

暴露型ランサムウェア攻撃統計

CIGマンスリーレポート 2024年1月号 Rev 1.00
(2023年12月分)

2023

12



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）



Know your enemy.
Defense leadership.®

● 監視している攻撃グループの活動拠点 (※1)：140件

内2023年12月にリークサイト掲載を確認した活動拠点：37件

※1 リークサイトやTelegramなどを含む

● 監視中の攻撃グループの活動拠点一覧

8BASE	CiphBit	Endurance	MALAS	Pay2Key	Sabbath (54bb47h)
ABYSS	CipherLocker	EntropyI	MalekTeam	Payload.bin	shaoleaks
AKIRA	Cloak	Everest	MALLOX	PLAY	SIEGEDSEC
AlphV / BlackCat	CLOP	FSTeam	MBC	Prometheus	Snatch
ArvinClub	Conti	Grief	Medusa	PUTIN TEAM	Sparta Blog
Astro_Team	CoomingProject	Groove	MEOU	Pysa	Spook
AtomSilo	CROSSLOCK	Hitler Ransomware	Metaencryptor	Qilin	STORMOUS
Avaddon	CryptBB	Hive	Midas	Quantum	Suncrypt
AvosLocker	CRYPTNET	HolyGhost	Mindware	RA GROUP	SynACK (El_Cometa)
Axxes	CryptOn	HUNTERS INTERNATIONAL	MOISHA	Ragnar Locker	ThreeAM
Babuk	Cuba	ICEFIRE	Money Message	Ragnarok	TRIGONA
BianLian	DAIXIN	INC Ransom	Monti	Rancoz	UnSafe
Bl4ckt0r (BlackTor)	DarkAngels	Karakurt	Mount Locker	RANSOM_CORP	V IS VENDETTA
BlackBasta	DARKBIT	Karma Leaks	N3tw0rm	Ransomed.vc (Raznatovic)	Vice Society
BlackByte	DARKPOWER	Knight (Cyclops)	N4UGHTYSEC	RansomEXX	VSOP (Onyx)
BlackDolphin	DarkRace	LAMBDA	Nefilim	RansomHouse	WEREWOLVES
BLACKMAGIC	DarkRypt	LaPiovra	NightSky	RansomwareBlog	x001xs
BlackMatter	Darkside	LAPSUS\$	NoEscape	Ranzy (AKO)	XING Team
BLACKSHADOW	Donut Files	LILITH	Nokoyawa	RedAlert (N13V)	Yanluowang
BLACKSUIT	Donut Leaks	LockBit	NONAME1	Relic	Zeon
BLOODY	DoppelPaymer	Lorenz	NONAME2	Revil (Sodinokibi)	
BULLY	dotAdmin	LostTrust	Omega	Rhysida	
CACTUS	DragonForce	LV BLOG	Onyx (VSOP)	ROOK	
CHEERS	Dunghill	MADCAT	Pandora	Royal	

※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
 (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)
 ※ 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)を含む。
 ※ 業種分類や集計方法を含む本レポートの各データ(値)はMBSID独自の観測および集計結果となる。
 ※ 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る。
 ※ 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元に集計している。
 ※ 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む。
 ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● LockBitとの類似点が見られる新興攻撃グループ「WEREWOLVES」を確認

2023年12月に、新興グループ「WEREWOLVES」の活動拠点の存在を確認した。

この攻撃グループは、LockBitと重複する一部の被害組織をリークサイトに掲載している、攻撃にLockBit Green（CONTIから流出したランサムウェアビルダーから生成されたLockBitランサムウェア）の亜種を使用している、LockBitと同様にリークサイト上でバグバウンティプログラム（バグ発見報奨金プログラム）を呼びかけている、といった複数の観点でLockBitとの関係性や類似点が見られることから、一部ではLockBitのアフィリエイトが関わっている可能性などを指摘する声もある。

また、リークサイトに掲載されている被害組織は、LockBitとの重複組織を省くと複数のロシア関連組織のみである点も興味深い。

● AlphV / BlackCatがテイクダウン後まもなく活動を再開

AlphV / BlackCatのリークサイトは日本時間2023/12/07の13時頃に一時ダウンを確認していたが、その後一部復帰し新規投稿が見られたものの、過去の暴露データが表示されないなど不安定な状況が続いていた。その後、2023/12/19 21時頃に法執行機関による差し押さえ画面に変化。まもなくアメリカ合衆国司法省から法執行機関の国際グループと協力してAlphV / BlackCatのリークサイトをテイクダウン（差し押さえ）したことが発表された。しかしその数時間後に、AlphV / BlackCatによって「このサイトは未押収です」という表示に同サイトが再び書き換えられ、一連の経緯の説明と共に、「FBIが入手したキーは一部の被害組織のみに関わるもので他の3000以上の攻撃には影響しない。今回の経験を反省し新しい攻撃ルールで厳格に活動を続ける」という攻撃者側の主張に一転して書き戻された。AlphV / BlackCatはその後、差し押さへの影響を受けていないミラーサイトへ移行、現在も継続的に被害組織が掲載されており、12月末には日本関連組織への攻撃声明の掲載も確認している。

● 引き続き複数の新興攻撃グループの出現や新たな活動拠点を確認

今月はWEREWOLVESの他に、DragonForce、Raznatovic、その他ハクティビストを含む複数の新興グループの出現や活動をj確認している。

DragonForceは地域、業種に関わらず様々な組織への攻撃を主張しており、その中には一部日本関連組織も含まれる。Raznatovicは大手国内組織への攻撃を主張したRansomed.vcがリブランドした攻撃グループである。このグループは2023年11月に活動停止を主張していたものの、2023年12月に入りRaznatovicとして活動を継続することを示唆する文章をリークサイト上に掲載した。その後、ペネトレーション・テスターの宣伝や流出データのオークションサイトなどに活動スタイルを変え模索している状況があり、2024年1月現在においては、前身のRansomed.vcの時に行っていた"窃取データの情報流出"を前面に出した恐喝手法とは若干毛色を変え、EU GDPR（EU一般データ保護規則）違反に言及したうえで、「違反の通報」と引き換えに対価を要求する恐喝を行っている。

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る。ぜひとも皆様の脅威情報の把握にご活用頂ければ幸いです。

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

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

※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。

（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）

※ 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）を含む。

※ 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独自の観測および集計結果となる。

※ 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る。

※ 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元に集計している。

※ 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む。

※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。

※ 集計方法の変更や、時間が長期経過し公開／公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

年間統計

(全世界)

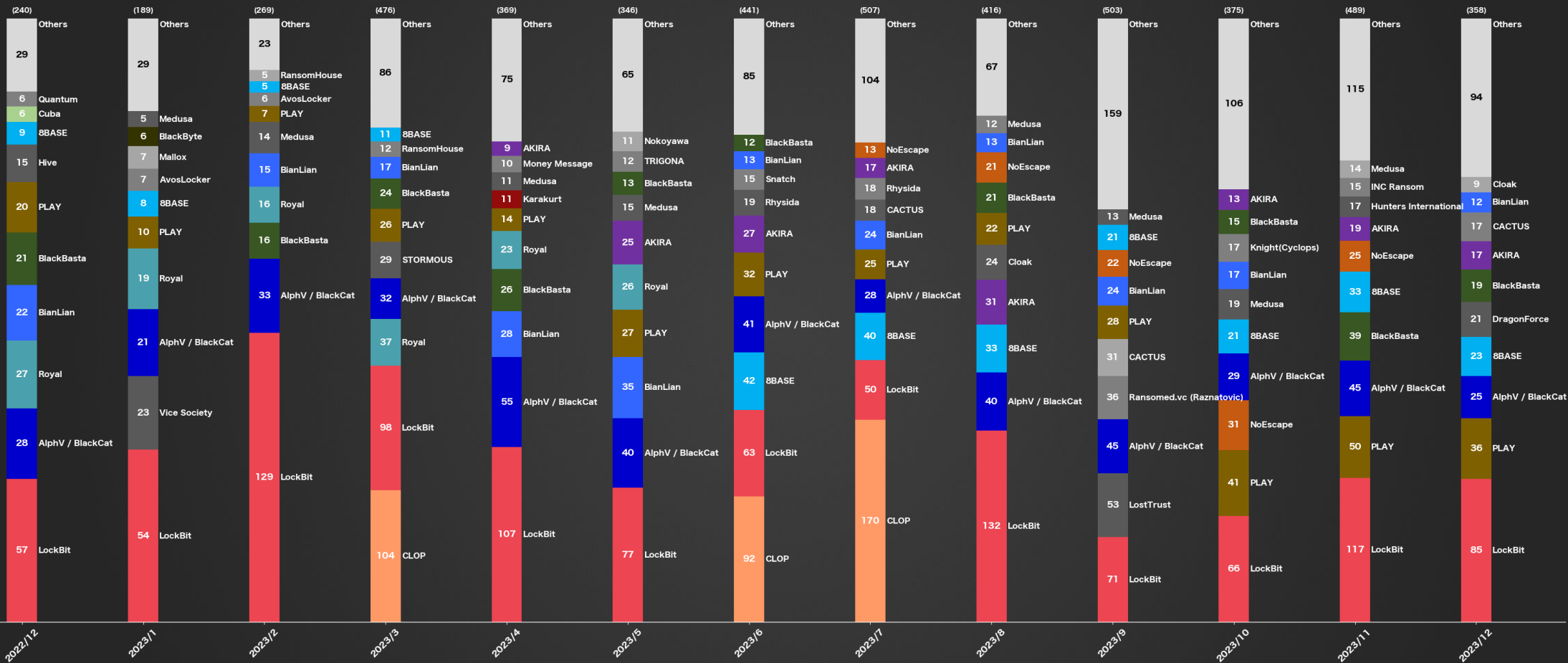
2023

12

- ※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
(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)
- ※ 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)を含む。
- ※ 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独自の観測および集計結果となる。
- ※ これらはい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る。
- ※ 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元に集計している。
- ※ 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む。
- ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
- ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 攻撃グループ割合で見る被害数の年間統計 (2022年12月~2023年12月 / 全世界) (MBSD調べ)

※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。



※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
 (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)
 ※ 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)を含む。
 ※ 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独自の観測および集計結果となる。
 ※ 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る。
 ※ 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元に集計している。
 ※ 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む。
 ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

2023

12

攻撃グループ 月別統計

(全世界) (過去3ヶ月分)

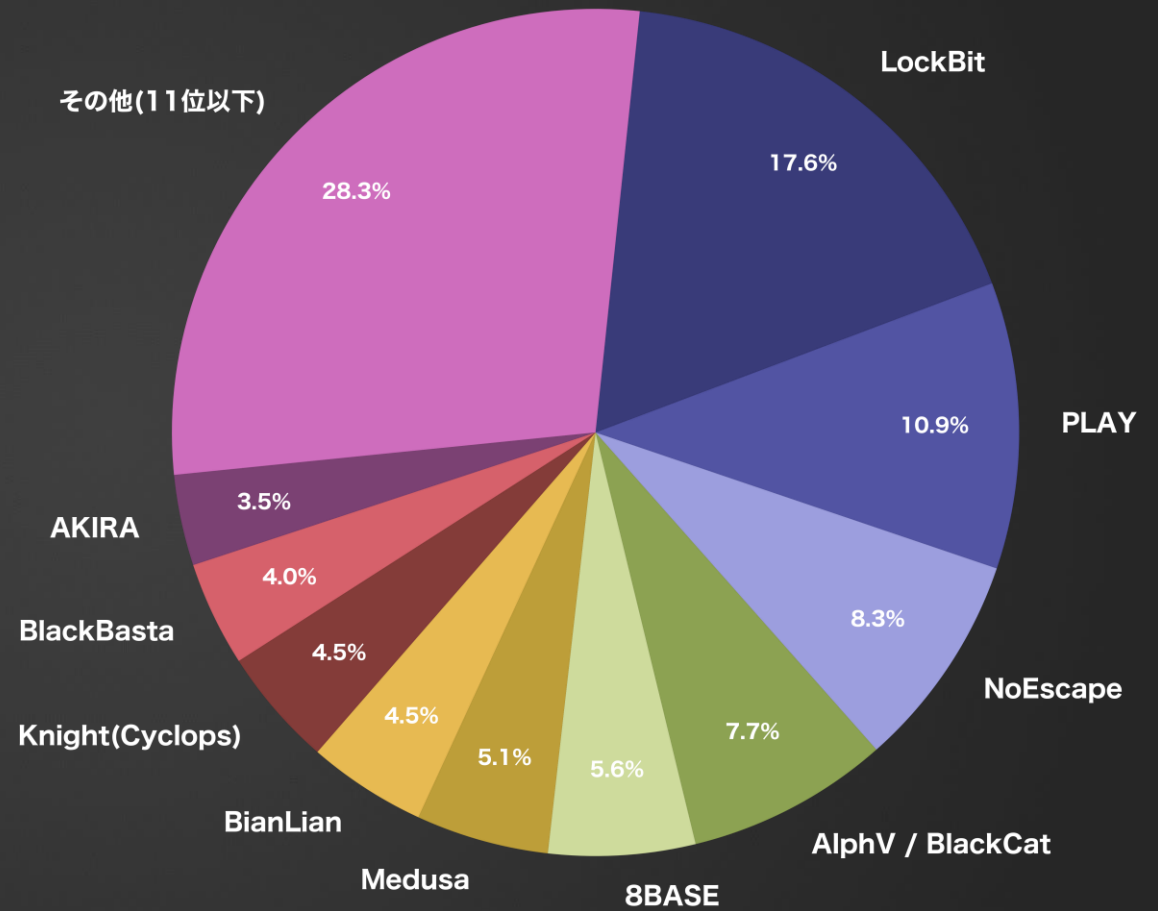
- ※ 特に注釈がない場合は、リークサイトに掲載された数に揃えた値とする。
(日本にフォーカスした一部の表/グラフのみ、公表や報道から判明した数を加味し集計)
- ※ 国内被害組織に関する各種データについては、海外拠点(支社/関連会社)を含む。
- ※ 業種分類や集計方法を含む本レポートの各データ(値)はMBSD独自の観測および集計結果となる。
- ※ これらはあくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
- ※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
- ※ ごく一部のランサムウェアの使用が明確に確認されていない暴露&恐喝グループの値も含む。
- ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
- ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 月別内訳 攻撃グループ TOP10 (2023年 10月 / 全世界) (MBSD調べ)

※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)
LockBit	66	17.6	- 5
PLAY	41	10.9	+ 13
NoEscape	31	8.3	+ 9
AlphV / BlackCat	29	7.7	- 16
8BASE	21	5.6	± 0
Medusa	19	5.1	+ 6
BianLian	17	4.5	- 7
Knight(Cyclops)	17	4.5	+ 6
BlackBasta	15	4.0	+ 12
AKIRA	13	3.5	+ 4

▼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)



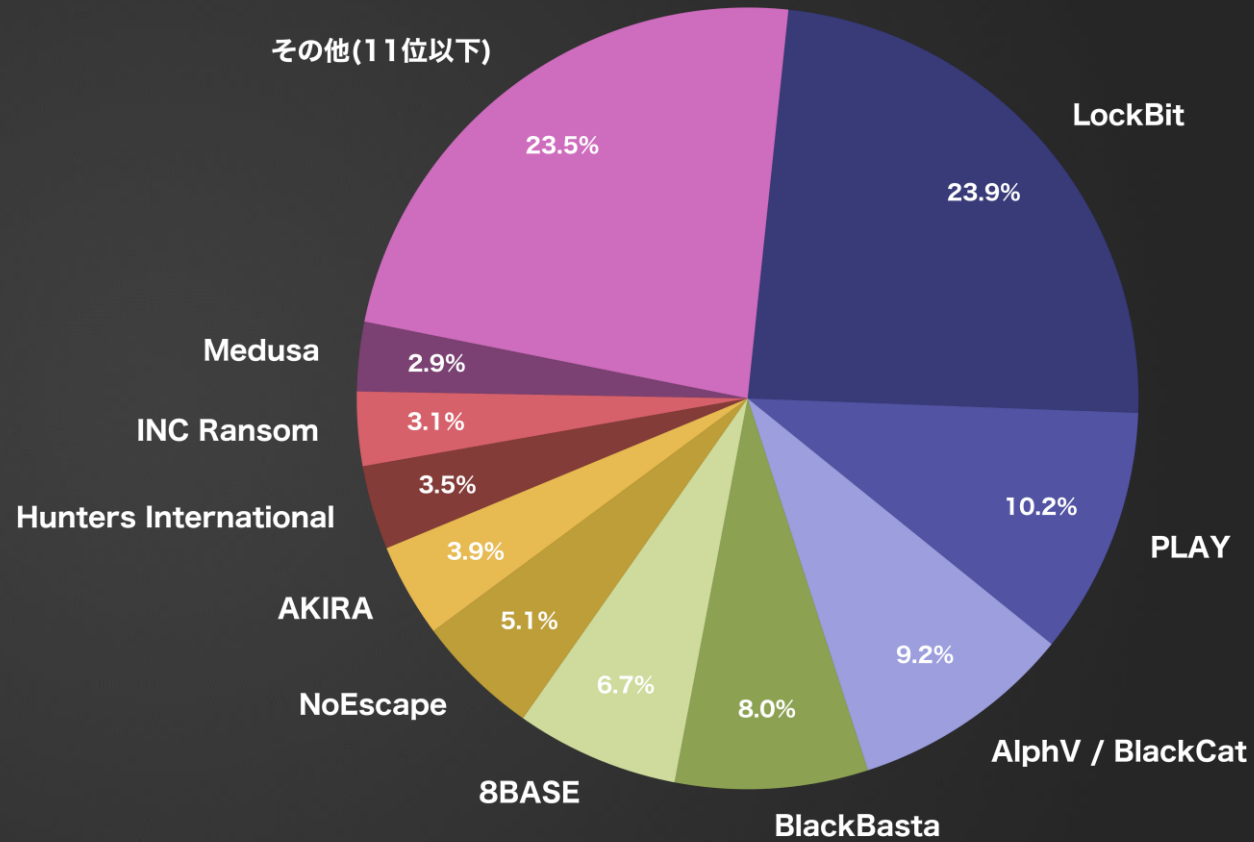
※特に注釈がない場合は、リークサイトに掲載された数に揃えた値とする。
 (日本にフォーカスした一部の表/グラフのみ、公表や報道から判明した数を加味し集計)
 ※国内被害組織に関する各種データについては、海外拠点(支社/関連会社)を含む。
 ※業種分類や集計方法を含む本レポートの各データ(値)はMBSD独自の観測および集計結果となる。
 ※これらはいくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
 ※攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
 ※ごく一部のランサムウェアの使用が明確に確認されていない暴露&恐喝グループの値も含む。
 ※攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 月別内訳 攻撃グループ TOP10 (2023年 11月 / 全世界) (MBSD調べ)

※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)
LockBit	117	23.9	+ 51
PLAY	50	10.2	+ 9
AlphV / BlackCat	45	9.2	+ 16
BlackBasta	39	8.0	+ 24
8BASE	33	6.7	+ 12
NoEscape	25	5.1	- 6
AKIRA	19	3.9	+ 6
Hunters International	17	3.5	+ 15
INC Ransom	15	3.1	+ 5
Medusa	14	2.9	- 5

▼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)



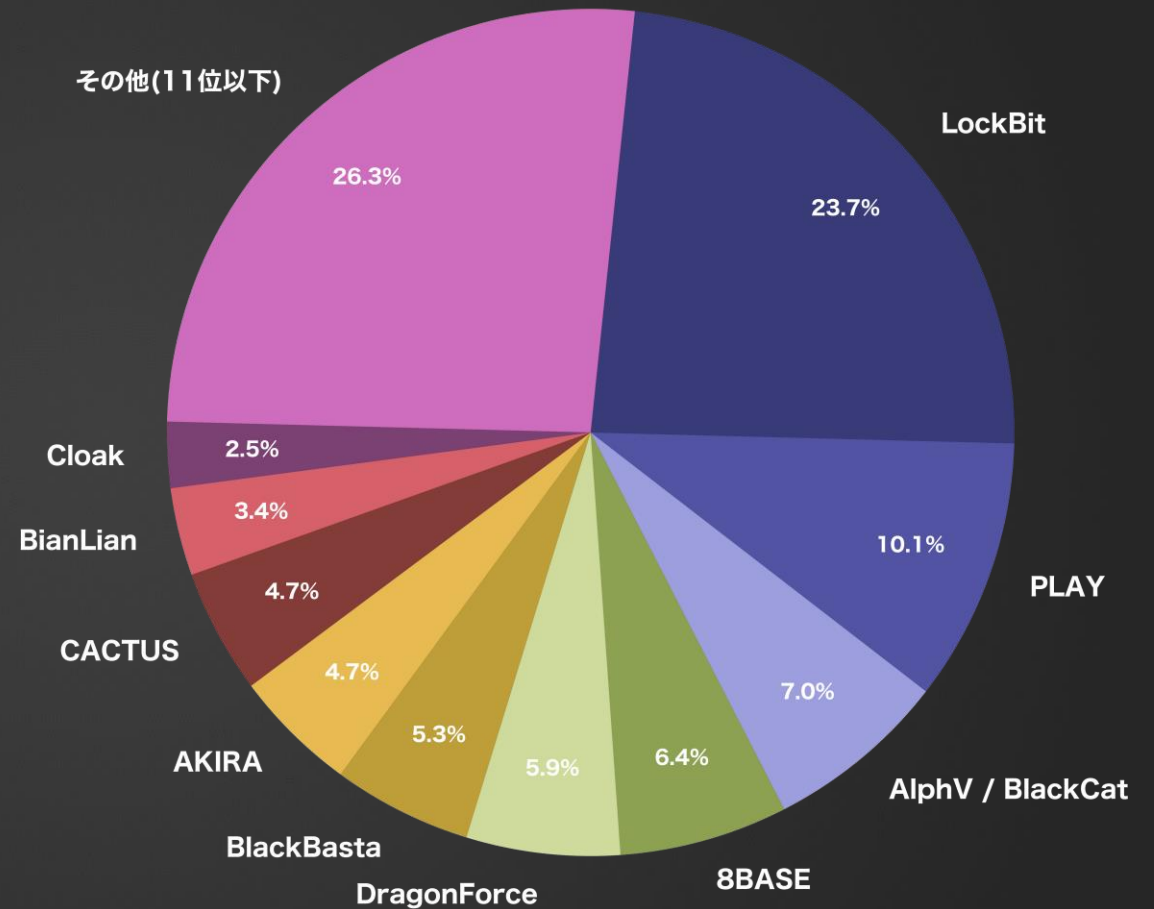
※特に注釈がない場合は、リークサイトに掲載された数に揃えた値とする。
 (日本にフォーカスした一部の表/グラフのみ、公表や報道から判明した数を加味し集計)
 ※国内被害組織に関する各種データについては、海外拠点(支社/関連会社)を含む。
 ※業種分類や集計方法を含む本レポートの各データ(値)はMBSD独自の観測および集計結果となる。
 ※これらはあくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
 ※攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
 ※ごく一部のランサムウェアの使用が明確に確認されていない暴露&恐喝グループの値も含む。
 ※攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 月別内訳 攻撃グループ TOP10 (2023年 12月 / 全世界) (MBSD調べ)

※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)
LockBit	85	23.7	- 32
PLAY	36	10.1	- 14
AlphV / BlackCat	25	7.0	- 20
8BASE	23	6.4	- 10
DragonForce	21	5.9	+ 21
BlackBasta	19	5.3	- 20
AKIRA	17	4.7	- 2
CACTUS	17	4.7	+ 7
BianLian	12	3.4	- 1
Cloak	9	2.5	+ 9

▼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)



※特に注釈がない場合は、リークサイトに掲載された数に揃えた値とする。
 (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)
 ※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)を含む。
 ※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独自の観測および集計結果となる。
 ※これらはい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る。
 ※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元に集計している。
 ※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む。
 ※攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

2023

12

被害国 月別統計

(全世界) (過去3ヶ月分)

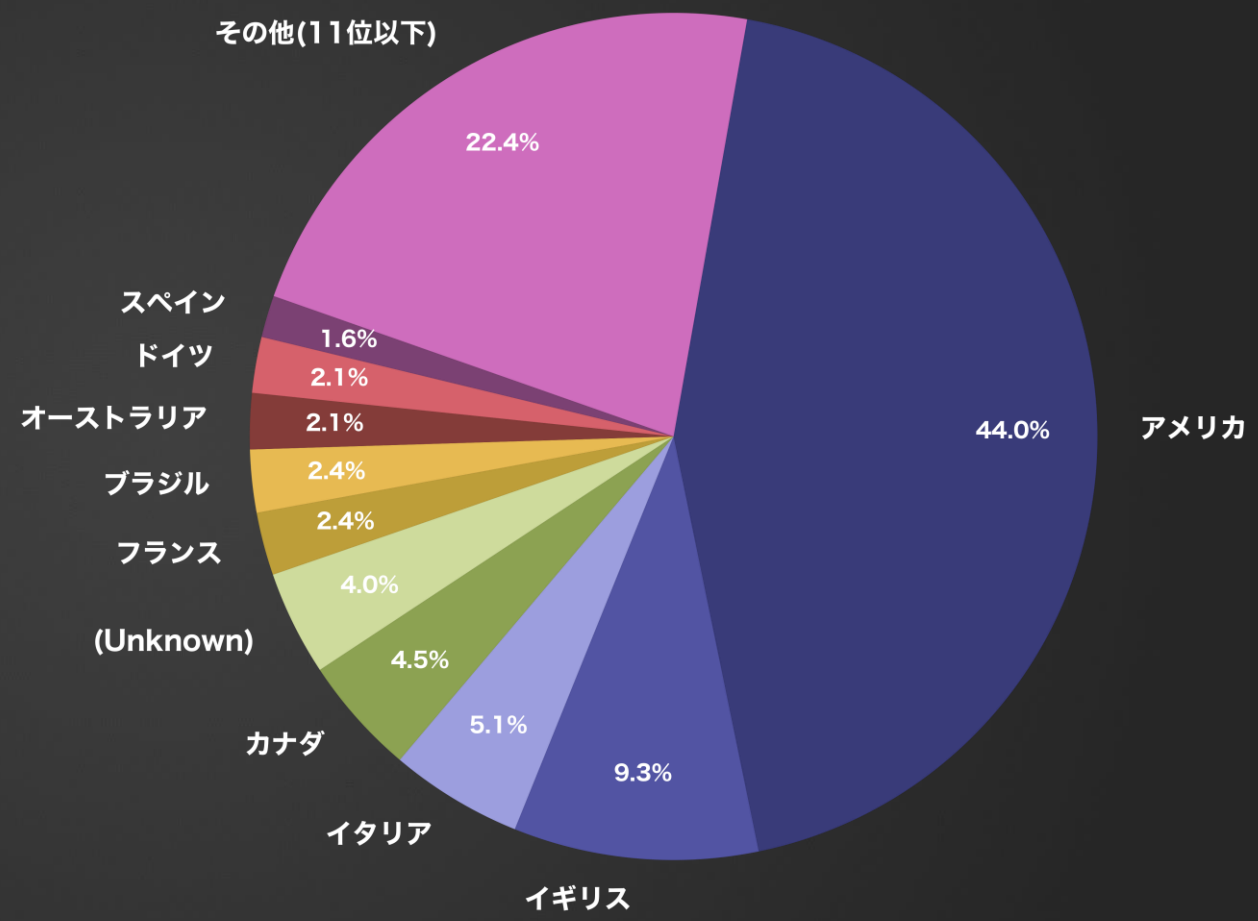
- ※ 特に注釈がない場合は、リークサイトに掲載された数に揃えた値とする。
(日本にフォーカスした一部の表/グラフのみ、公表や報道から判明した数を加味し集計)
- ※ 国内被害組織に関する各種データについては、海外拠点(支社/関連会社)を含む。
- ※ 業種分類や集計方法を含む本レポートの各データ(値)はMBSD独自の観測および集計結果となる。
- ※ これらはいくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
- ※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
- ※ ごく一部のランサムウェアの使用が明確に確認されていない暴露&恐喝グループの値も含む。
- ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
- ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 月別内訳 被害国TOP10 (2023年 10月 / 全世界) (MBSD調べ)

※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	165	44.0	- 68
イギリス	35	9.3	+ 8
イタリア	19	5.1	+ 8
カナダ	17	4.5	- 5
(Unknown)	15	4.0	- 9
フランス	9	2.4	- 9
ブラジル	9	2.4	+ 2
オーストラリア	8	2.1	- 4
ドイツ	8	2.1	- 8
スペイン	6	1.6	- 2

▼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)



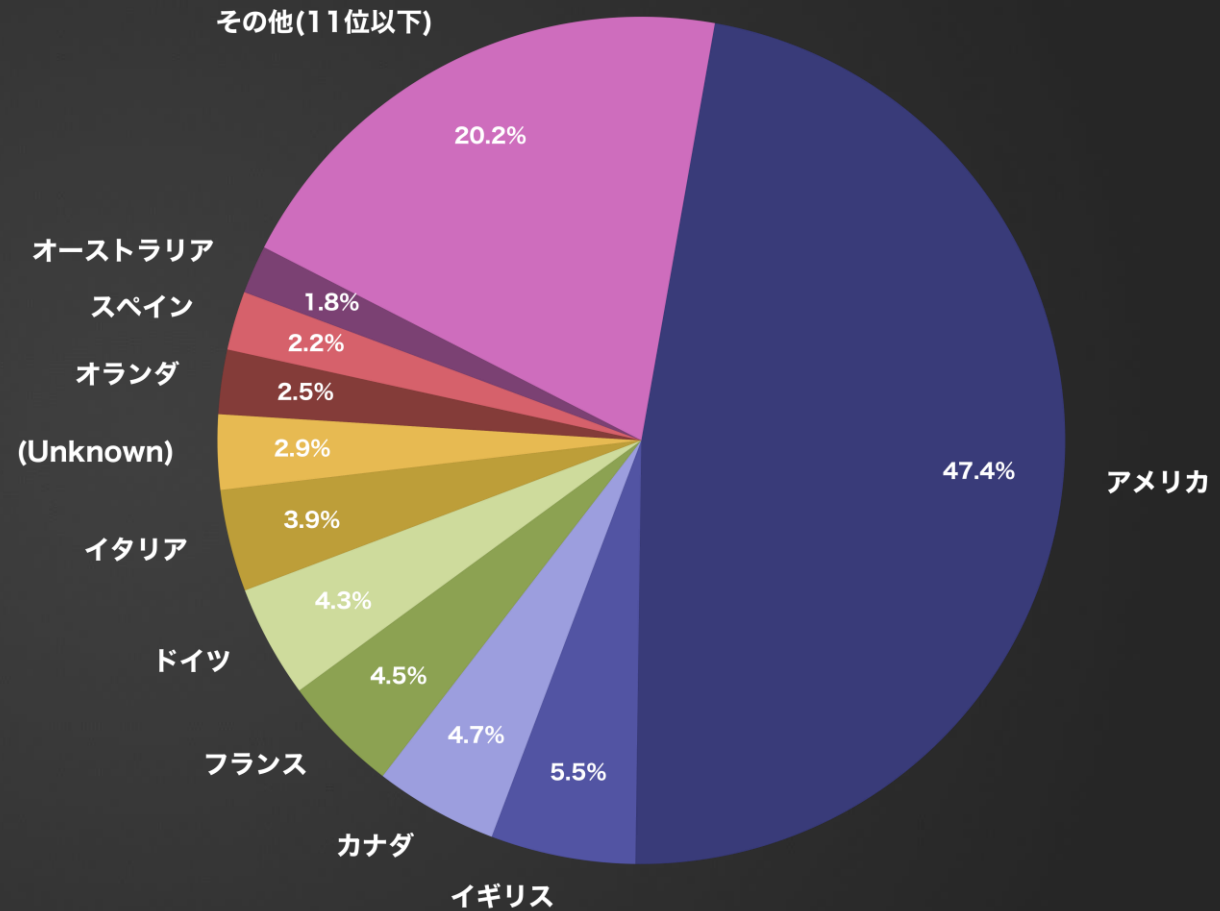
※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
 (日本にフォーカスした一部の表/グラフのみ、公表や報道から判明した数を加味し集計)
 ※ 国内被害組織に関する各種データについては、海外拠点(支社/関連会社)を含む。
 ※ 業種分類や集計方法を含む本レポートの各データ(値)はMBSD独自の観測および集計結果となる。
 ※ これらはいくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
 ※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
 ※ ごく一部のランサムウェアの使用が明確に確認されていない暴露&恐喝グループの値も含む。
 ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 月別内訳 被害国TOP10 (2023年 **11月** / **全世界**) (MBSD調べ)

※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	232	47.4	+ 67
イギリス	27	5.5	- 8
カナダ	23	4.7	+ 6
フランス	22	4.5	+ 13
ドイツ	21	4.3	+ 13
イタリア	19	3.9	± 0
(Unknown)	14	2.9	- 1
オランダ	12	2.5	+ 9
スペイン	11	2.2	+ 5
オーストラリア	9	1.8	+ 1

▼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)



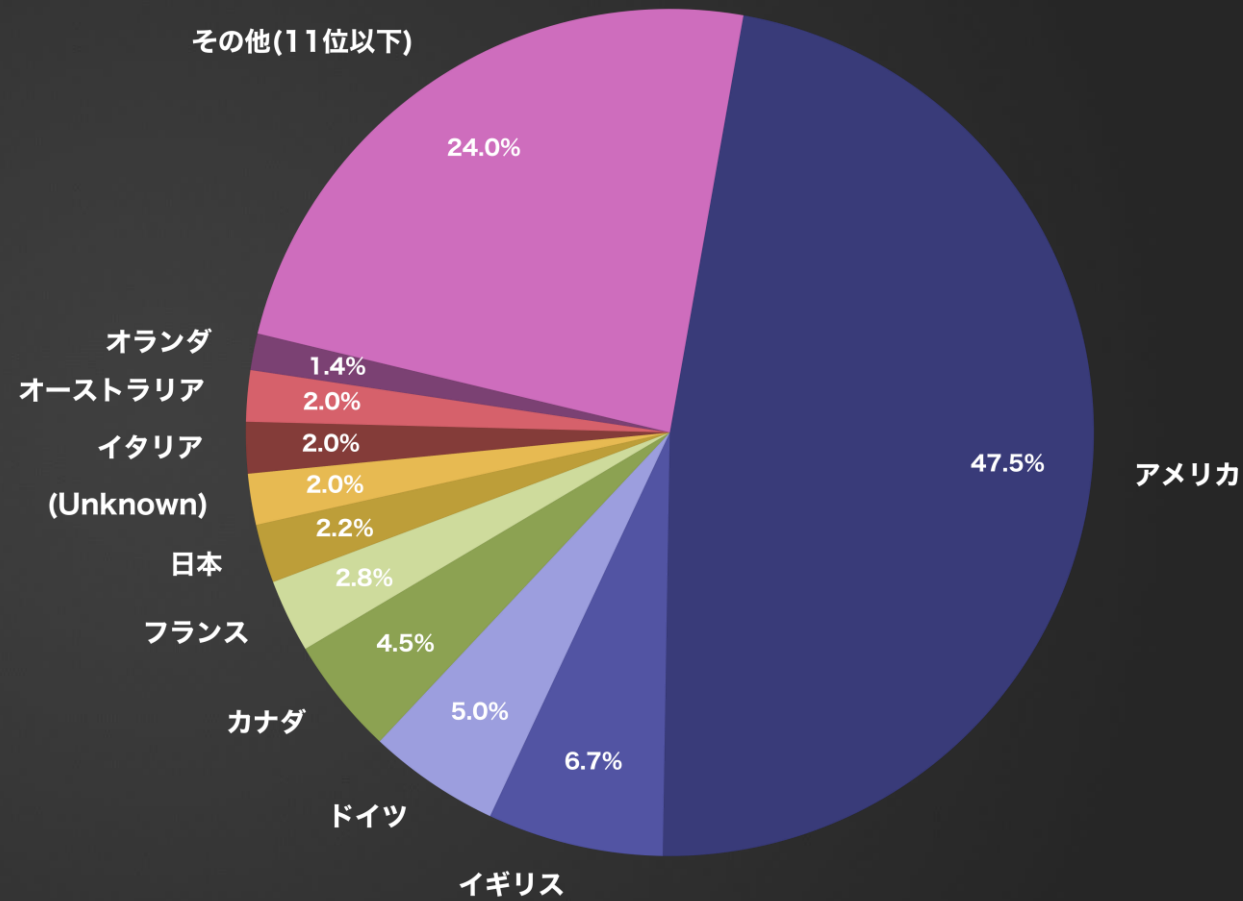
※特に注釈がない場合は、リークサイトに掲載された数に揃えた値とする。
 (日本にフォーカスした一部の表/グラフのみ、公表や報道から判明した数を加味し集計)
 ※国内被害組織に関する各種データについては、海外拠点(支社/関連会社)を含む。
 ※業種分類や集計方法を含む本レポートの各データ(値)はMBSD独自の観測および集計結果となる。
 ※これらはいくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
 ※攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
 ※ごく一部のランサムウェアの使用が明確に確認されていない暴露&恐喝グループの値も含む。
 ※攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 月別内訳 被害国TOP10 (2023年 **12**月 / **全世界**) (MBSD調べ)

※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	170	47.5	- 61
イギリス	24	6.7	- 3
ドイツ	18	5.0	- 3
カナダ	16	4.5	- 7
フランス	10	2.8	- 12
日本	8	2.2	+ 3
(Unknown)	7	2.0	- 7
イタリア	7	2.0	- 12
オーストラリア	7	2.0	- 2
オランダ	5	1.4	- 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)



※ 特に注釈がない場合は、リークサイトに掲載された数に揃えた値とする。
 (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)
 ※ 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)を含む。
 ※ 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独自の観測および集計結果となる。
 ※ これらはい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る。
 ※ 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元に集計している。
 ※ 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む。
 ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

2023

12

被害国 月別統計

(アジア) (過去3ヶ月分)

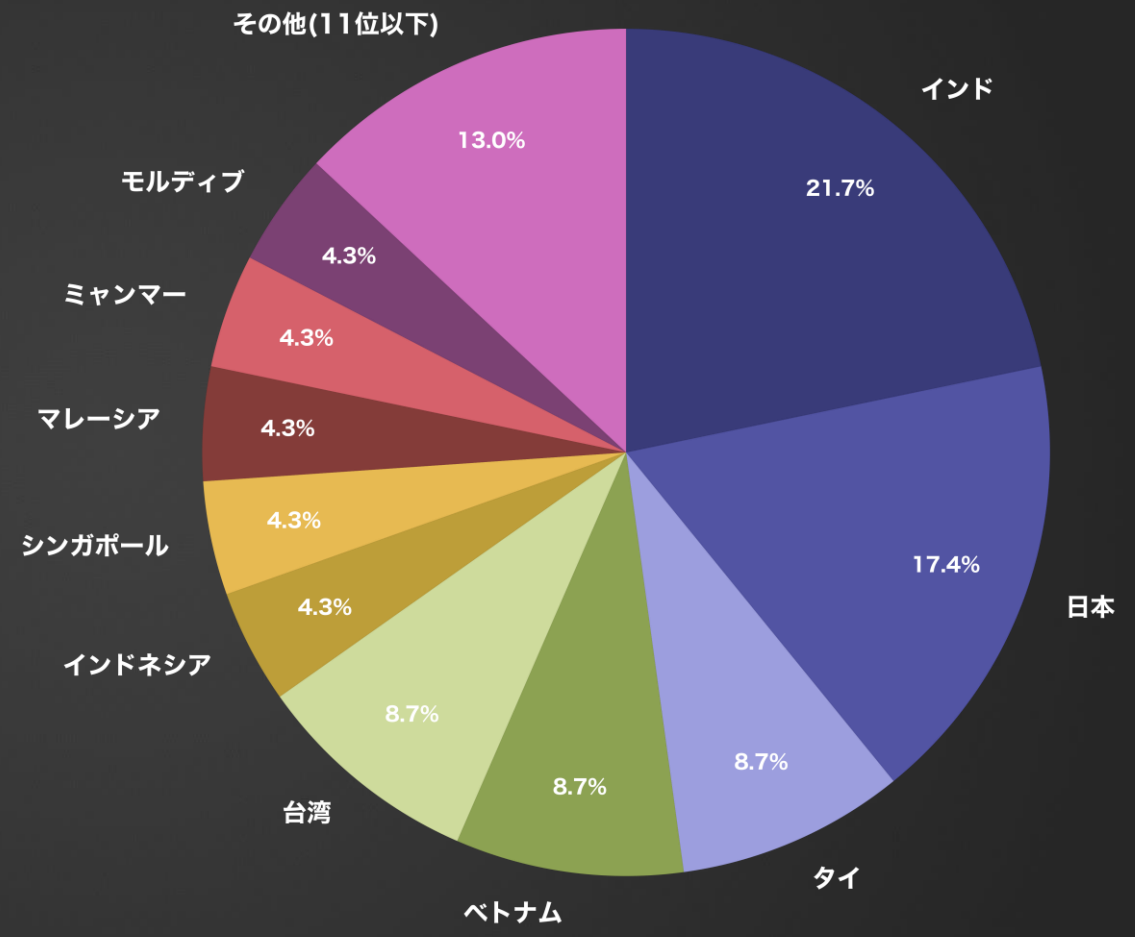
- ※ 特に注釈がない場合は、リークサイトに掲載された数に揃えた値とする。
(日本にフォーカスした一部の表/グラフのみ、公表や報道から判明した数を加味し集計)
- ※ 国内被害組織に関する各種データについては、海外拠点(支社/関連会社)を含む。
- ※ 業種分類や集計方法を含む本レポートの各データ(値)はMBSD独自の観測および集計結果となる。
- ※ これらはいくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
- ※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
- ※ ごく一部のランサムウェアの使用が明確に確認されていない暴露&恐喝グループの値も含む。
- ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
- ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 月別内訳 被害国TOP10 (2023年 **10月** / **アジア**) (MBSD調べ)

※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	5	21.7	+ 5
日本	4	17.4	- 7
タイ	2	8.7	- 1
ベトナム	2	8.7	± 0
台湾	2	8.7	+ 2
インドネシア	1	4.3	± 0
シンガポール	1	4.3	- 3
マレーシア	1	4.3	± 0
ミャンマー	1	4.3	+ 1
モルディブ	1	4.3	+ 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)



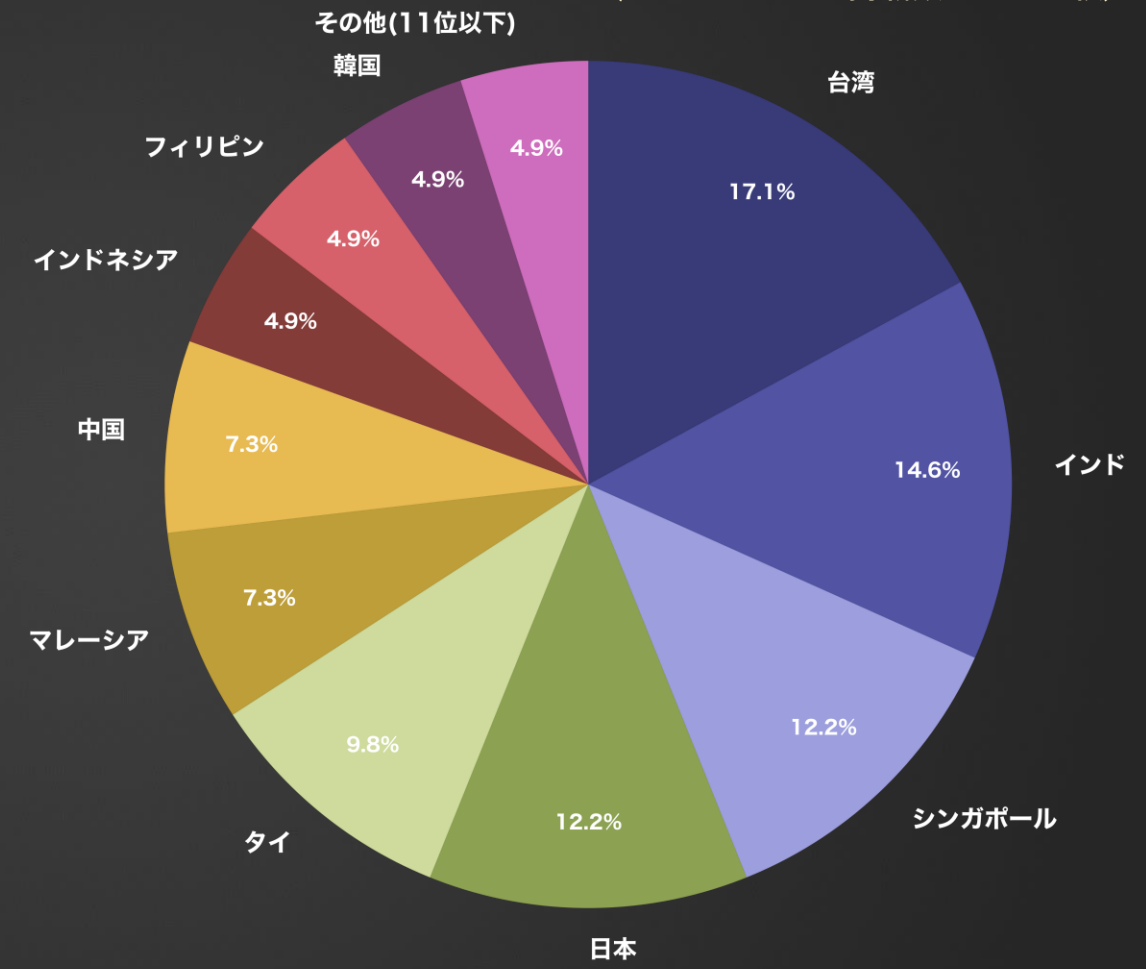
※ 特に注釈がない場合は、リークサイトに掲載された数に揃えた値とする。
 (日本にフォーカスした一部の表/グラフのみ、公表や報道から判明した数を加味し集計)
 ※ 国内被害組織に関する各種データについては、海外拠点(支社/関連会社)を含む。
 ※ 業種分類や集計方法を含む本レポートの各データ(値)はMBSD独自の観測および集計結果となる。
 ※ これらはいくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
 ※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
 ※ ごく一部のランサムウェアの使用が明確に確認されていない暴露&恐喝グループの値も含む。
 ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 月別内訳 被害国TOP10 (2023年 11月 / アジア) (MBSID調べ)

※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。

▼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)

国名	件数	割合(%)	前月比(件数)
台湾	7	17.1	+ 5
インド	6	14.6	+ 1
シンガポール	5	12.2	+ 4
日本	5	12.2	+ 1
タイ	4	9.8	+ 2
マレーシア	3	7.3	+ 2
中国	3	7.3	+ 2
インドネシア	2	4.9	+ 1
フィリピン	2	4.9	+ 2
韓国	2	4.9	+ 1



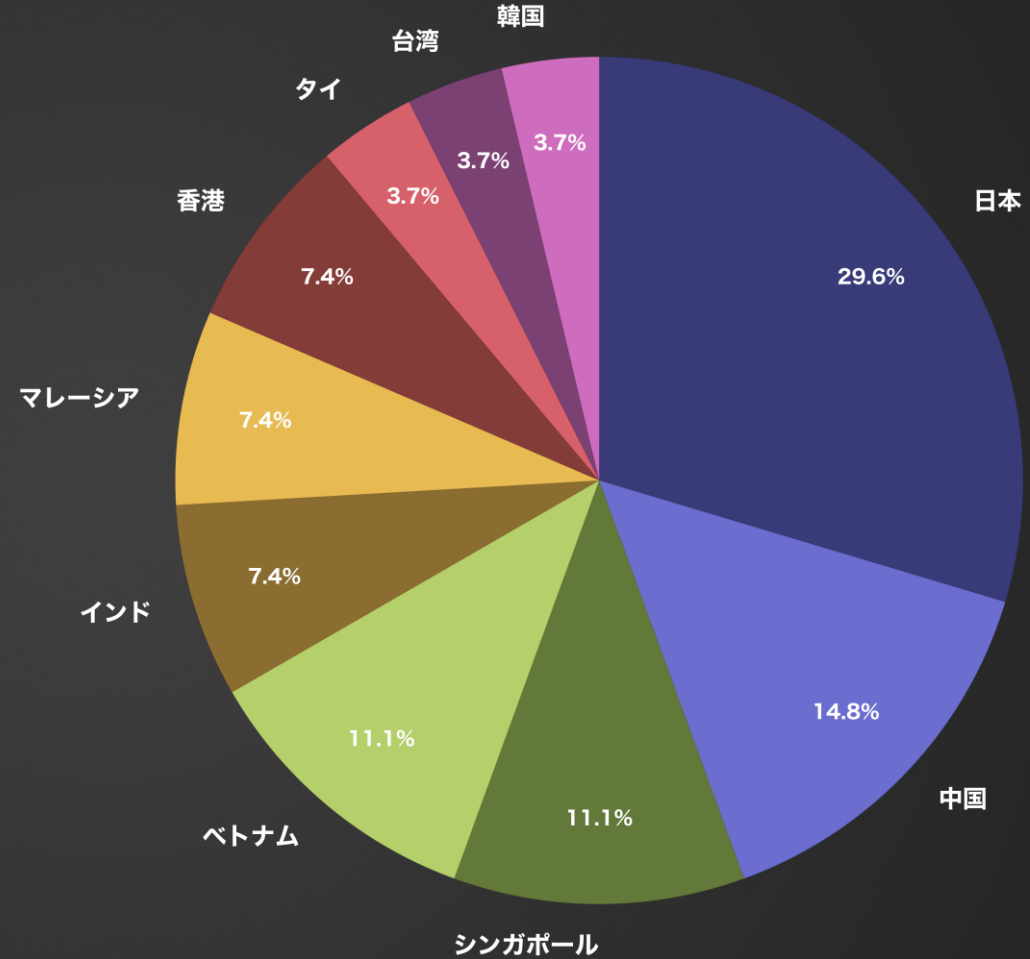
※ 特に注釈がない場合は、リークサイトに掲載された数に揃えた値とする。
 (日本にフォーカスした一部の表/グラフのみ、公表や報道から判明した数を加味し集計)
 ※ 国内被害組織に関する各種データについては、海外拠点(支社/関連会社)を含む。
 ※ 業種分類や集計方法を含む本レポートの各データ(値)はMBSID独自の観測および集計結果となる。
 ※ これらはいくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
 ※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
 ※ ごく一部のランサムウェアの使用が明確に確認されていない暴露&恐喝グループの値も含む。
 ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 月別内訳 被害国TOP10 (2023年 12月 / アジア) (MBSID調べ)

※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	8	29.6	+ 3
中国	4	14.8	+ 1
シンガポール	3	11.1	- 2
ベトナム	3	11.1	+ 3
インド	2	7.4	- 4
マレーシア	2	7.4	- 1
香港	2	7.4	+ 1
タイ	1	3.7	- 3
台湾	1	3.7	- 6
韓国	1	3.7	- 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)



※ 特に注釈がない場合は、リークサイトに掲載された数に揃えた値とする。
 (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)
 ※ 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)を含む。
 ※ 業種分類や集計方法を含む本レポートの各データ(値)はMBSID独自の観測および集計結果となる。
 ※ これらはい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る。
 ※ 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元に集計している。
 ※ 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む。
 ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

2023

12

業種 月別統計

(全世界) (過去3ヶ月分)

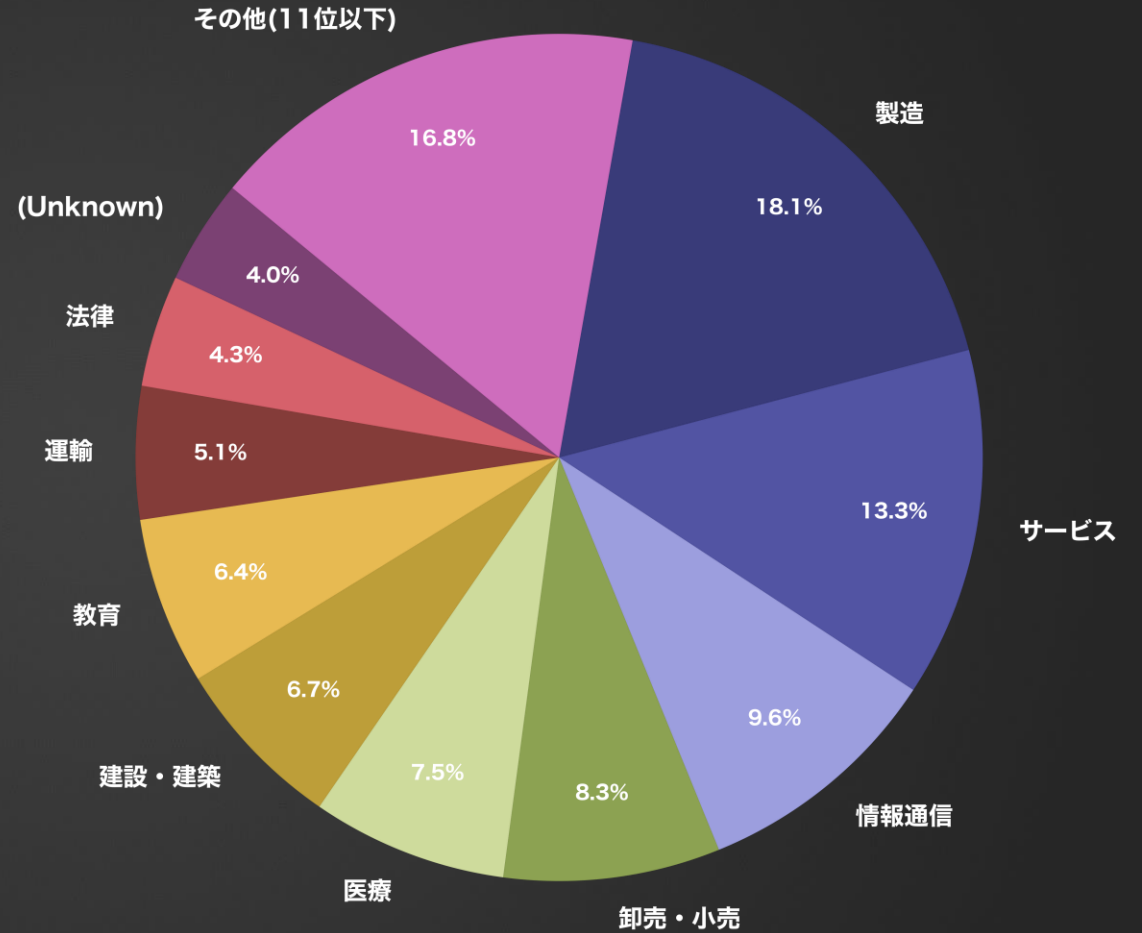
- ※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
(日本にフォーカスした一部の表/グラフのみ、公表や報道から判明した数を加味し集計)
- ※ 国内被害組織に関する各種データについては、海外拠点(支社/関連会社)を含む。
- ※ 業種分類や集計方法を含む本レポートの各データ(値)はMBSD独自の観測および集計結果となる。
- ※ これらはいくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
- ※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
- ※ ごく一部のランサムウェアの使用が明確に確認されていない暴露&恐喝グループの値も含む。
- ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
- ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 月別内訳 業種 TOP10 (2023年 10月 / 全世界) (MBSD調べ)

※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	68	18.1	- 4
サービス	50	13.3	- 2
情報通信	36	9.6	- 8
卸売・小売	31	8.3	- 13
医療	28	7.5	- 9
建設・建築	25	6.7	- 21
教育	24	6.4	+ 1
運輸	19	5.1	- 4
法律	16	4.3	- 9
(Unknown)	15	4.0	- 7

▼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)



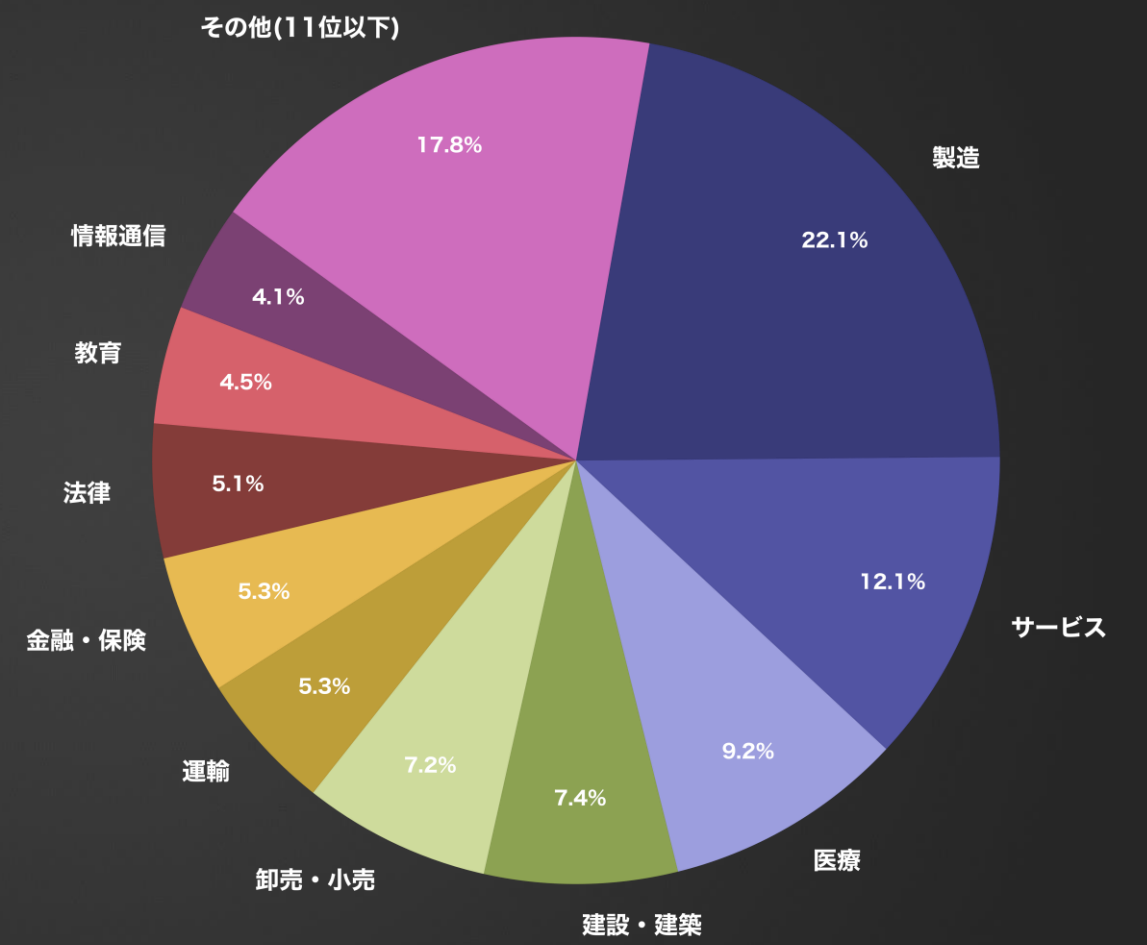
※ 特に注釈がない場合は、リークサイトに掲載された数に揃えた値とする。
 (日本にフォーカスした一部の表/グラフのみ、公表や報道から判明した数を加味し集計)
 ※ 国内被害組織に関する各種データについては、海外拠点(支社/関連会社)を含む。
 ※ 業種分類や集計方法を含む本レポートの各データ(値)はMBSD独自の観測および集計結果となる。
 ※ これらはいくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
 ※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
 ※ ごく一部のランサムウェアの使用が明確に確認されていない暴露&恐喝グループの値も含む。
 ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 月別内訳 業種 TOP10 (2023年 11月 / 全世界) (MBSD調べ)

※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	108	22.1	+ 40
サービス	59	12.1	+ 9
医療	45	9.2	+ 17
建設・建築	36	7.4	+ 11
卸売・小売	35	7.2	+ 4
運輸	26	5.3	+ 7
金融・保険	26	5.3	+ 16
法律	25	5.1	+ 9
教育	22	4.5	- 2
情報通信	20	4.1	- 16

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



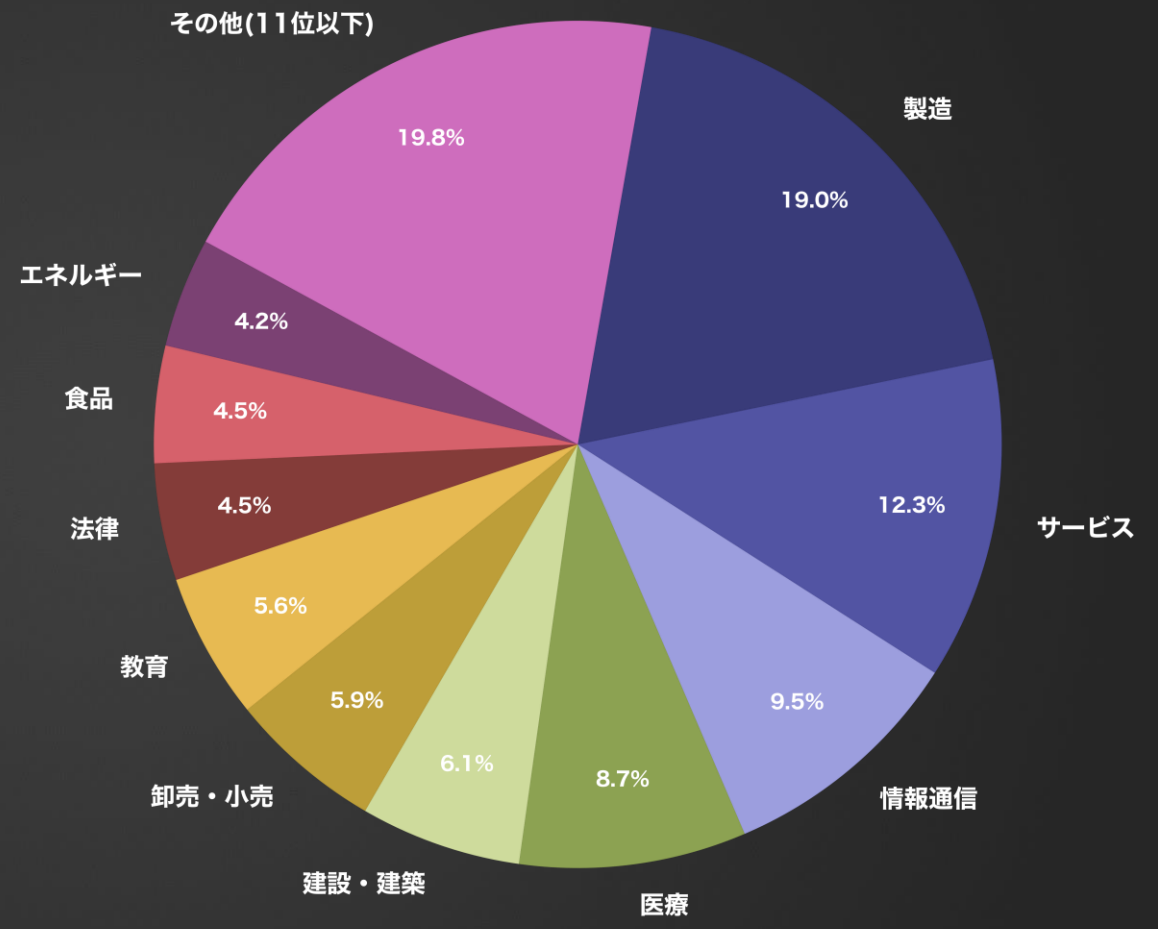
※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
 (日本にフォーカスした一部の表/グラフのみ、公表や報道から判明した数を加味し集計)
 ※ 国内被害組織に関する各種データについては、海外拠点(支社/関連会社)を含む。
 ※ 業種分類や集計方法を含む本レポートの各データ(値)はMBSD独自の観測および集計結果となる。
 ※ これらはいくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
 ※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
 ※ ごく一部のランサムウェアの使用が明確に確認されていない暴露&恐喝グループの値も含む。
 ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 月別内訳 業種 TOP10 (2023年 12月 / 全世界) (MBSD調べ)

※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	68	19.0	- 40
サービス	44	12.3	- 14
情報通信	34	9.5	+ 14
医療	31	8.7	- 14
建設・建築	22	6.1	- 14
卸売・小売	21	5.9	- 14
教育	20	5.6	- 2
法律	16	4.5	- 9
食品	16	4.5	± 0
エネルギー	15	4.2	+ 9

▼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)



※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
 (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)
 ※ 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)を含む。
 ※ 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独自の観測および集計結果となる。
 ※ 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る。
 ※ 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元に集計している。
 ※ 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む。
 ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

2023

12

被害数の推移に関する統計

(全世界及び国内)

- ※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
(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)
- ※ 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)を含む。
- ※ 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独自の観測および集計結果となる。
- ※ これらはい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る。
- ※ 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元に集計している。
- ※ 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む。
- ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
- ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

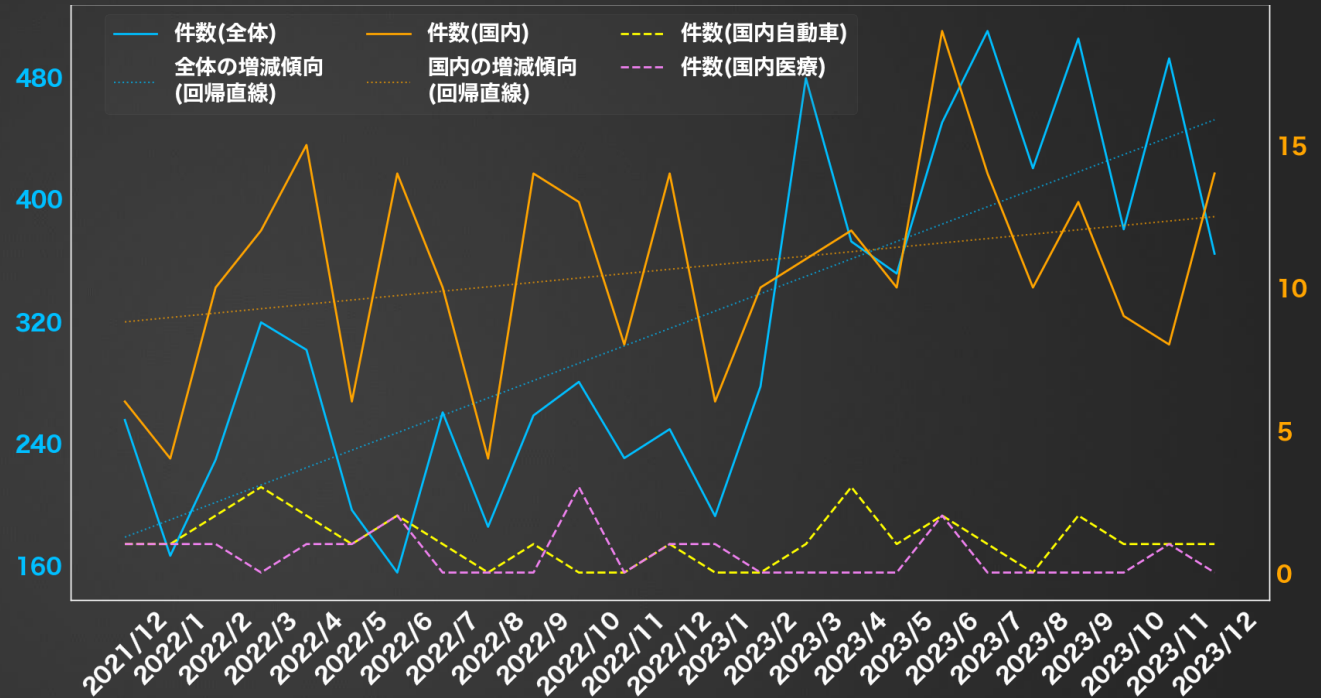
● 被害数の推移 (2021年12月～2023年12月 / 全世界及び国内) (MBSID調べ)

※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。

期間	件数(全体)	件数(国内)	件数(国内自動車)	件数(国内医療)
2021/12	255	6	1	1
2022/1	166	4	1	1
2022/2	229	10	2	1
2022/3	319	12	3	0
2022/4	301	15	2	1
2022/5	196	6	1	1
2022/6	155	14	2	2
2022/7	260	10	1	0
2022/8	185	4	0	0
2022/9	258	14	1	0
2022/10	280	13	0	3
2022/11	230	8	0	0
2022/12	249	14	1	1
2023/1	192	6	0	1
2023/2	277	10	0	0
2023/3	479	11	1	0
2023/4	372	12	3	0
2023/5	351	10	1	0
2023/6	450	19	2	2
2023/7	510	14	1	0
2023/8	420	10	0	0
2023/9	505	13	2	0
2023/10	380	9	1	0
2023/11	492	8	1	1
2023/12	364	14	1	0
合計	7875	266	28	15

▼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)

※特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
 (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)
 ※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)を含む。
 ※業種分類や集計方法を含む本レポートの各データ(値)はMBSID独自の観測および集計結果となる。
 ※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る。
 ※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元に集計している。
 ※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む。
 ※攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

2023

12

資本金別 月別統計

(国内)

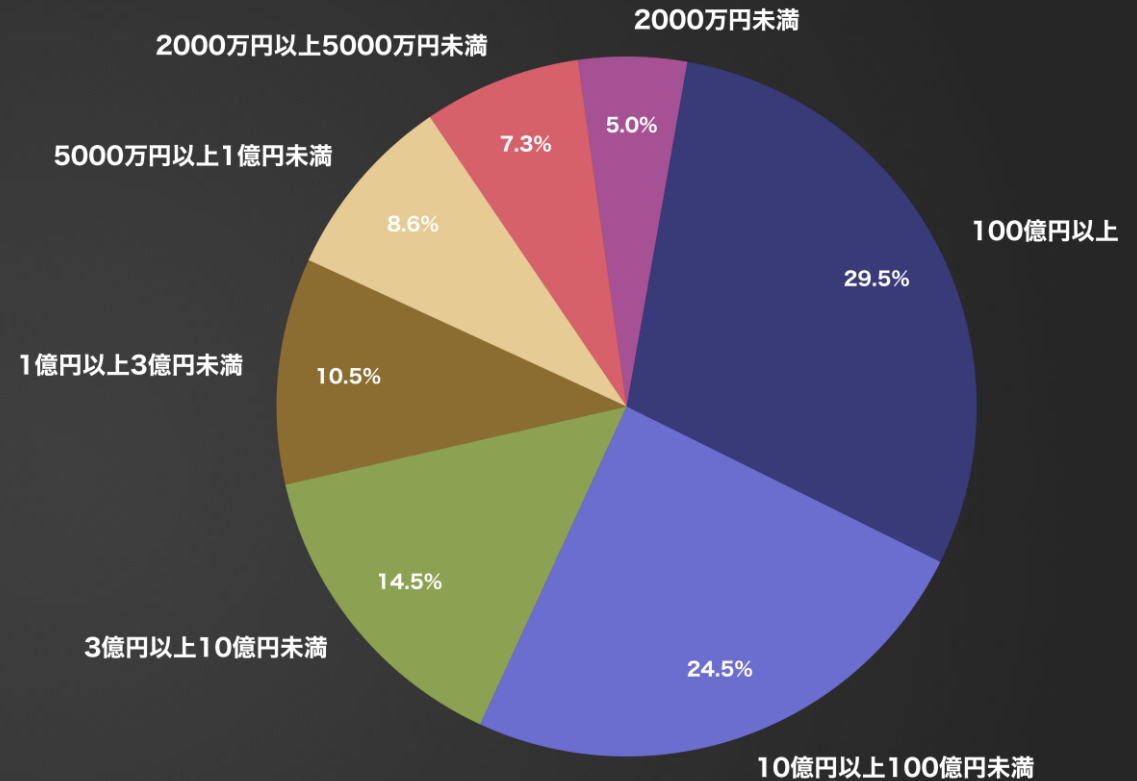
- ※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
(日本にフォーカスした一部の表/グラフのみ、公表や報道から判明した数を加味し集計)
- ※ 国内被害組織に関する各種データについては、海外拠点(支社/関連会社)を含む。
- ※ 業種分類や集計方法を含む本レポートの各データ(値)はMBSD独自の観測および集計結果となる。
- ※ これらはいくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
- ※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
- ※ ごく一部のランサムウェアの使用が明確に確認されていない暴露&恐喝グループの値も含む。
- ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
- ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 月別内訳 資本金別 (2021年12月~2023年12月 / 国内) (MBSD調べ)

※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

▼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)

資本金	件数	割合 (%)
100億円以上	65	29.5
10億円以上100億円未満	54	24.5
3億円以上10億円未満	32	14.5
1億円以上3億円未満	23	10.5
5000万円以上1億円未満	19	8.6
2000万円以上5000万円未満	16	7.3
2000万円未満	11	5.0



▼このうち中小企業に該当する割合

- ・3億円未満が該当するとした場合：31.4%
- ・10億円未満が該当するとした場合：45.9%

(※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)

※特に注釈がない場合は、リークサイトに掲載された数に揃えた値とする。
 (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)
 ※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)を含む。
 ※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独自の観測および集計結果となる。
 ※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る。
 ※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元に集計している。
 ※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む。
 ※攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

2023

12

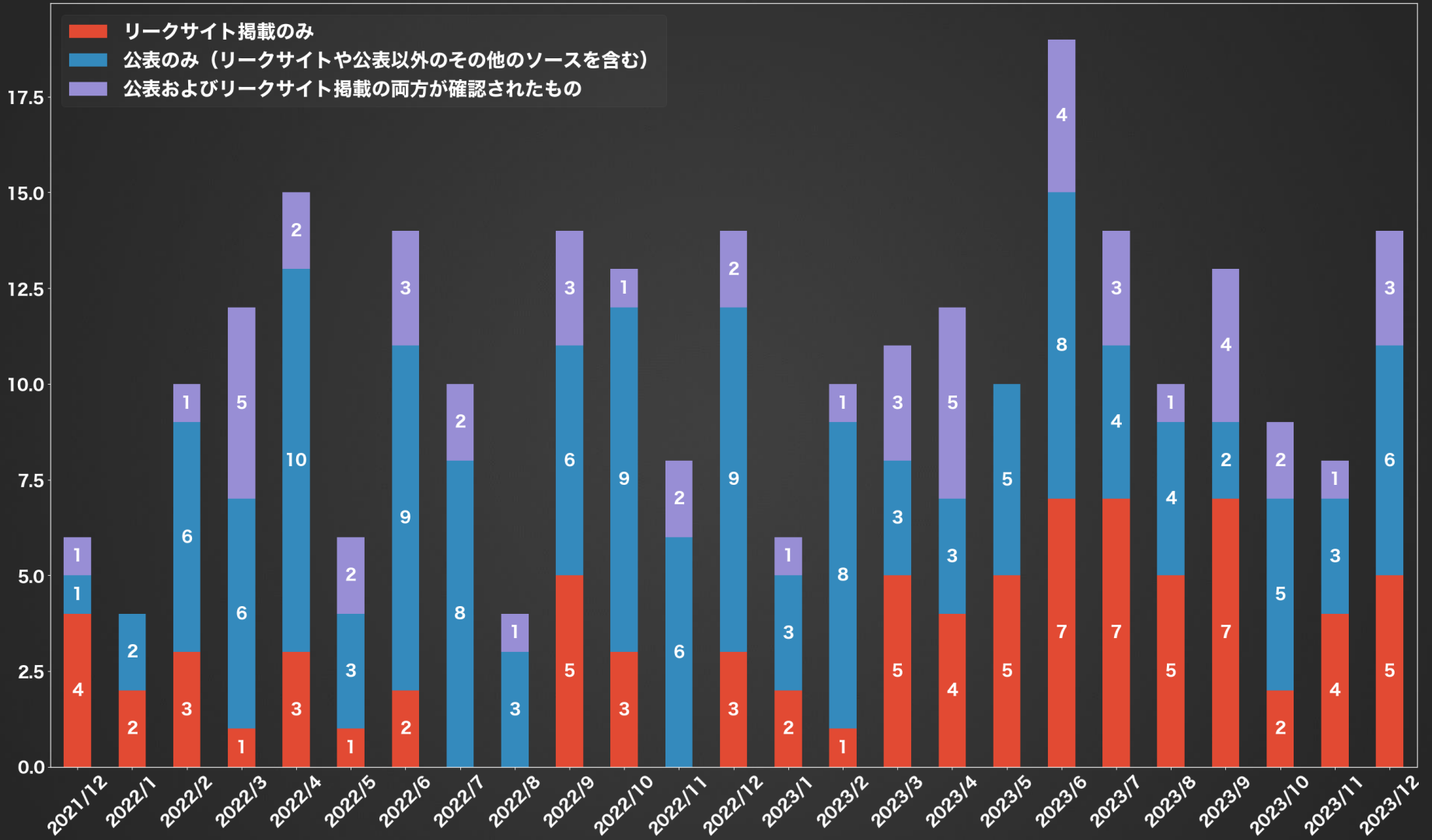
公表と暴露に関する統計

(国内)

- ※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
(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)
- ※ 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)を含む。
- ※ 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独自の観測および集計結果となる。
- ※ これらはい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る。
- ※ 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元に集計している。
- ※ 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む。
- ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
- ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 公表割合 月別内訳 (2021年12月~2023年12月 / **国内**) (MBSD調べ)

▼ランサムウェア攻撃における公表数と掲載数の分析



※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
 (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)
 ※ 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)を含む。
 ※ 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独自の観測および集計結果となる。
 ※ これらはい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る。
 ※ 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元に集計している。
 ※ 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む。
 ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

(※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)

2023

12

公となった国内被害組織 概要一覧

- ※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
(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)
- ※ 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)を含む。
- ※ 業種分類や集計方法を含む本レポートの各データ(値)はMBSI独自の観測および集計結果となる。
- ※ 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る。
- ※ 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元に集計している。
- ※ 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む。
- ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
- ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

● 公となった国内被害組織概要一覧（過去1年間／2022年12月～2023年12月）(MBSD調べ)

※ (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
2022/12	(Unknown)	医療法人
2022/12	(Unknown)	私立大学
2022/12	(Unknown)	公益社団法人
2022/12	(Unknown)	電子機器販売会社(海外拠点)
2022/12	(Unknown)	公立図書館
2022/12	(Unknown)	情報通信機器販売・保守サービス会社
2022/12	(Unknown)	情報通信機器販売・保守サービス会社
2022/12	(Unknown)	食品メーカー
2022/12	(Unknown)	システム開発会社
2022/12	LockBit	産業用機械メーカー
2022/12	LockBit	仮設機材メーカー(海外拠点)
2022/12	AlphV / BlackCat	自動車向け部品メーカー(海外拠点)
2022/12	AlphV / BlackCat	プラスチック製品メーカー(海外拠点)
2022/12	BianLian	電子部品メーカー(海外拠点)
2023/1	(Unknown)	ポンプメーカー
2023/1	(Unknown)	漁業組合
2023/1	(Unknown)	社会福祉法人
2023/1	LockBit	非鉄金属製品メーカー(海外拠点)
2023/1	LockBit	非鉄金属製品メーカー
2023/1	LockBit	複合材料メーカー(海外拠点)
2023/2	(Unknown)	電気通信事業者
2023/2	(Unknown)	インターネット サービス プロバイダ
2023/2	(Unknown)	医療機器メーカー(海外拠点)
2023/2	(Unknown)	加工食品メーカー
2023/2	(Unknown)	原子力発電関係会社
2023/2	(Unknown)	信用調査会社
2023/2	(Unknown)	私立中学・高校
2023/2	(Unknown)	広域行政事務組合
2023/2	LockBit	WEBデザイン会社
2023/2	LockBit	音響製品メーカー

被害月	攻撃グループ	業種概要
2023/3	(Unknown)	食品容器メーカー
2023/3	(Unknown)	倉庫管理運営会社
2023/3	(Unknown)	メディアコンテンツ制作会社
2023/3	(Unknown)	中古車販売会社
2023/3	STORMOUS	大手電機メーカー
2023/3	STORMOUS	産業機械メーカー(海外拠点)
2023/3	CLOP	電力システム開発会社(海外拠点)
2023/3	CLOP	ITサービス会社
2023/3	Royal	機械部品メーカー
2023/3	Donuts Leaks	大手機械部品メーカー
2023/3	Donuts Leaks	国内ホテル
2023/4	(Unknown)	建設会社
2023/4	(Unknown)	広告サービス会社
2023/4	(Unknown)	情報通信サービス会社
2023/4	LockBit	工具メーカー
2023/4	LockBit	電機メーカー(海外拠点)
2023/4	LockBit	電子機器メーカー(海外拠点)
2023/4	LockBit	生活家電メーカー
2023/4	LockBit	複合商社(海外拠点)
2023/4	Royal	大手繊維メーカー(海外拠点)
2023/4	Royal	大手自動車部品メーカー(海外拠点)
2023/4	BlackByte	自動車販売会社
2023/4	Qilin	大手専門商社(海外拠点)
2023/5	(Unknown)	大手コンクリート製品メーカー
2023/5	(Unknown)	教育委員会
2023/5	(Unknown)	ソフトウェアメーカー
2023/5	(Unknown)	児童養護施設
2023/5	(Unknown)	コンクリート製品メーカー
2023/5	LockBit	自動車部品メーカー(海外拠点)
2023/5	LockBit	デザイン事務所

被害月	攻撃グループ	業種概要
2023/5	LockBit	大手電子部品メーカー(海外拠点)
2023/5	AlphV / BlackCat	大手通信プロバイダ(海外拠点)
2023/5	Royal	大手精密機器メーカー(海外拠点)
2023/6	(Unknown)	大手製薬会社
2023/6	(Unknown)	ソフトウェアメーカー
2023/6	(Unknown)	住宅機器メーカー
2023/6	(Unknown)	大手文具メーカー
2023/6	(Unknown)	インテリア雑貨販売会社
2023/6	(Unknown)	医療機器販売会社
2023/6	(Unknown)	大手通信販売会社
2023/6	(Unknown)	インテリア販売会社
2023/6	LockBit	大手ファスナーメーカー(海外拠点)
2023/6	LockBit	複合商社
2023/6	AlphV / BlackCat	ソフトウェアメーカー
2023/6	CLOP	大手テクノロジー企業
2023/6	Royal	自動車シートメーカー(海外拠点)
2023/6	BlackByte	大手楽器メーカー(海外拠点)
2023/6	Qilin	大手住宅総合メーカー
2023/6	Medusa	大手商社(海外拠点)
2023/6	AKIRA	大手自動車用品メーカー(海外拠点)
2023/6	Mallox	ソフトウェアメーカー
2023/6	Mallox	ソフトウェアメーカー
2023/7	(Unknown)	学校法人
2023/7	(Unknown)	大手信販会社
2023/7	(Unknown)	化粧品メーカー
2023/7	LockBit	船舶ターミナルシステム
2023/7	AlphV / BlackCat	大手食品メーカー(海外拠点)
2023/7	CLOP	総合エレクトロニクスメーカー(海外拠点)
2023/7	CLOP	総合画像機器メーカー(海外拠点)
2023/7	CLOP	大手飲料メーカー(海外拠点)

※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
 (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)
 ※ 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)を含む。
 ※ 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独自の観測および集計結果となる。
 ※ これらはい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る。
 ※ 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元に集計している。
 ※ 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む。
 ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

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

● 公となった国内被害組織概要一覧（過去1年間／2022年12月～2023年12月）(MBSID調べ)

※ (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
2023/7	CLOP	たばこ製造販売会社(海外拠点)
2023/7	CLOP	自動車部品メーカー(海外拠点)
2023/7	CLOP	大手電気機器メーカー(海外拠点)
2023/7	AKIRA	大手音楽関連商品メーカー(海外拠点)
2023/7	NoEscape	土木建設会社
2023/7	PLAY	大手生活用品メーカー(海外拠点)
2023/8	(Unknown)	大手教育関連事業会社
2023/8	(Unknown)	教育関連事業会社
2023/8	(Unknown)	電気設備工事会社
2023/8	(Unknown)	容器メーカー
2023/8	LockBit	大手物流会社(海外拠点)
2023/8	LockBit	総合機器装置メーカー
2023/8	AlphV / BlackCat	大手精密機器メーカー
2023/8	CLOP	大手印刷機械メーカー
2023/8	Mallox	和菓子メーカー
2023/8	NoEscape	電気設備工事会社
2023/9	Ragnar Locker	情報機器製品販売会社(海外拠点)
2023/9	(Unknown)	建材メーカー
2023/9	(Unknown)	大手住宅メーカー
2023/9	LockBit	大手塗料メーカー(海外拠点)
2023/9	STORMOUS	大手電子機器メーカー
2023/9	AlphV / BlackCat	大手運輸サービス会社(海外拠点)
2023/9	AlphV / BlackCat	自動車部品メーカー(海外拠点)
2023/9	BlackByte	自動車部品メーカー
2023/9	Qilin	大手繊維製品メーカー(海外拠点)
2023/9	AKIRA	パッケージ製品メーカー(海外拠点)
2023/9	Money Message	インターホン製品販売メーカー(海外拠点)
2023/9	Ransomed.vc	大手テクノロジー企業
2023/9	Ransomed.vc	大手情報通信会社(攻撃声明に誤り / 被害なし)
2023/10	(Unknown)	大手衣類販売会社

被害月	攻撃グループ	業種概要
2023/10	(Unknown)	電子部品サービス会社
2023/10	(Unknown)	農業支援会社
2023/10	(Unknown)	小売店経営会社
2023/10	(Unknown)	国立大学
2023/10	AlphV / BlackCat	大手専門商社
2023/10	NoEscape	自動車部品メーカー
2023/10	PLAY	眼鏡メーカー
2023/10	Ransomed.vc	インターネットプロバイダー
2023/11	(Unknown)	耐火製品メーカー
2023/11	(Unknown)	公立病院
2023/11	LockBit	自転車部品メーカー
2023/11	AlphV / BlackCat	大手電子部品メーカー
2023/11	AlphV / BlackCat	畜産機器メーカー
2023/11	Medusa	金融サービス会社(海外拠点)
2023/11	INC Ransom	大手輸送用機器メーカー(海外拠点)
2023/11	Hunters International	大手機械部品メーカー
2023/12	(Unknown)	大手出版社
2023/12	(Unknown)	一般社団法人
2023/12	(Unknown)	地方新聞社
2023/12	(Unknown)	地方自治体
2023/12	(Unknown)	システムコンサルティング会社
2023/12	(Unknown)	地域事業
2023/12	LockBit	エネルギーサービス運営管理会社
2023/12	LockBit	社会福祉法人
2023/12	LockBit	大手服飾メーカー
2023/12	AlphV / BlackCat	統合型リゾート施設(海外拠点)
2023/12	AKIRA	大手自動車メーカー(海外拠点)
2023/12	PLAY	産業用品メーカー(海外拠点)
2023/12	KNIGHT	プラスチック加工会社
2023/12	DragonForce	大手食品メーカー(海外拠点)

※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
 (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)
 ※ 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)を含む。
 ※ 業種分類や集計方法を含む本レポートの各データ(値)はMBSID独自の観測および集計結果となる。
 ※ これらはい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る。
 ※ 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元に集計している。
 ※ 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む。
 ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※ 集計方法の変更や、時間が長期経過し公開/公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。

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

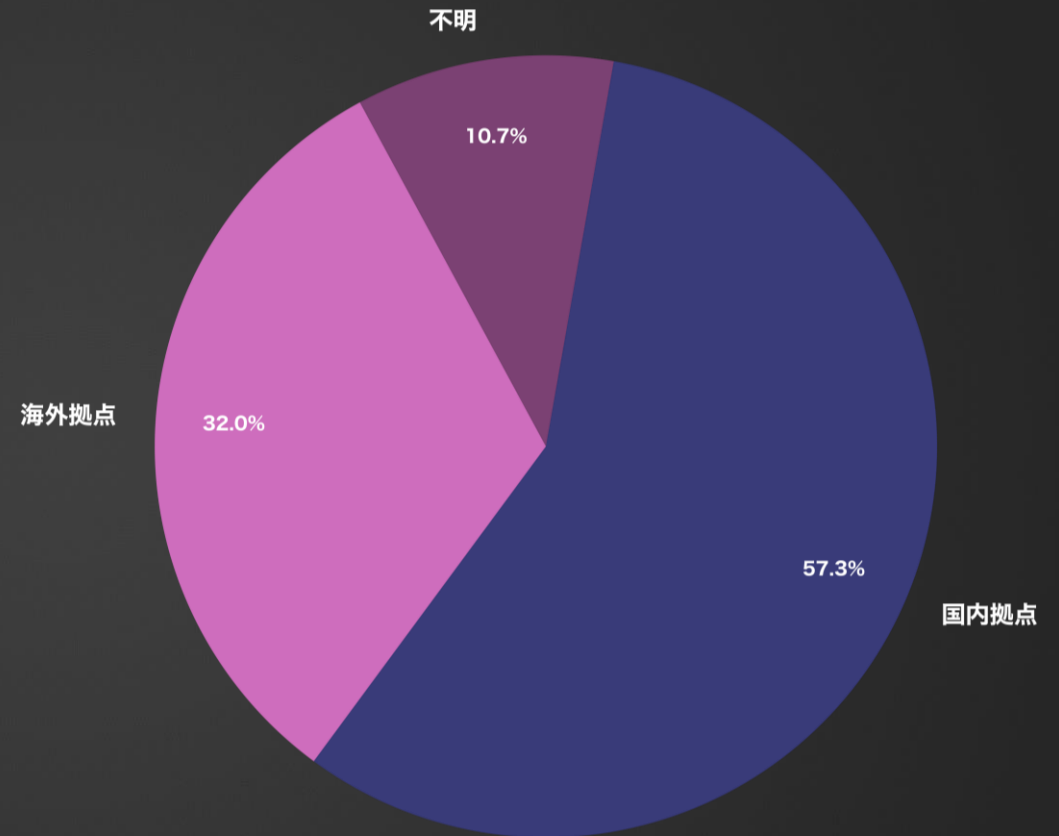
● 公となった国内被害組織における拠点割合（過去1年間／2022年12月～2023年12月）（MBSD調べ）

（※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	86	57.3
海外拠点	48	32.0
不明	16	10.7



（※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）

※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
 （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）
 ※ 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／関係会社）を含む。
 ※ 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独自の観測および集計結果となる。
 ※ これらはい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る。
 ※ 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元に集計している。
 ※ 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む。
 ※ 攻撃グループや被害組織について、正確な情報が公開されていないものは「(Unknown)」としている。
 ※ 集計方法の変更や、時間が長期経過し公開／公表されるケースもある等の関係上、常に最新月のレポートを参照してほしい。



Know your enemy.
Defense leadership.®

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