025年8月)

建設・建築

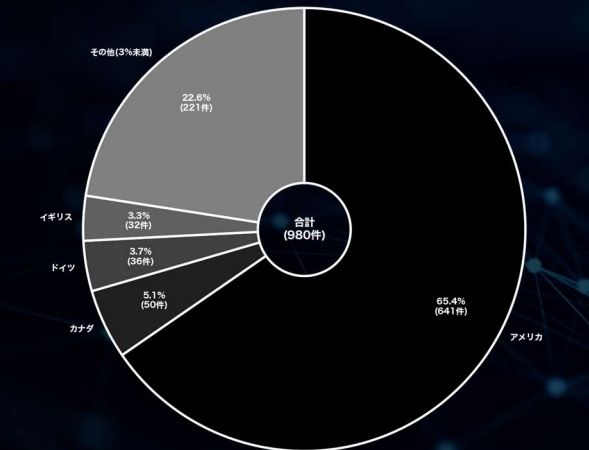
「建設・建築」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2024年11月で、73件の掲載があった。一方、最も少なかった月は2024年1月で、21件であった。被害組織の所在国の割合では、アメリカが約65%と最も多く、次いでカナダとドイツがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも94のグループが関与しており、特に「PLAY」が109件のリークサイト掲載を実施している。次いで「AKIRA」と「RansomHub」がそれぞれ89件と86件の掲載を行っている。製造関連などと比べると件数は少ないものの、明確な増加傾向にある。



▼攻撃グループ別



▼国別



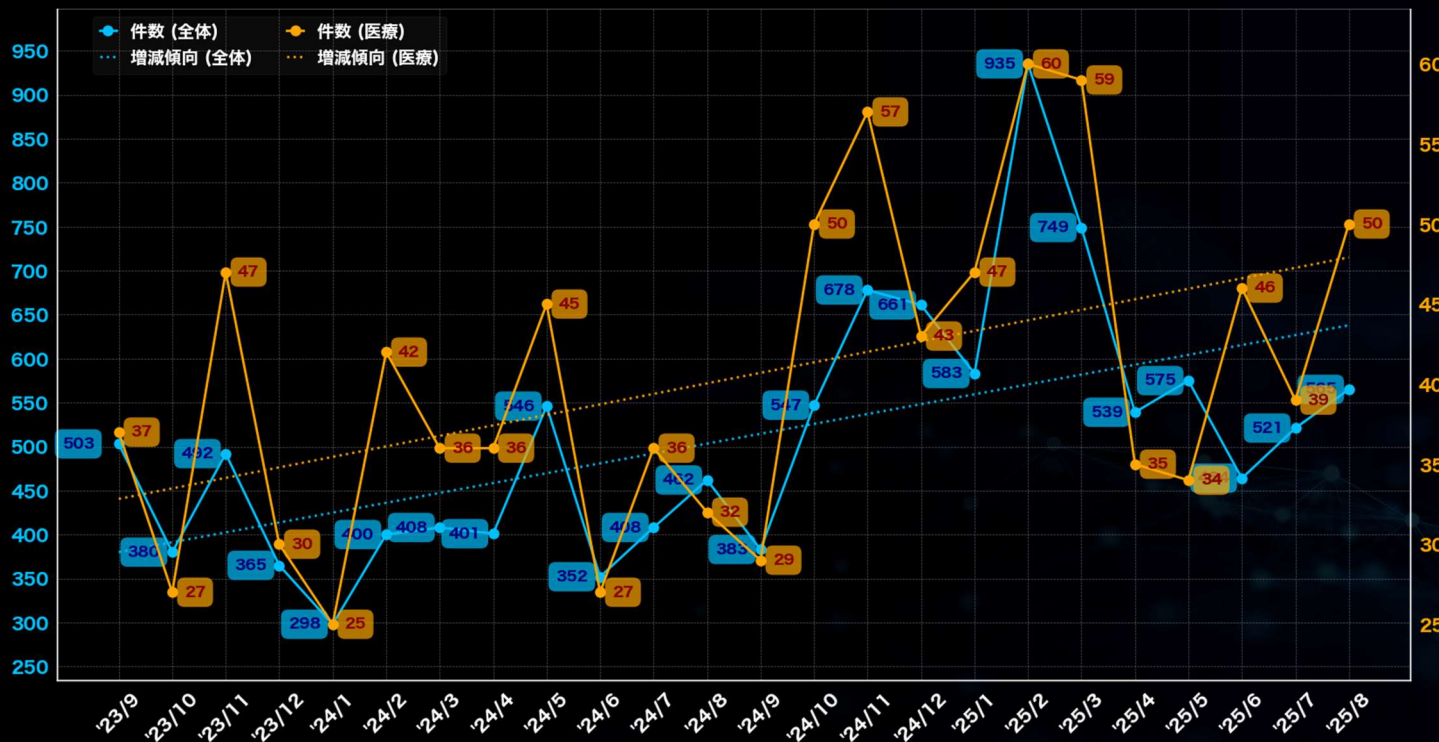
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

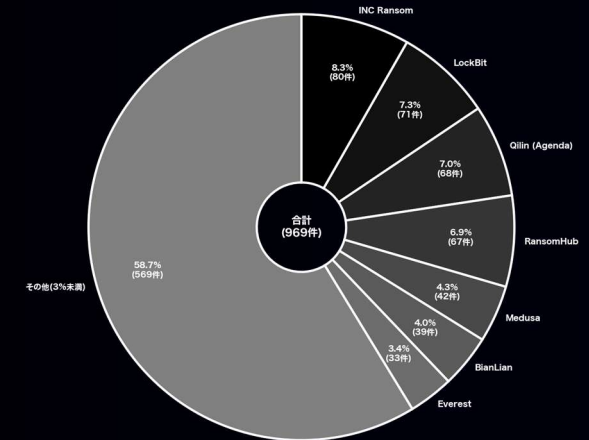
(過去2年間／2023年9月～2025年8月)

医療

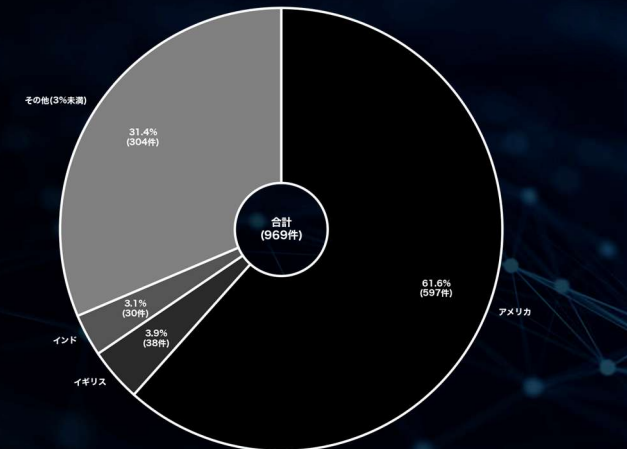
「医療」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、60件の掲載があった。一方、最も少なかった月は2024年1月で、25件であった。被害組織の所在国の割合では、アメリカが約62%と最も多く、次いでイギリス、インドがそれぞれ約4%と約3%である。攻撃グループについては、少なくとも106のグループが関与しており、特に「INC Ransom」が80件のリークサイト掲載を実施している。次いで「LockBit」と「Qilin (Agenda) (Rhysida)」がそれぞれ71件と68件の掲載を行っている。かつては低水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



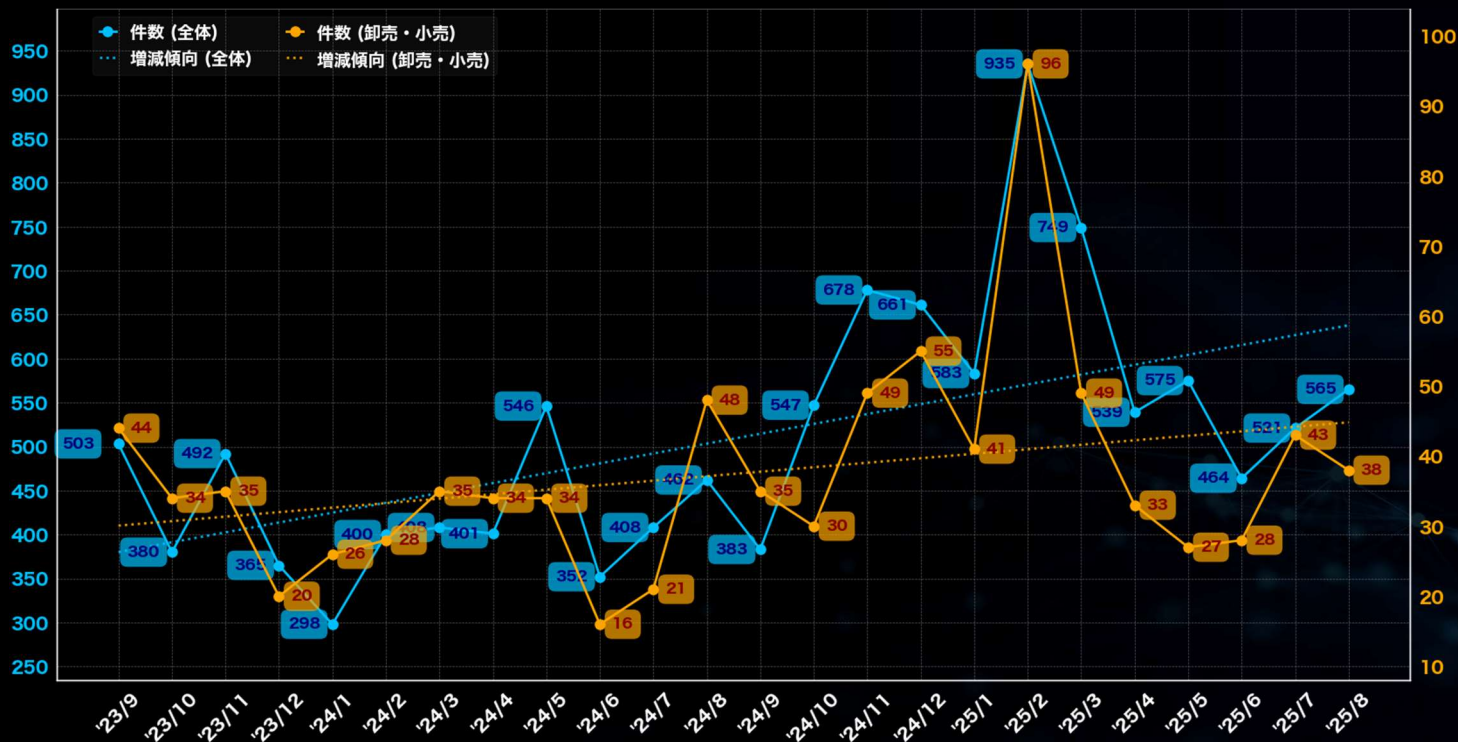
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

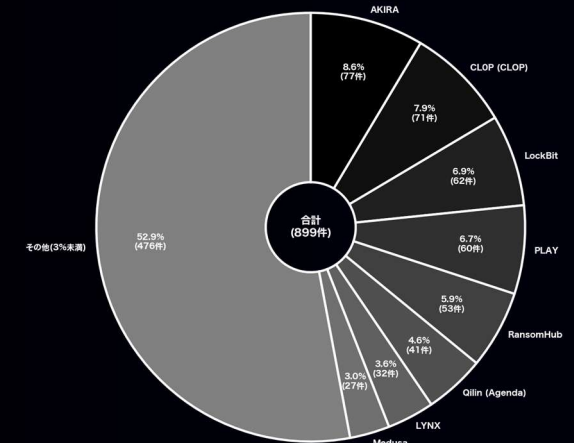
(過去2年間／2023年9月～2025年8月)

卸売・小売

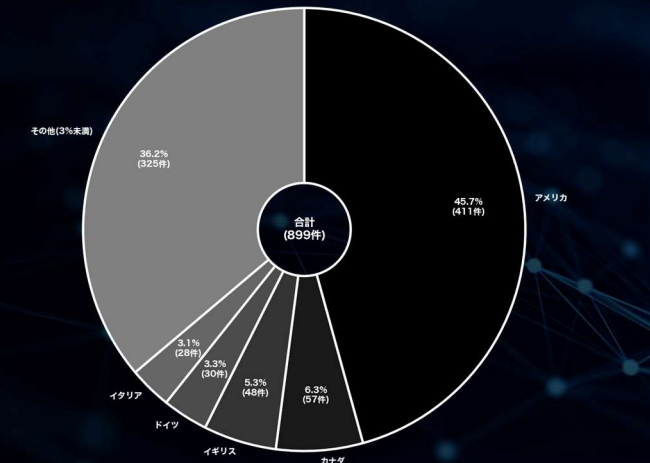
「卸売・小売」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、96件の掲載があった。一方、最も少なかった月は2024年6月で、16件であった。被害組織の所在国の割合では、アメリカが約46%と最も多く、次いでカナダとイギリスがそれぞれ約6%と約5%である。攻撃グループについては、少なくとも90のグループが関与しており、特に「AKIRA」が77件のリークサイト掲載を実施している。次いで「CLOP (CLOP)」と「LockBit」が71件と62件の掲載を行っている。卸売・小売関連は大きな増減の波があるものの、過去2年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



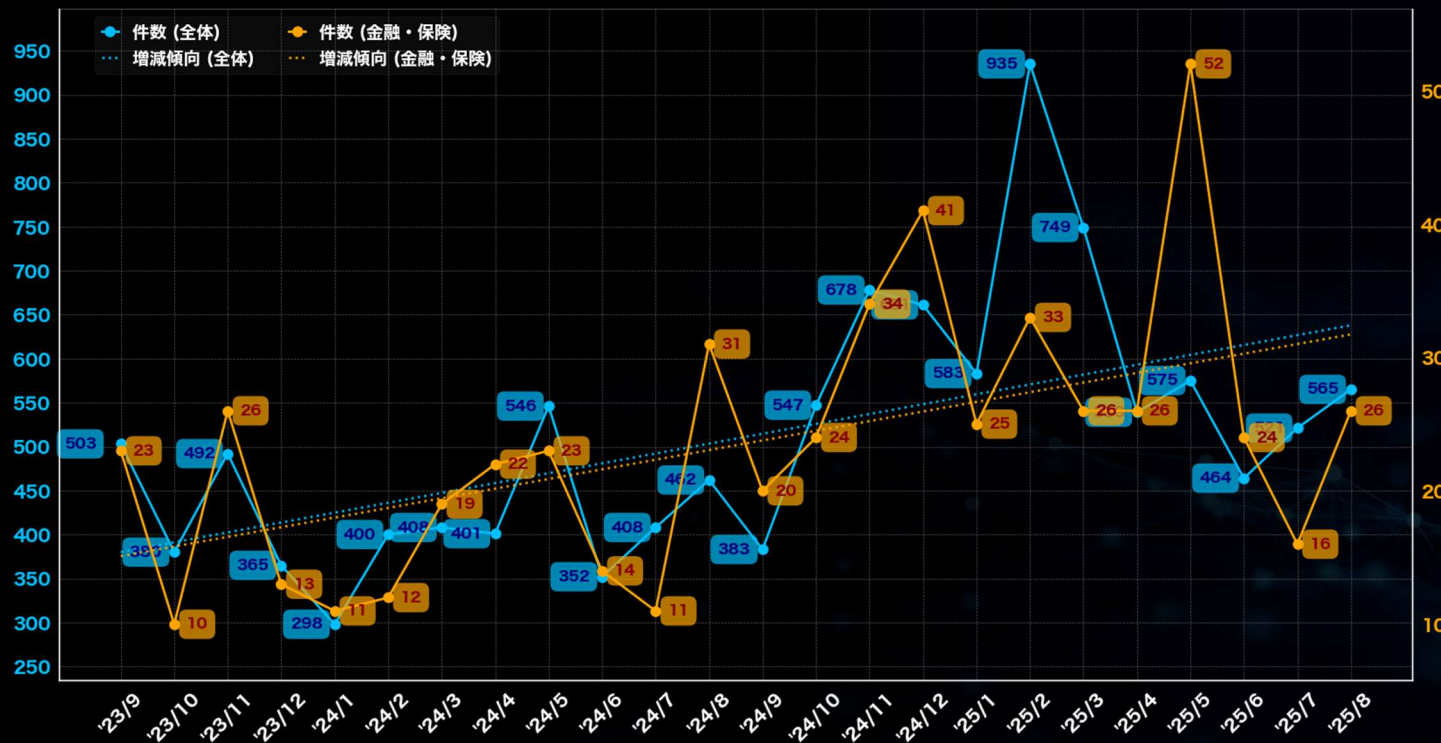
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

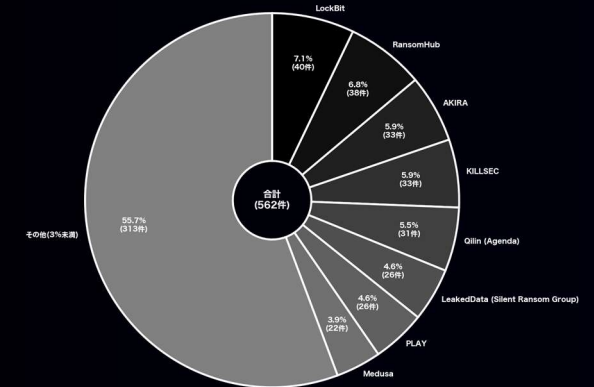
(過去2年間／2023年9月～2025年8月)

金融・保険

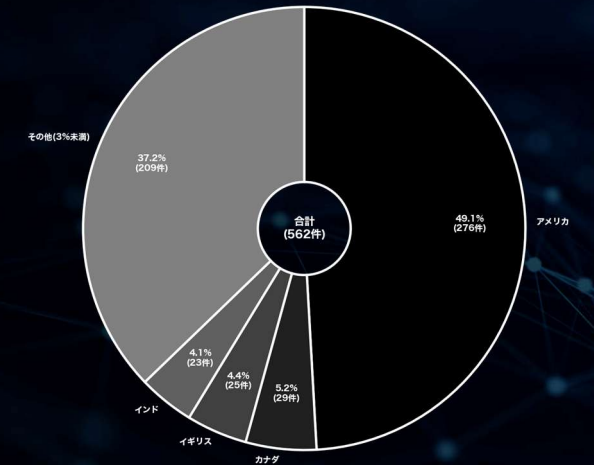
「金融・保険」業界に対するランサムウェア攻撃のリークサイト掲載件数は、最も多かった月が2025年5月で、52件の掲載があった。一方、最も少なかった月は2023年10月で、10件であった。被害組織の所在国の割合では、アメリカが約49%と最も多く、次いでカナダとイギリスがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも98のグループが関与しており、特に「LockBit」が40件のリークサイト掲載を実施している。次いで「RansomHub」と「AKIRA」がそれぞれ38件と33件の掲載を行っている。金融・保険関連は全体件数に対する割合は低いものの明確な増加傾向にある。



▼攻撃グループ別



▼国別



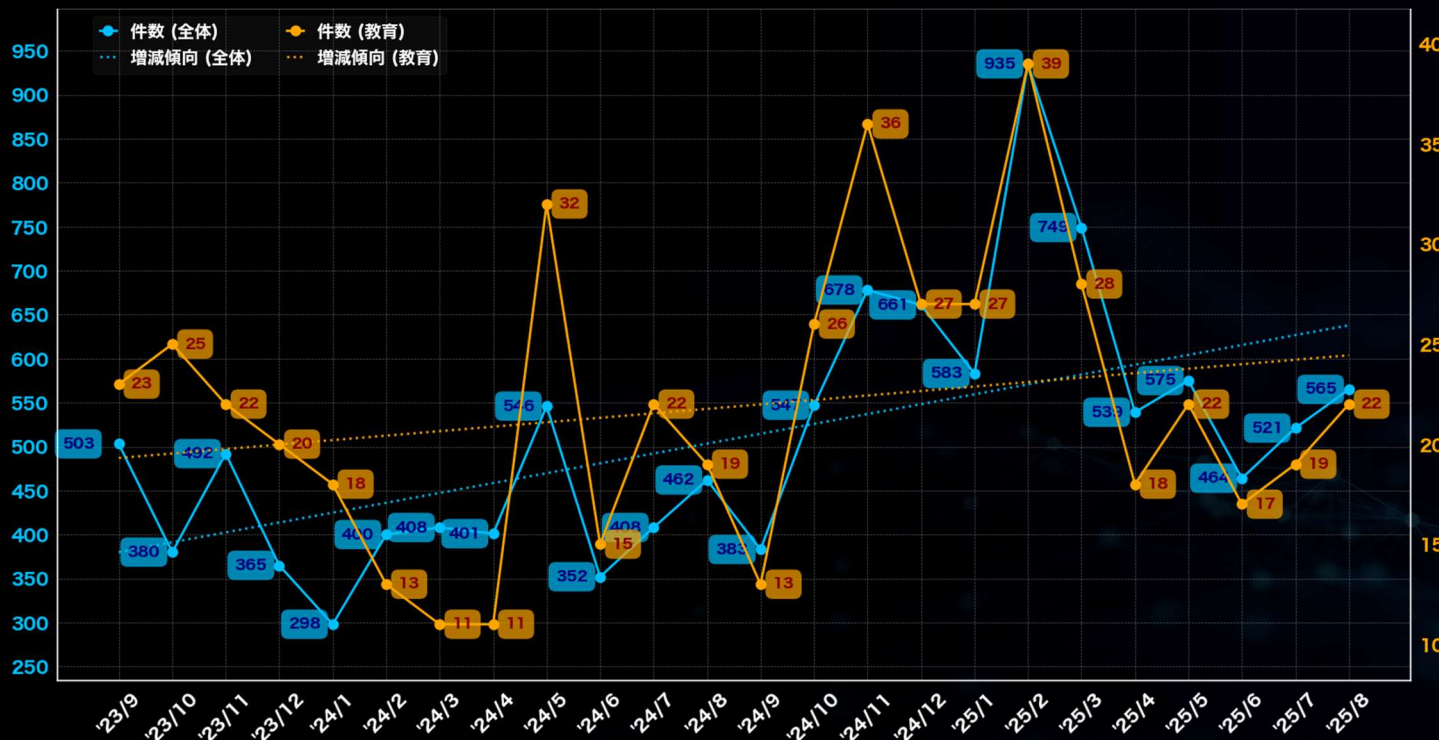
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

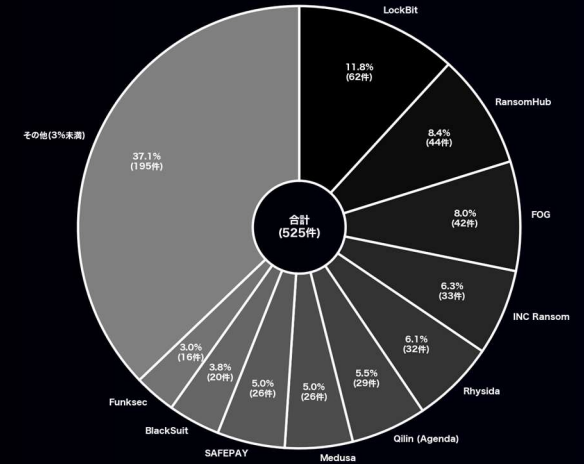
(過去2年間／2023年9月～2025年8月)

教育

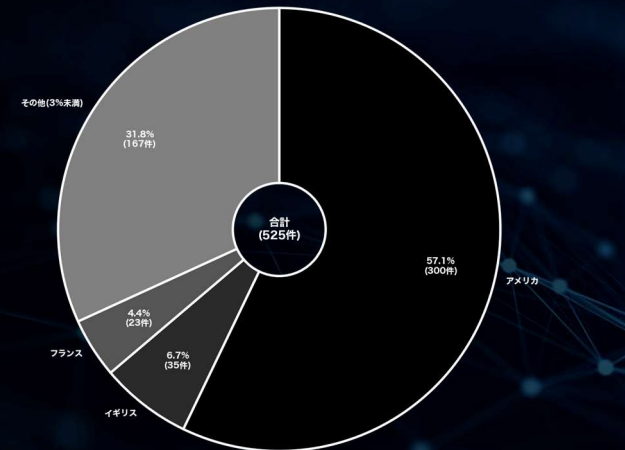
「教育」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、39件の掲載があった。一方、最も少なかった月は2024年3月と4月で、11件であった。被害組織の所在国の割合では、アメリカが約57%と最も多く、次いでイギリスとフランスがそれぞれ約7%と約4%である。攻撃グループについては、少なくとも81のグループが関与しており、特に「LockBit」が62件のリークサイト掲載を実施している。次いで「RansomHub」と「FOG」がそれぞれ44件と42件の掲載を行っている。教育業界は、攻撃グループ別で見ると、同業界を主な標的の一つとする「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



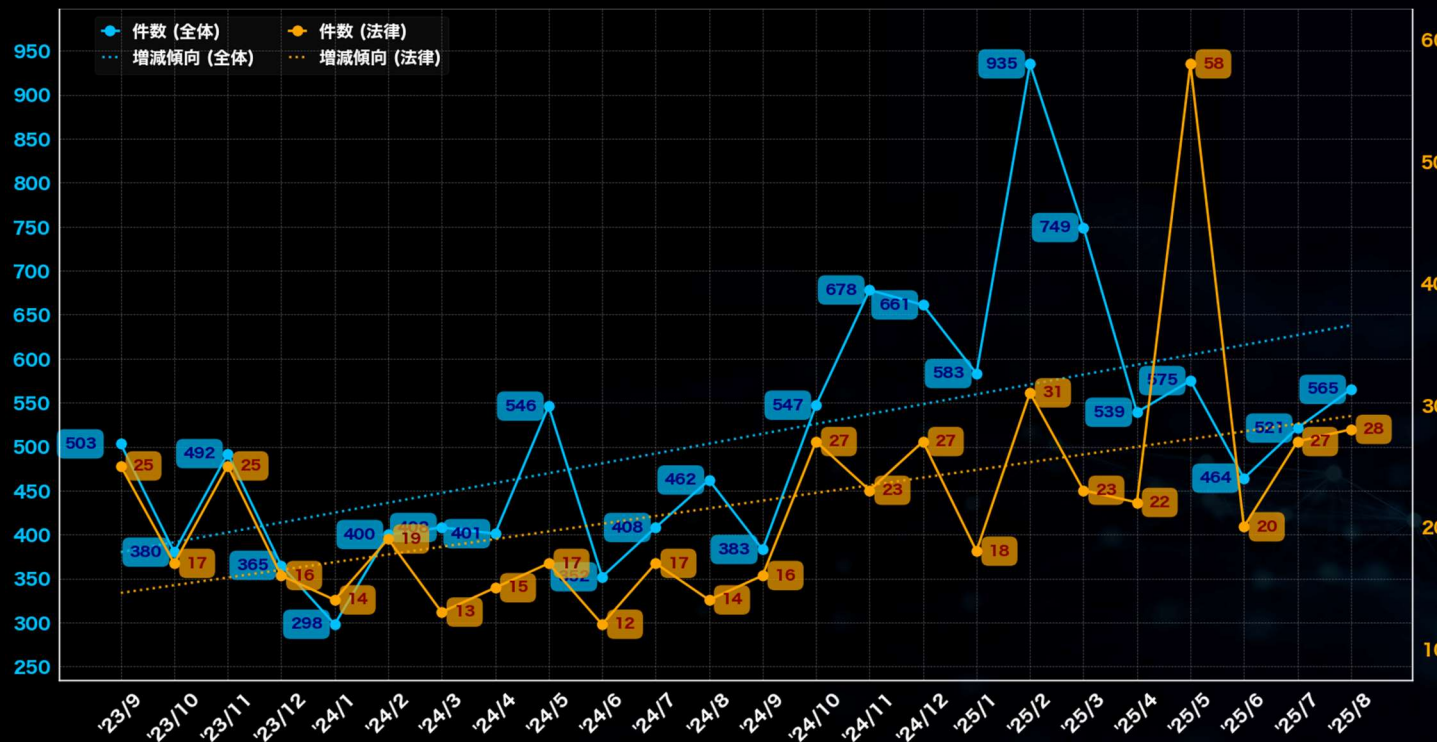
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

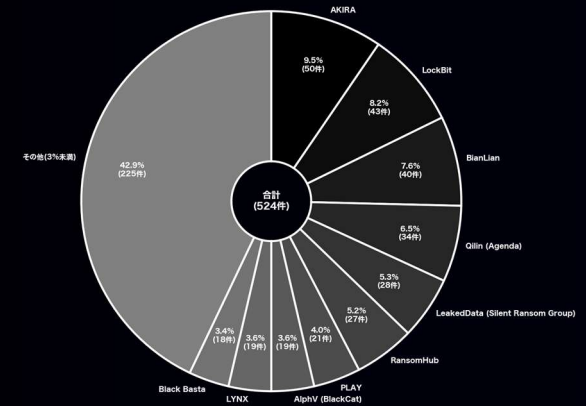
(過去2年間／2023年9月～2025年8月)

法律

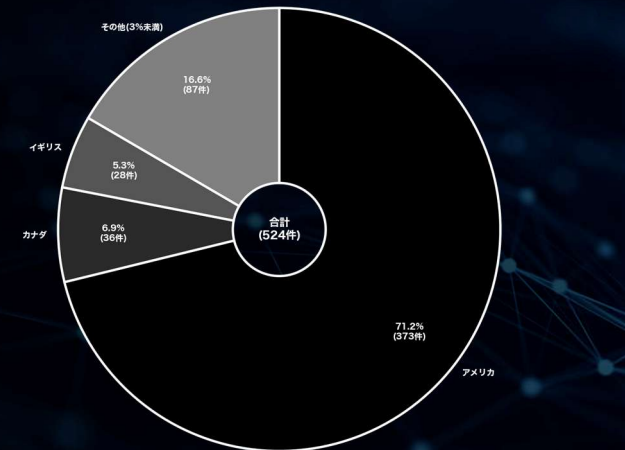
「法律」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年5月で、58件の掲載があった。一方、最も少なかった月は2024年6月で、12件であった。被害組織の所在国の割合では、アメリカが約71%と最も多く、次いでカナダとイギリスがそれぞれ約7%と約5%である。攻撃グループについては、少なくとも77のグループが関与しており、特に「AKIRA」が50件のリークサイト掲載を実施している。次いで「LockBit」と「BianLian」がそれぞれ43件と40件の掲載を行っている。法律関連は2023年末以降、減少傾向が見られたが、2024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



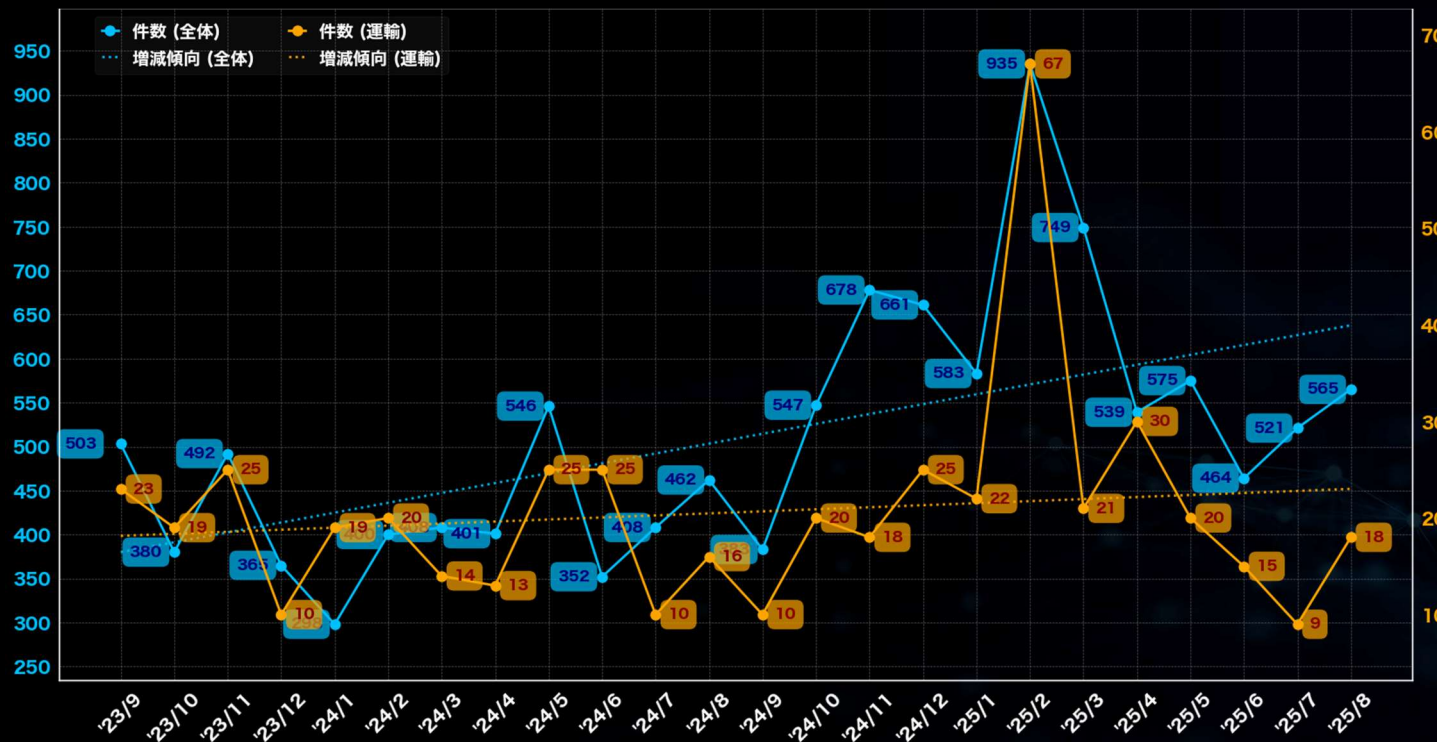
(※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる)

業種に関する分析 (全世界)

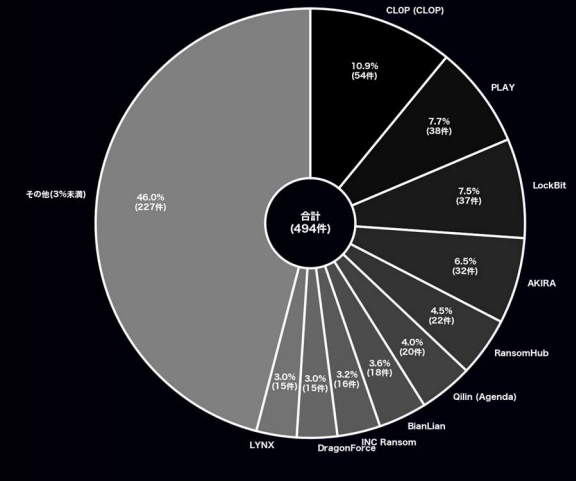
(過去2年間／2023年9月～2025年8月)

運輸

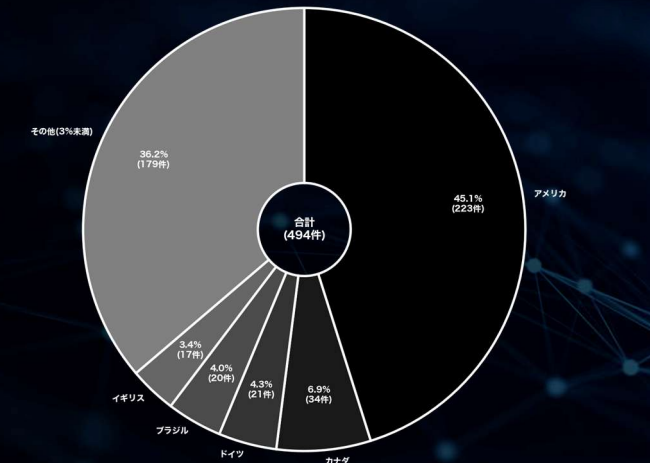
「運輸」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、67件の掲載があった。一方、最も少なかった月は2025年7月で9件であった。被害組織の所在国の割合では、アメリカが約45%と最も多く、次いでカナダとドイツがそれぞれ約7%と約4%である。攻撃グループについては、少なくとも85のグループが関与しており、特に「CLOP (CLOP)」が54件のリークサイト掲載を実施している。次いで「PLAY」と「LockBit」がそれぞれ38件と37件の掲載を行っている。運輸関係は全体件数に対する割合こそ低く、過去2年間では著し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)

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 :

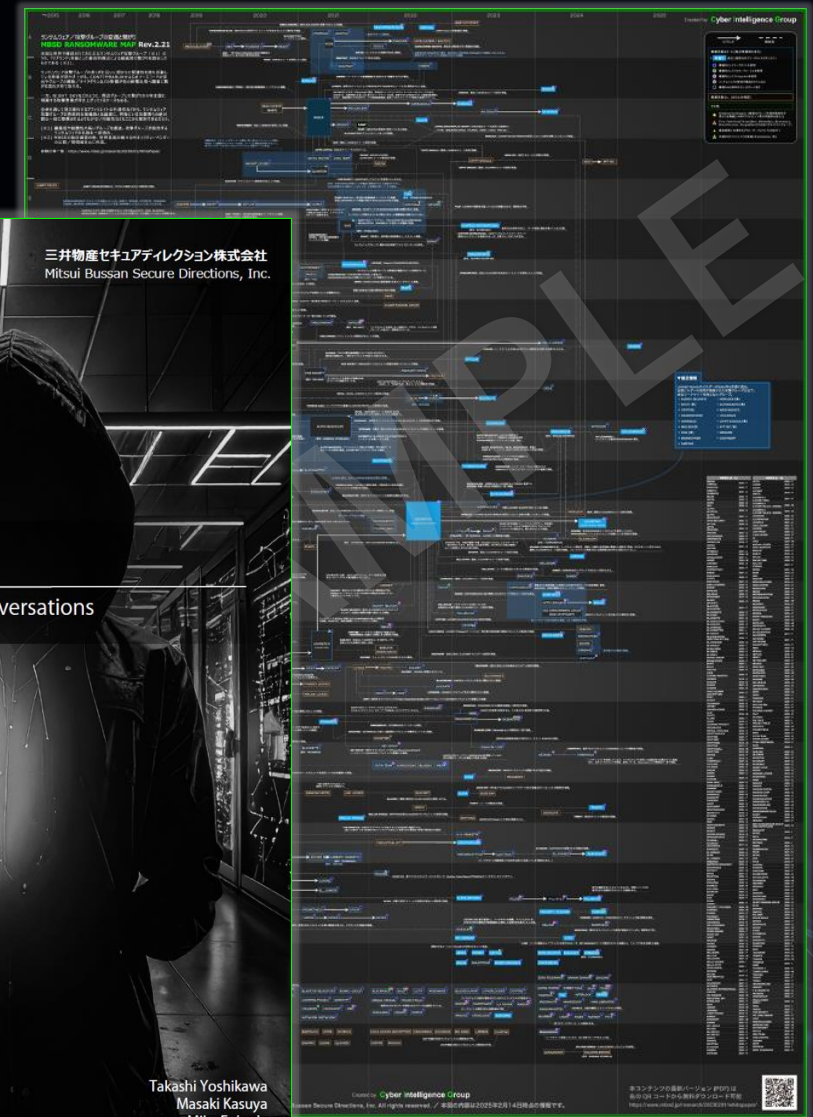
<https://www.mbsd.jp/research/cig/>

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

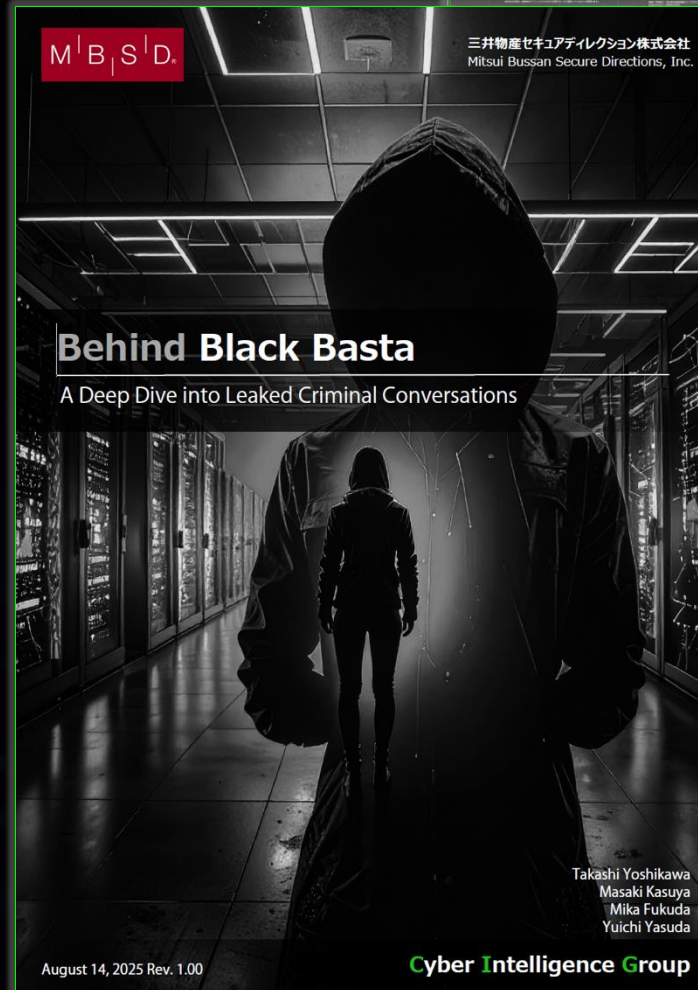
- 分析レポート :

<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