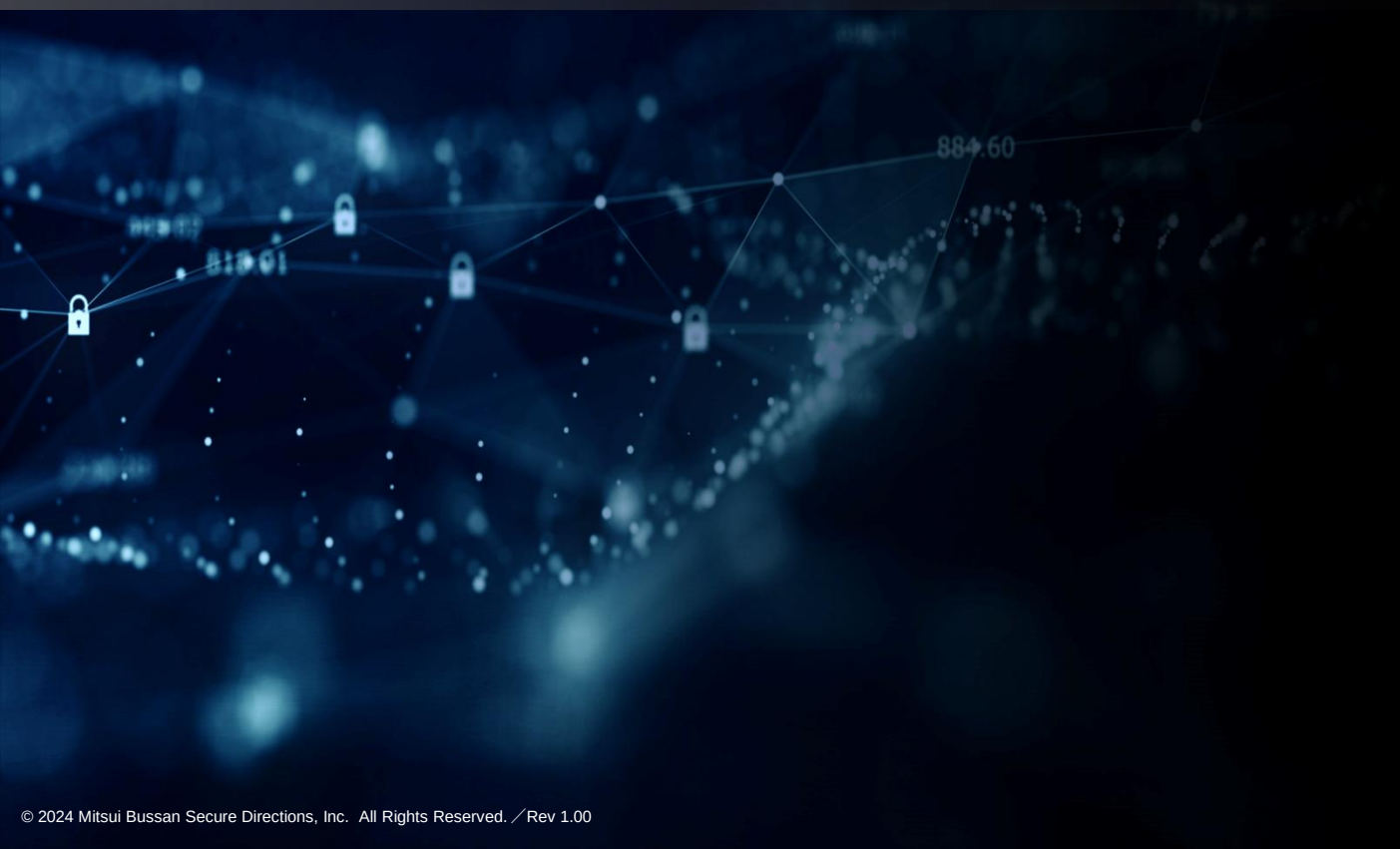
M|B|S|D Know your enemy. Defense leadership.®

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3月号 Rev 1.00
(2024年2月分)

2024
2



Created by Cyber Intelligence Group

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）

MBSD Know your enemy. Defense leadership.®

● 監視している攻撃グループ数：159グループ（※1）

※1 活動停止した攻撃グループを含む

→内2024年2月にリークサイト掲載を確認した攻撃グループ数：36件

● 監視中の攻撃グループ一覧

8BASE	CiphBit	Endurance	MALAS	Payload.bin	Sabbath (54bb47h)
ABYSS	CipherLocker	Entropy	MalekTeam	PLAY	shaoleaks
AKIRA	Cloak	Everest	MALLOX	Prometheus	SIEGEDSEC
AKO	CLOP	FSTeam	MBC	PUTIN TEAM	SLUG
Alpha(MYDATA)	Conti	Grief	Medusa	Pysa	Snatch
AlphV / BlackCat	CoomingProject	Groove	MEOW	Qilin	Solidbit
ArvinClub	CROSSLOCK	Haron	Metaencryptor	Quantum	Sparta Blog
Astro Team	CryptBB	Hitler Ransomware	Midas	RA GROUP	Spook
AtomSilo	CRYPTNET	Hive	Mindware	Ragnar Locker	STORMOUS
Avaddon	CryptOn	HolyGhost	~~Mogilevich~~(fraud)	Ragnarok	Sugar
AvosLocker	Cuba	Hotarus	MOISHA	Rancoz	Suncrypt
Axxes	Cyclops	HUNTERS INTERNATIONAL	Money Message	Ransom Cartel	SynACK
Babuk	DAGON LOCKER	ICEFIRE	Monti	RANSOM CORP	ThreeAM(3AM)
BianLian	DAIXIN	INC Ransom	Mount Locker	Ransomed.vc	TRIGONA
Bl4ckt0r (BlackTor)	DarkAngels	Insane	N3tw0rm	RansomEXX	TRISEC
BlackBasta	DARKBIT	Karakurt	N4UGHTYSEC	RansomHouse	UnSafe
BlackByte	DARKPOWER	Karma Leaks	Nefilim	ransomhub	V IS VENDETTA
BlackDolphin	DarkRace	Knight	Nevada	RansomwareBlog	Vice Society
BlackMatter	DarkRypt	LAMBDA	NightSky	Ranzy	VSOP
Blackout	Darkside	LaPiovra	NoEscape	Raznatovic	WEREWOLVES
BLACKSUIT	Donut	LAPSUS$	Nokoyawa	RedAlert (N13V)	x001xs
BLOODY	DoppelPaymer	LILITH	NONAME(2023年確認)	Relic	XING Team
BLUESKY	dotAdmin	LockBit	NONAME(VFOKX)	Revil (Sodinokibi)	Yanluowang
BULLY	DragonForce	Lorenz	Omega	Rhysida	Zeon
CACTUS	Dunghill	LostTrust	Onyx	ROOK	
CHEERS	eCh0raix	LV BLOG	Pandora	Royal	
ChileLocker	El_Cometa	MADCAT	Pay2Key	Rransom	

※ 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。

暴露型ランサムウェア攻撃統計CIGマンスリーレポート

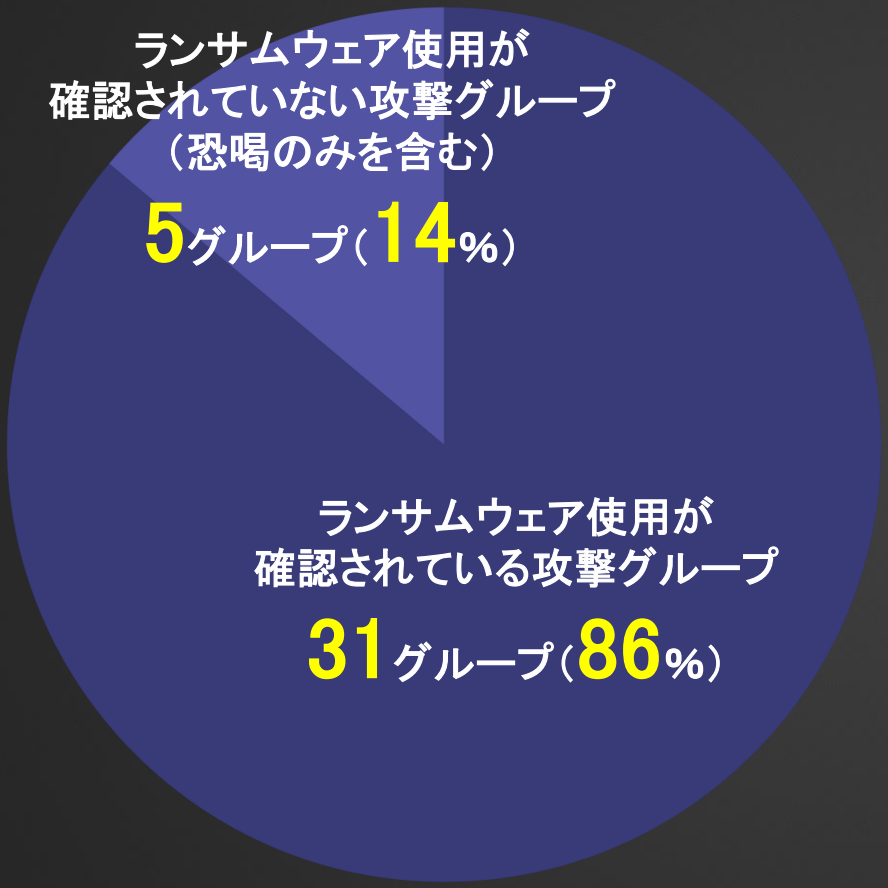
監視中のランサムウェア攻撃グループ情報（ランサムウェア使用の割合）

MBSD Know your enemy. Defense leadership.®

※1 リークサイトやTelegramなどを含む

● 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 （2024年2月）

（※2024年2月にリークサイト掲載を確認した攻撃グループ全36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が存在する。また、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、2024年2月に活動中である事が確認された全36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。

※ 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。

Created by Cyber Intelligence Group

今月のハイライト

LockBitのサーバーが法執行機関に一部押収されるも、数日後には活動再開

LockBitはランサムウェア攻撃グループの中でも最も古いグループの一つであり2019年頃から活動。リークサイト掲載数では全体平均の約2割がLockBitによる攻撃となる状況が長年続いており、その中にはこれまで様々な日本関連組織も含まれてきた。
日本時間2024年2月20日未明、LockBitのサーバーが法執行機関による共同作戦「Operation Chronos」の一環で押収され、リークサイトがダウン。最も影響力のある攻撃グループという背景もありその壊滅が期待された。しかし2月25日頃には新たなリークサイトがミラーサイトを含め複数出現し、LockBitが活動を再開。
活動再開に際してLockBitは、今回のダウンは自らの怠惰が招いた事態であり、今後は自身の姿勢を改め、政府機関に対して積極的に攻撃を仕掛ける趣旨の声明をリークサイト上に記載、法執行機関へ報復を表明した。そのため、今後は各国の政府機関やそれに準ずる組織への攻撃の激化も予想される。
また、LockBitが以前から提示しているバグ報奨金プログラムに触れ、今回の攻撃の起点となった捜査機関側の人物に対し、FBIよりも多額の報奨金の支払いを示唆した上で勧誘する旨のメッセージを掲載するなどで挑発した。
これまで他の攻撃グループでは、活動継続が困難となった際にリブランド（グループ名の変更などを行い別グループに見せかけること）し姿をくらませる状況が見られてきた中、LockBitはその名前を変えずに活動継続してきた数少ない攻撃グループであった。今回の摘発においても、引き続きLockBitというブランド名を変えることなく活動継続の道を選んだ点は興味深く、首謀者のプライドと執念が感じられる。
今回の一連の出来事は、押収がLockBitにとって一定の打撃となったと考えられる一方で、同時に、攻撃グループを根絶することの難しさがあらためて浮き彫りとなった例であるともいえる。

AlphV/BlackCatが3月初旬から活動停止か

AlphV/BlackCat（以降、AlphV）は、2023年12月に法執行機関によって一度リークサイトをダウンさせられたが、事前に準備していたミラーサイトを通じて活動を継続していた。しかし2024年3月5日、AlphVのリークサイトが再び法執行機関による押収を示す画面に切り替わった事を確認。
ただし、今回の「押収」は自作自演であり、法執行機関によるテイクダウンに見せかけ姿をくらませた可能性が疑われている。
その理由の一つに、同時期に水面下で確認されていた状況として、AlphVのアフィリエイトを主張する人物による内部情報の暴露が挙げられる。このアフィリエイトはハッカーフォーラムに「AlphVがアメリカの医療関連組織から身代金として2200万ドルを受け取った後、自分たちへの支払いを先延ばしにした挙句に全額を持ち逃げしたが、当該被害組織の重要データは未だに自分たちが保持している」といった趣旨の内容を投稿、同時にAlphVとの協業はやめるよう呼びかけていた。また一方で、AlphVが連絡に使用するToxのステータス画面に”ソースコードを500万ドルで販売する”というコメントが表示されている状況も確認されており、こうした状況に加えて、海外メディアによる取材に法執行機関は（3月の押収画面の切り替わりへの）関与を否定している。
いずれにせよ、AlphVに対する法執行機関の圧力は強まっており、米国務省はAlphVの主要メンバーの個人特定、逮捕に繋がる情報提供者へ最大1500万ドル報奨金の発表。またCISA、 FBI 、及びHHS（保健福祉省）は同グループの攻撃に対する警戒を促す声明を出しており、今回の一件は内部からの反発や法執行機関の圧力から逃れるために、AlphVが意図的に姿を消したとする見方が自然であるともいえる。

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ある。

●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。

Know your enemy.
Defense leadership.®

年間 統計
（全世界）

2024

2

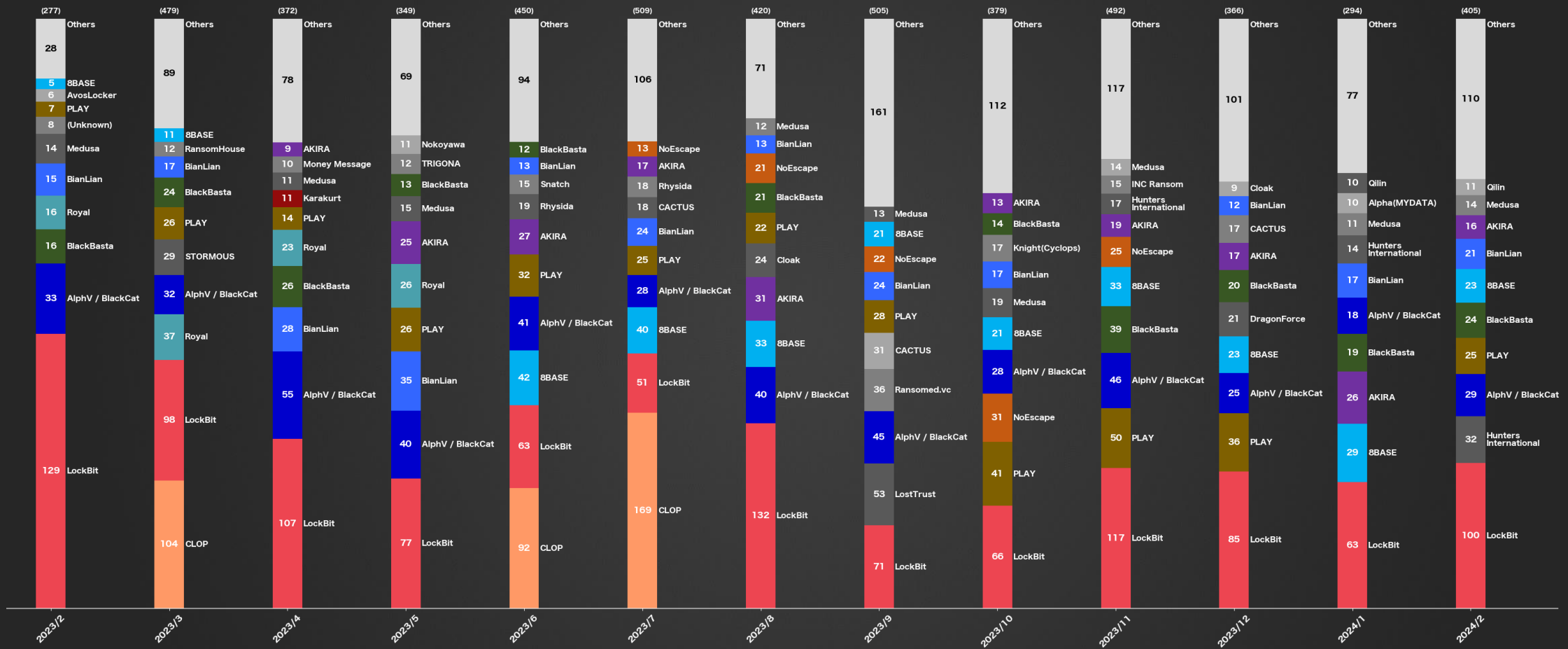
※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
　（日本にフォーカスした一部の表／グラフのみ、公表や報道から判明した数を加味し集計）
※ 国内被害組織に関する各種データについては、海外拠点（支社／関連会社）を含む。
※ 業種分類や集計方法を含む本レポートの各データ（値）はMBSD独自の観測および集計結果となる。
※ これらはあくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
※ ごく一部のランサムウェアの使用が明確に確認されていない暴露＆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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート – ①

Know your enemy. Defense leadership.

● 攻撃グループ割合で見る被害数の年間統計（2023年2月～2024年2月／全世界）(MBSD調べ)



※ 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。

Created by Cyber Intelligence Group

M|B|S|D Know your enemy. Defense leadership.

2024

2

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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ④

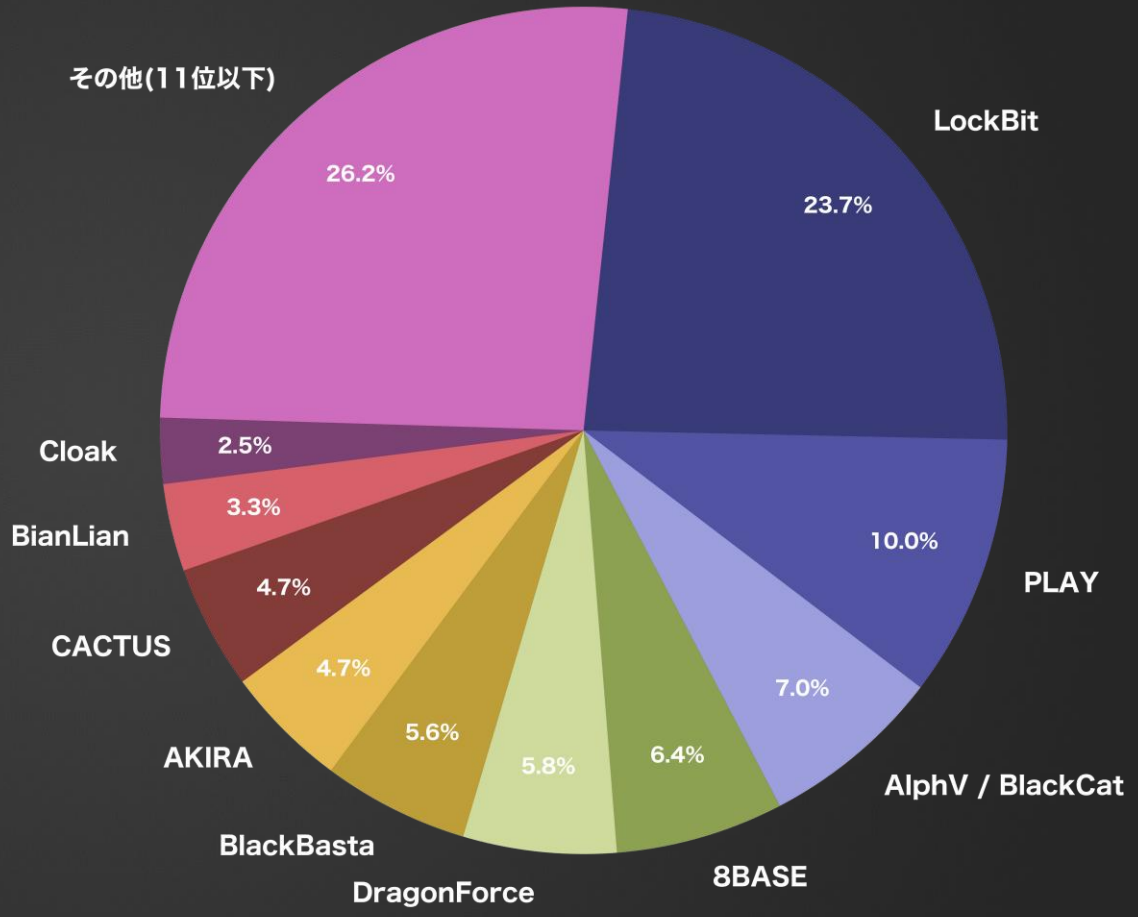
Know your enemy.
Defense leadership.

● 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	10.0	- 14
AlphV / BlackCat	25	7.0	- 20
8BASE	23	6.4	- 10
DragonForce	21	5.8	+ 21
BlackBasta	20	5.6	- 19
AKIRA	17	4.7	- 2
CACTUS	17	4.7	+ 7
BianLian	12	3.3	- 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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ④

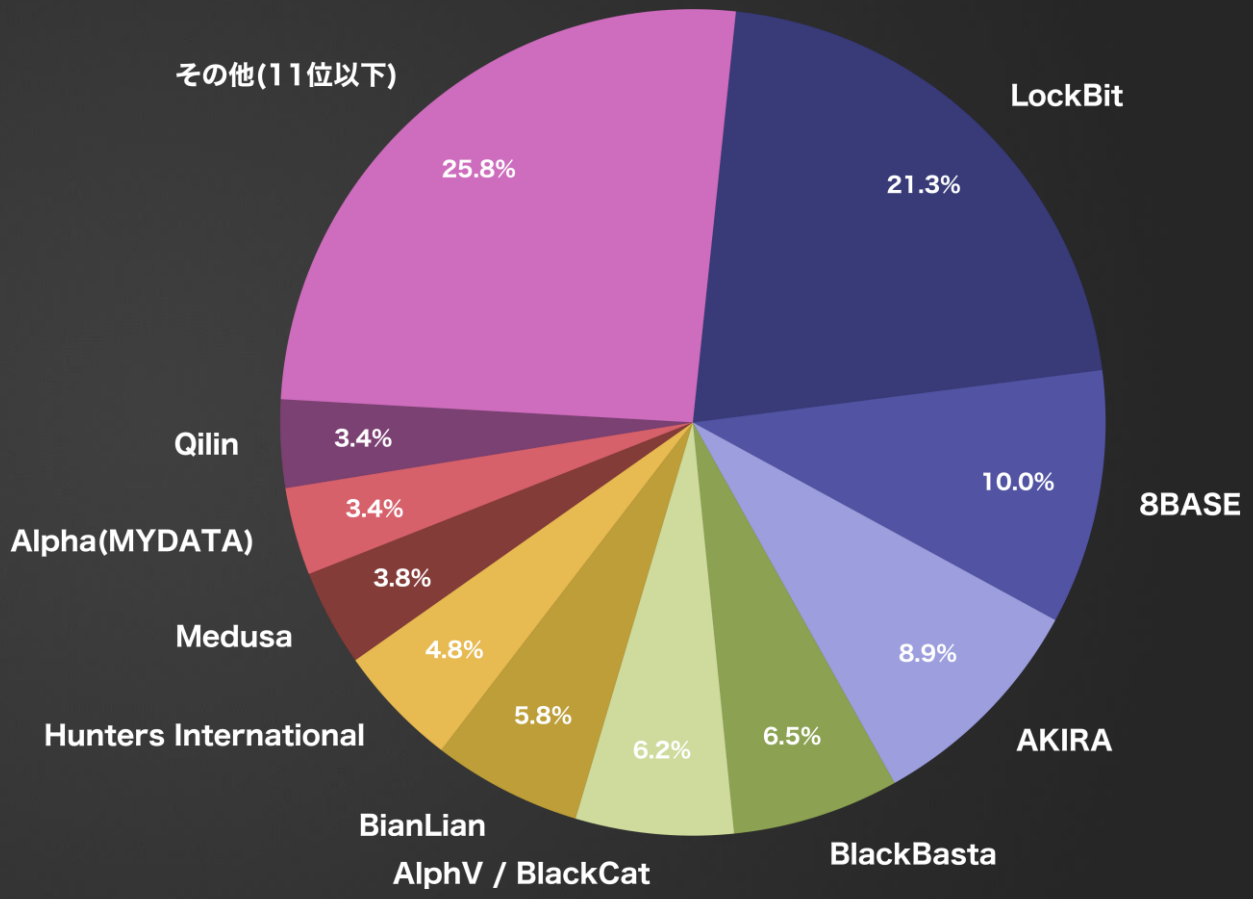
Know your enemy.
Defense leadership.

● 月別内訳 攻撃グループ TOP10 （2024年 1 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	62	21.3	- 23
8BASE	29	10.0	+ 6
AKIRA	26	8.9	+ 9
BlackBasta	19	6.5	- 1
AlphV / BlackCat	18	6.2	- 7
BianLian	17	5.8	+ 5
Hunters International	14	4.8	+ 8
Medusa	11	3.8	+ 2
Alpha(MYDATA)	10	3.4	+ 10
Qilin	10	3.4	+ 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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ④

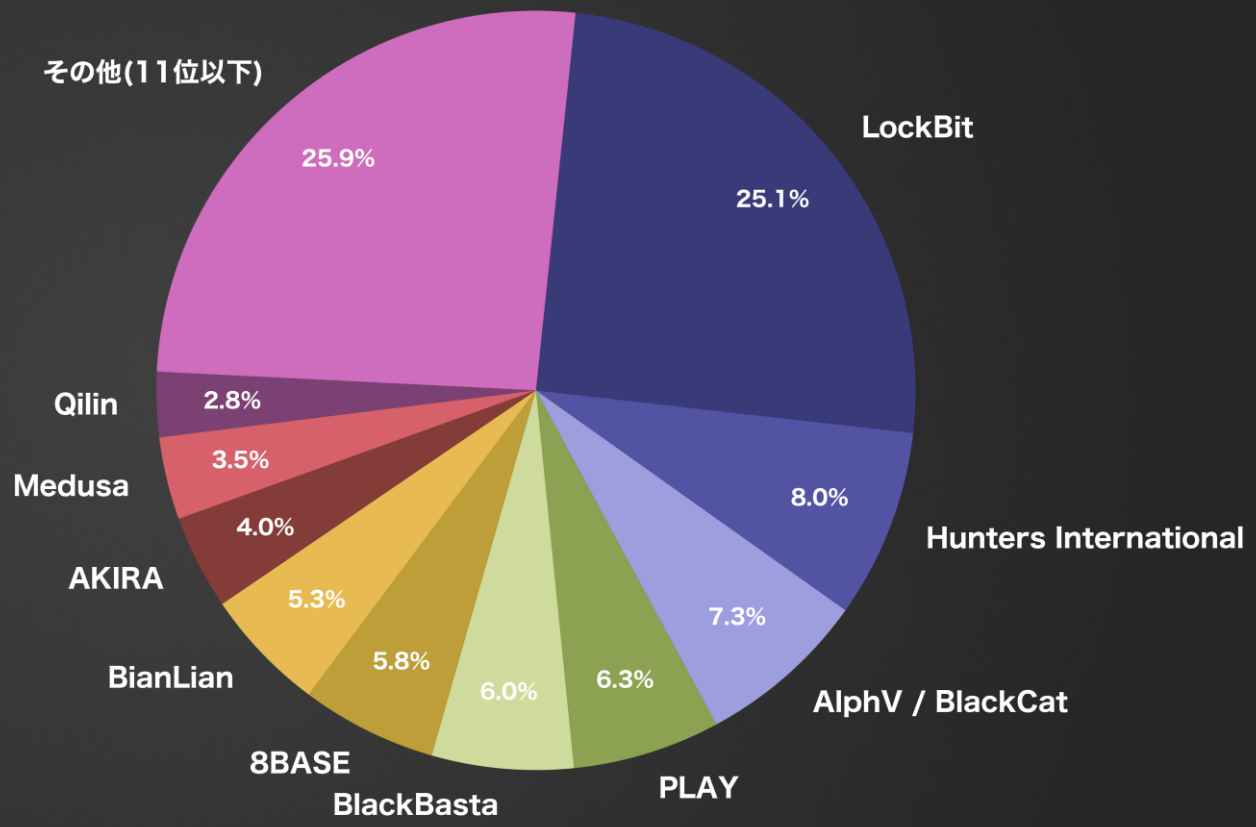
Know your enemy.
Defense leadership.®

● 月別内訳 攻撃グループ TOP10 （2024年 2 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	100	25.1	+ 38
Hunters International	32	8.0	+ 18
AlphV / BlackCat	29	7.3	+ 11
PLAY	25	6.3	+ 20
BlackBasta	24	6.0	+ 5
8BASE	23	5.8	- 6
BianLian	21	5.3	+ 4
AKIRA	16	4.0	- 10
Medusa	14	3.5	+ 3
Qilin	11	2.8	+ 1

▼ランサムウェア攻撃グループの勢力割合
（リークサイトの掲載数による比較）



※ 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。

Created by Cyber Intelligence Group

M|B|S|D Know your enemy. Defense leadership.

2024

2

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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑦

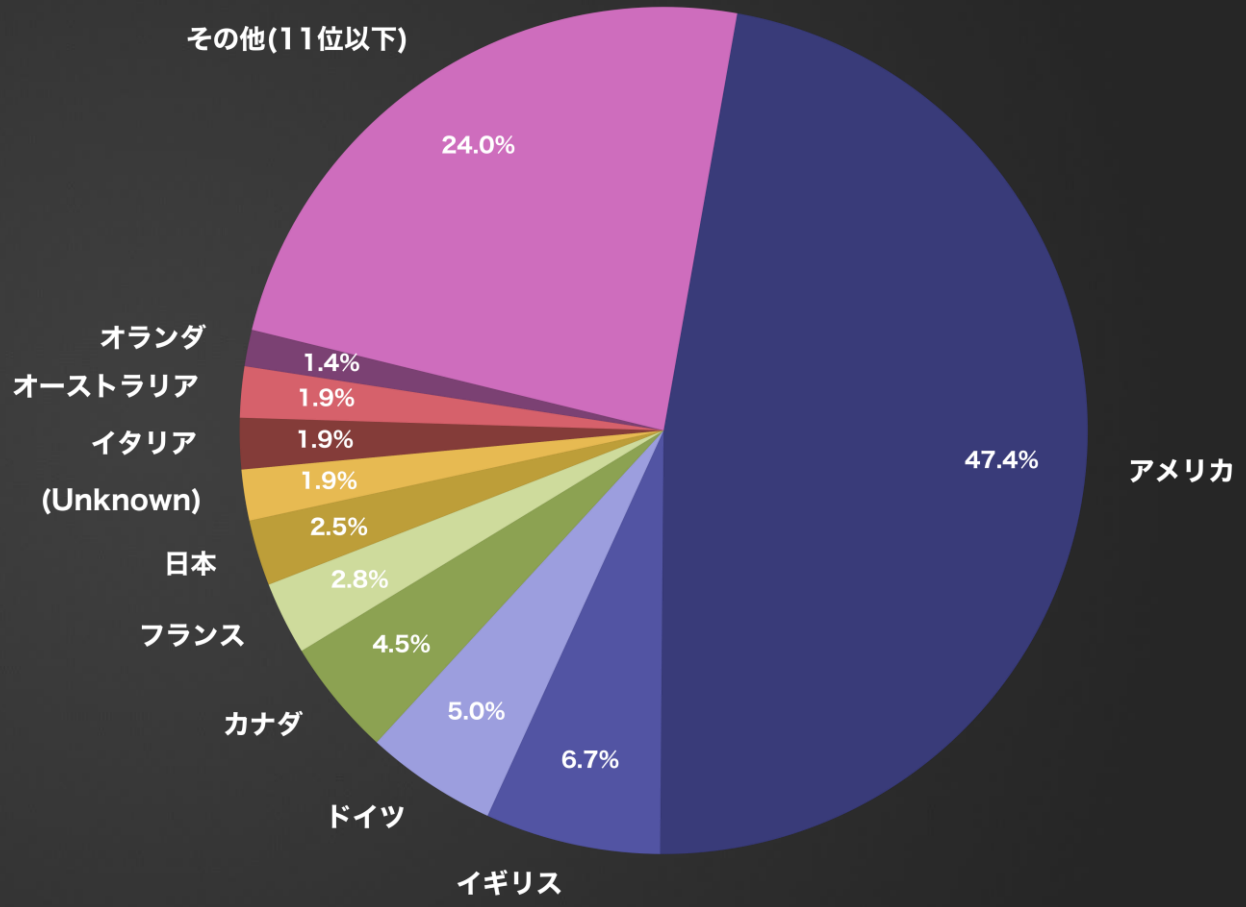
Know your enemy.
Defense leadership.®

● 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	47.4	- 62
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	9	2.5	+ 4
(Unknown)	7	1.9	- 7
イタリア	7	1.9	- 12
オーストラリア	7	1.9	- 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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑦

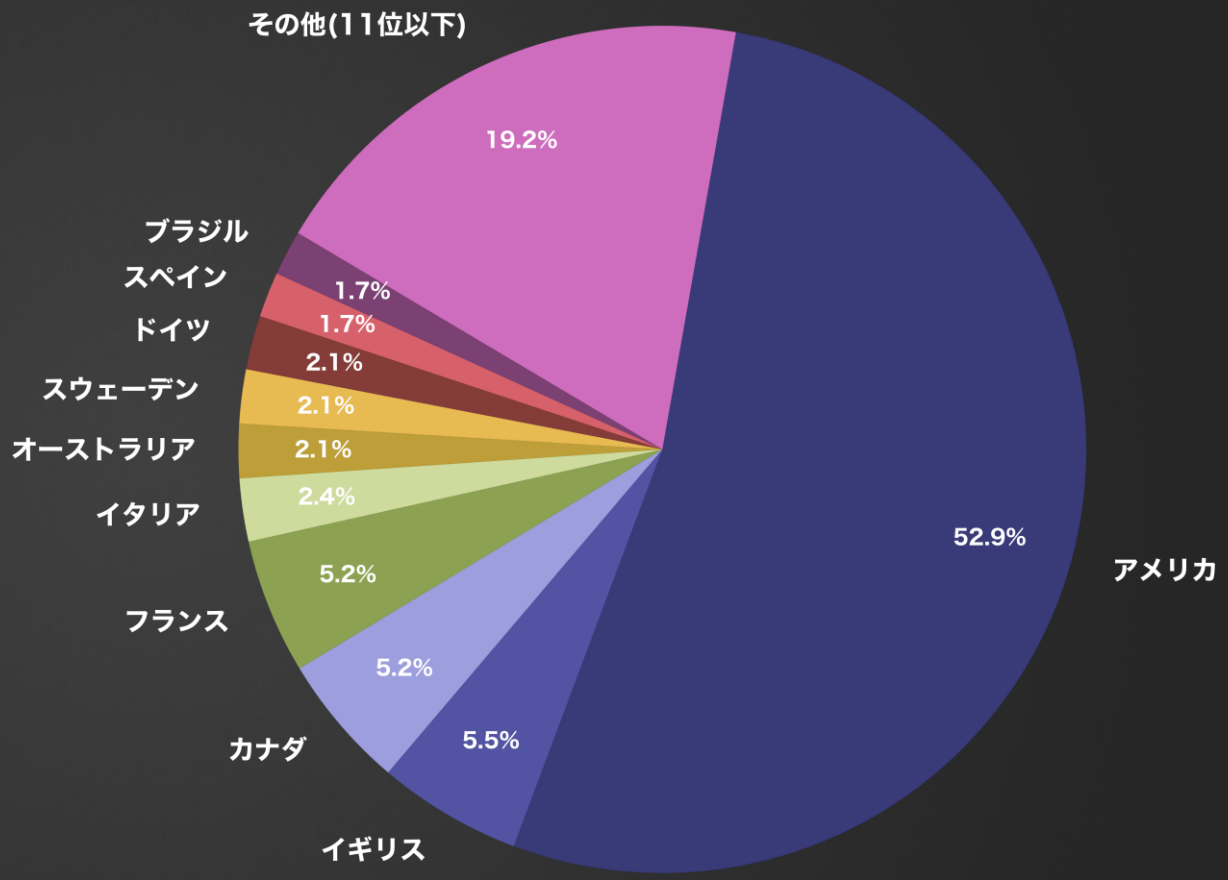
Know your enemy.
Defense leadership.®

● 月別内訳 被害国TOP10 （ 2024年 1 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	154	52.9	- 16
イギリス	16	5.5	- 8
カナダ	15	5.2	- 1
フランス	15	5.2	+ 5
イタリア	7	2.4	± 0
オーストラリア	6	2.1	- 1
スウェーデン	6	2.1	+ 3
ドイツ	6	2.1	- 12
スペイン	5	1.7	+ 1
ブラジル	5	1.7	+ 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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑦

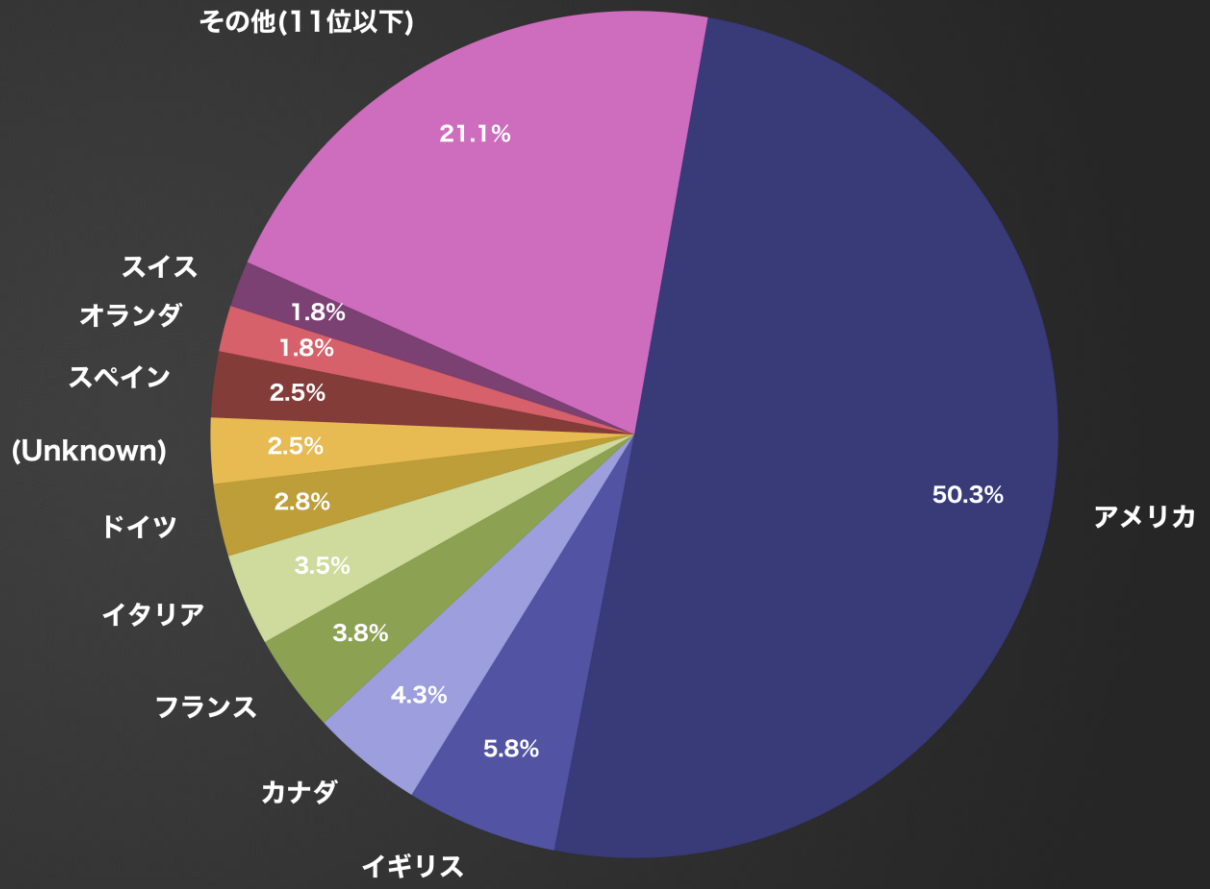
Know your enemy.
Defense leadership.

● 月別内訳 被害国TOP10 （ 2024年 2 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	200	50.3	+ 46
イギリス	23	5.8	+ 7
カナダ	17	4.3	+ 2
フランス	15	3.8	± 0
イタリア	14	3.5	+ 7
ドイツ	11	2.8	+ 5
(Unknown)	10	2.5	+ 9
スペイン	10	2.5	+ 5
オランダ	7	1.8	+ 5
スイス	7	1.8	+ 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）



※ 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。

Created by Cyber Intelligence Group

M|B|S|D Know your enemy. Defense leadership.®

2024

2

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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑩

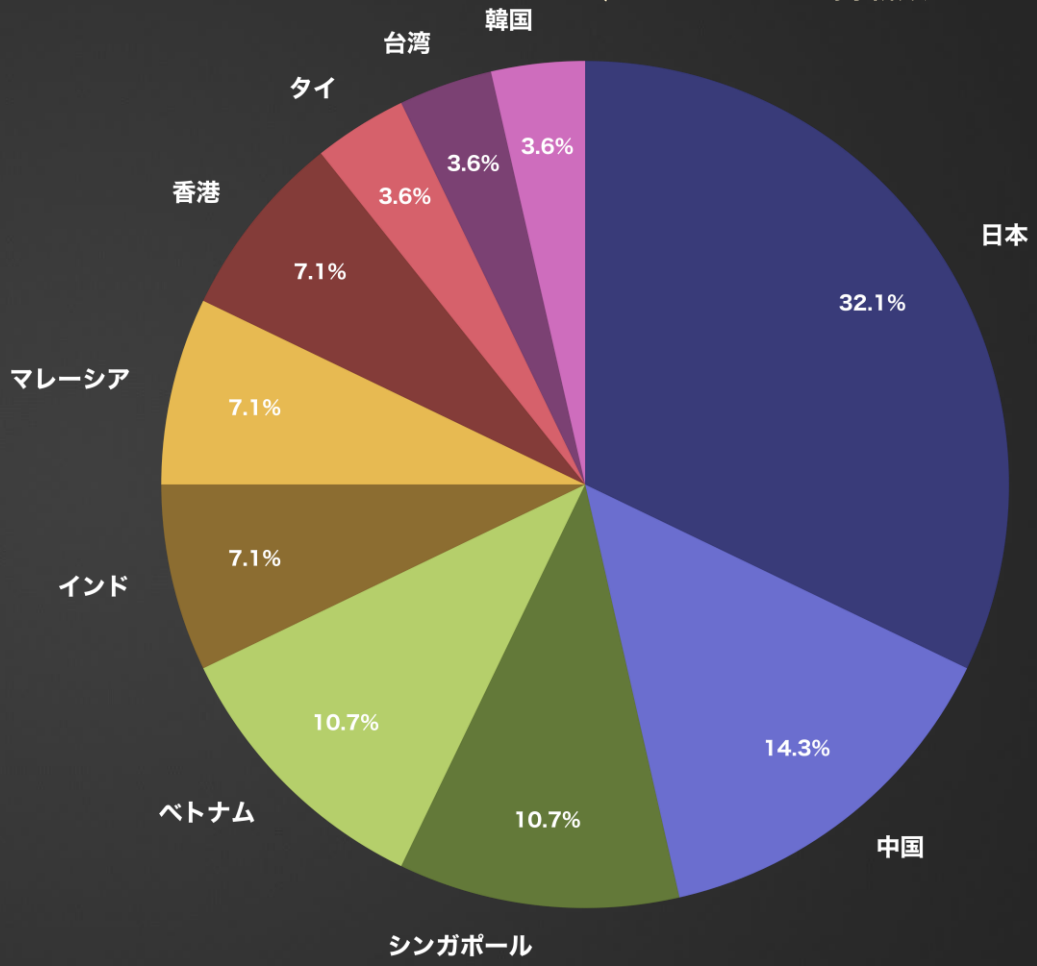
Know your enemy.
Defense leadership.®

● 月別内訳 被害国TOP10 （ 2023年 12 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)
日本	9	32.1	+ 4
中国	4	14.3	+ 1
シンガポール	3	10.7	- 2
ベトナム	3	10.7	+ 3
インド	2	7.1	- 4
マレーシア	2	7.1	- 1
香港	2	7.1	+ 1
タイ	1	3.6	- 3
台湾	1	3.6	- 6
韓国	1	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）



※ 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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑩

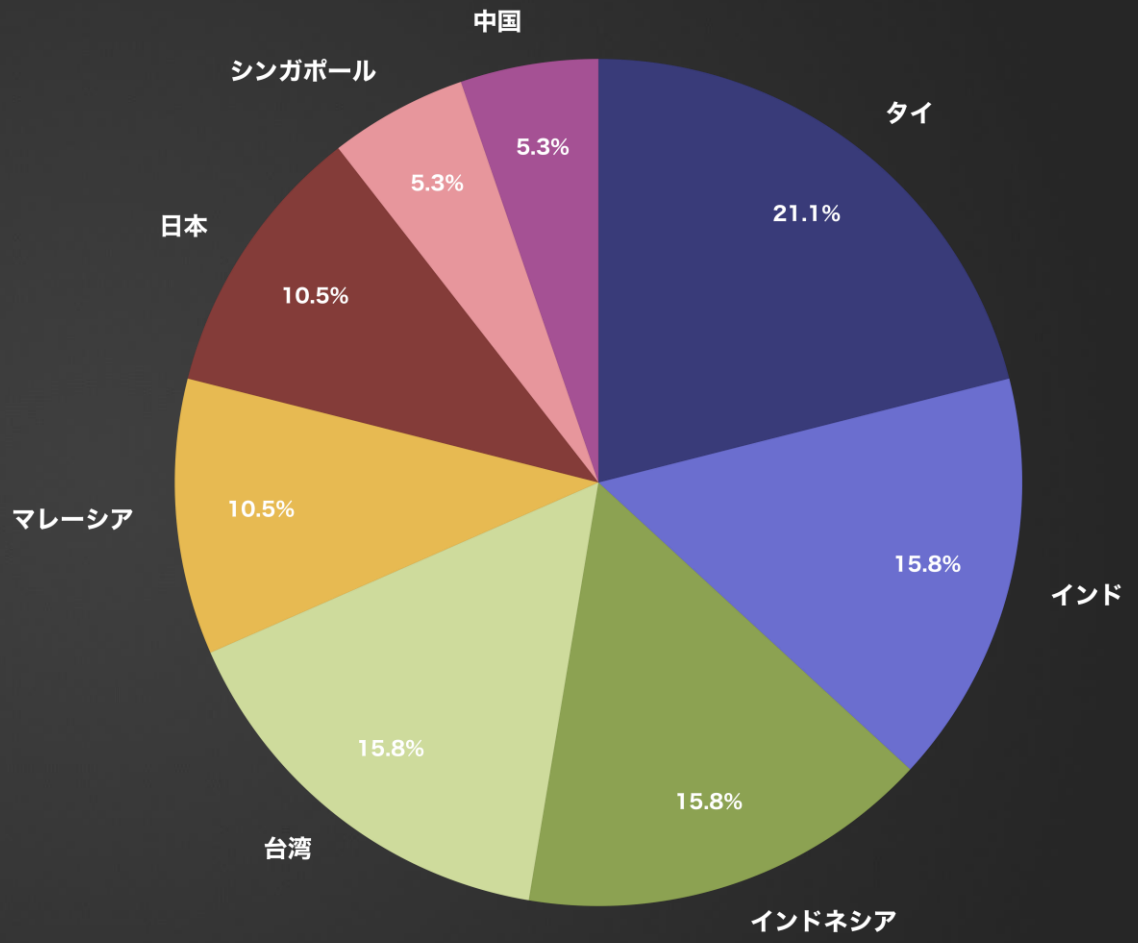
Know your enemy.
Defense leadership.

● 月別内訳 被害国TOP10 （ 2024年 1 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)
タイ	4	21.1	+ 3
インド	3	15.8	+ 1
インドネシア	3	15.8	+ 3
台湾	3	15.8	+ 2
マレーシア	2	10.5	± 0
日本	2	10.5	- 7
シンガポール	1	5.3	- 2
中国	1	5.3	- 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）



※ 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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑩

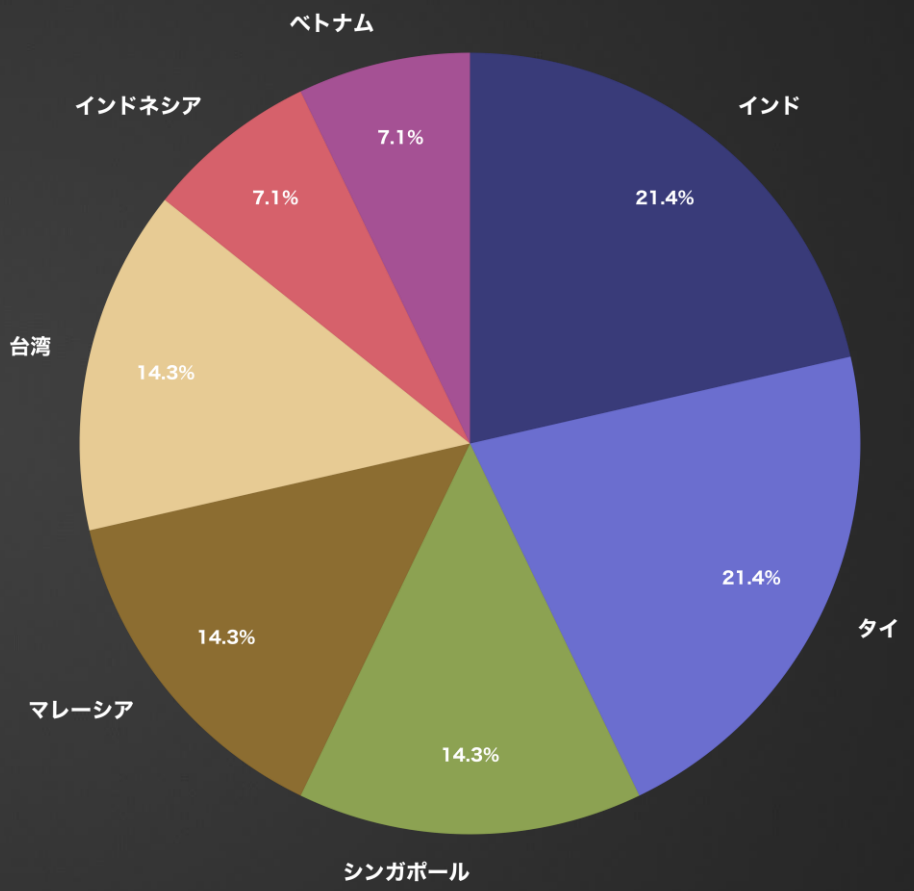
Know your enemy.
Defense leadership.

● 月別内訳 被害国TOP10 （ 2024年 2 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	3	21.4	± 0
タイ	3	21.4	- 1
シンガポール	2	14.3	+ 1
マレーシア	2	14.3	± 0
台湾	2	14.3	- 1
インドネシア	1	7.1	- 2
ベトナム	1	7.1	+ 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。

Created by Cyber Intelligence Group

Know your enemy.
Defense leadership.®

2024

2

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。

 ／Rev 1.00

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑬

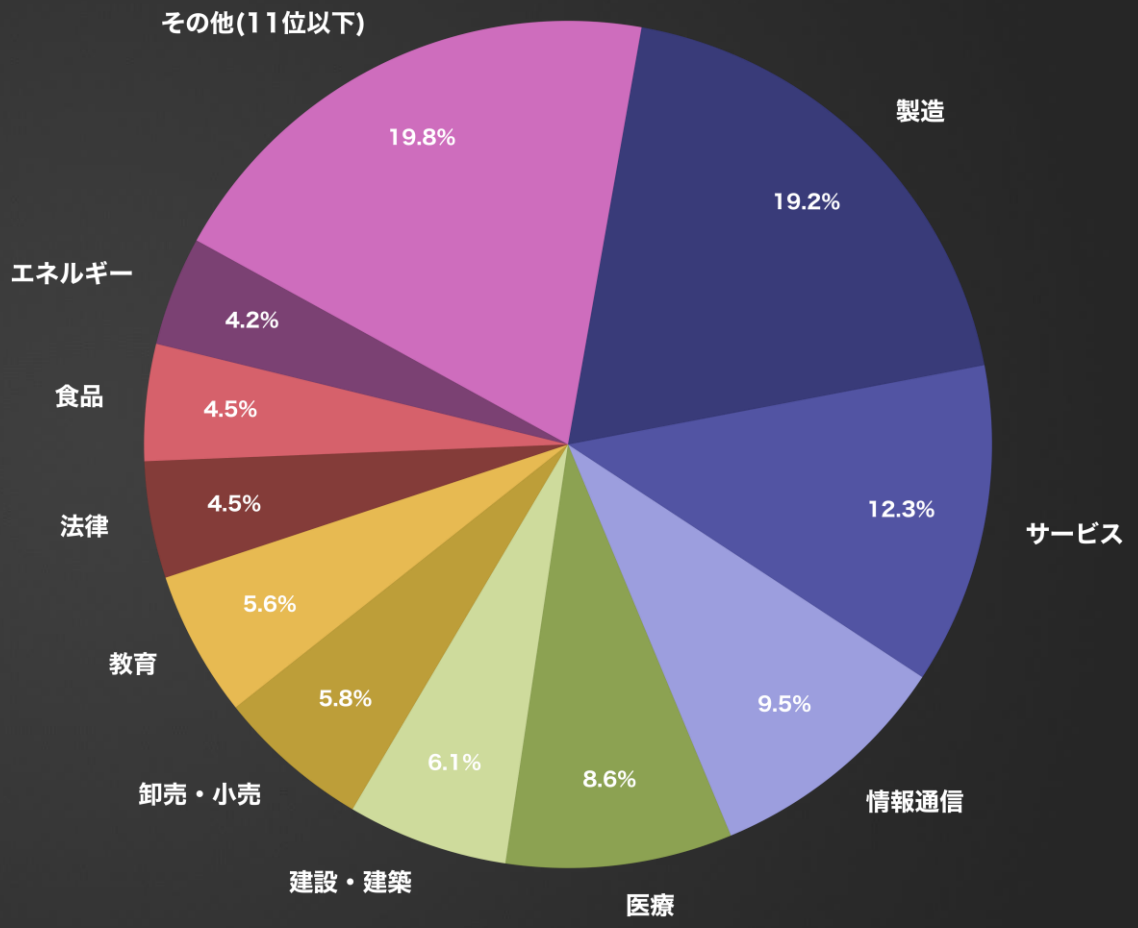
Know your enemy.
Defense leadership.®

● 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	69	19.2	- 39
サービス	44	12.3	- 15
情報通信	34	9.5	+ 14
医療	31	8.6	- 14
建設・建築	22	6.1	- 14
卸売・小売	21	5.8	- 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	+ 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）



※ 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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑬

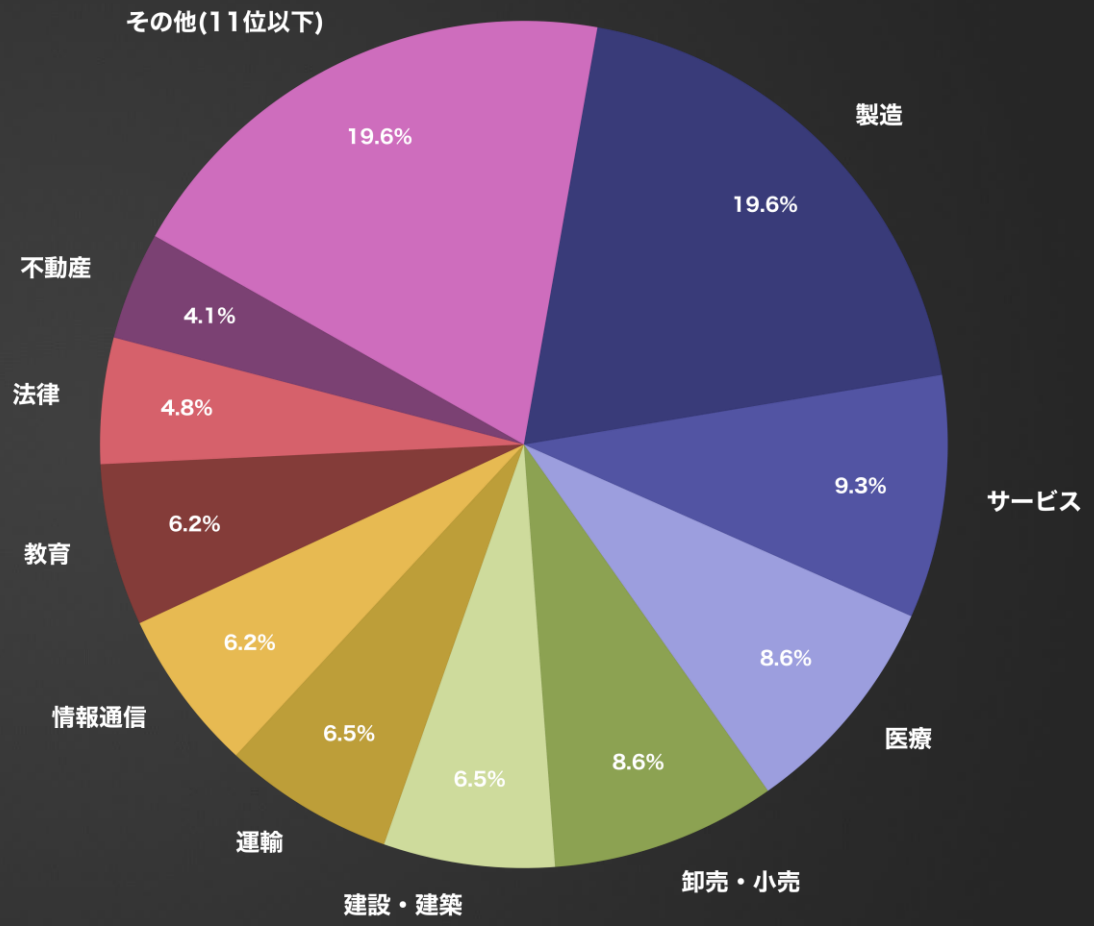
Know your enemy.
Defense leadership.®

● 月別内訳 業種 TOP10 （2024年 1 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	57	19.6	- 12
サービス	27	9.3	- 17
医療	25	8.6	- 6
卸売・小売	25	8.6	+ 4
建設・建築	19	6.5	- 3
運輸	19	6.5	+ 10
情報通信	18	6.2	- 16
教育	18	6.2	- 2
法律	14	4.8	- 2
不動産	12	4.1	+ 4

▼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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑬

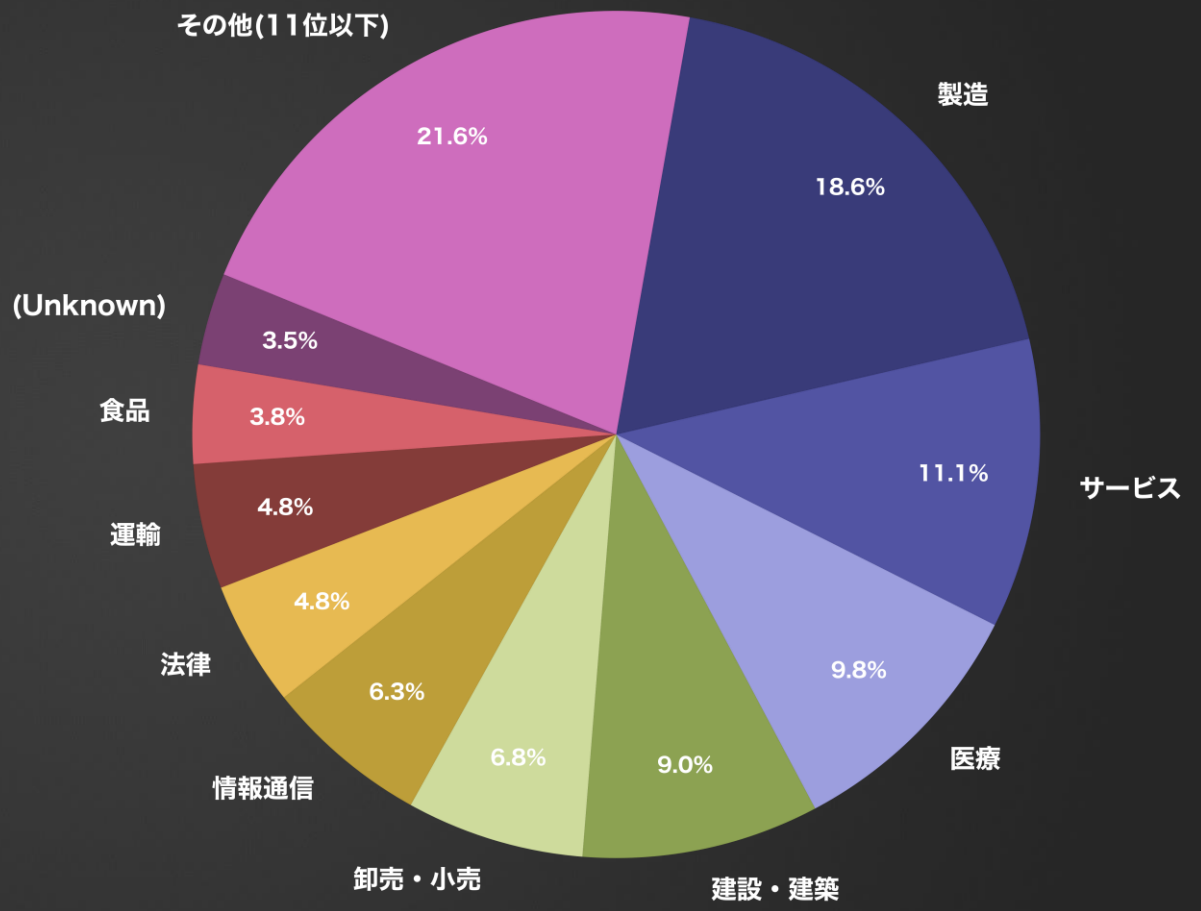
Know your enemy.
Defense leadership.

● 月別内訳 業種 TOP10 （2024年 2 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	74	18.6	+ 17
サービス	44	11.1	+ 17
医療	39	9.8	+ 14
建設・建築	36	9.0	+ 17
卸売・小売	27	6.8	+ 2
情報通信	25	6.3	+ 7
法律	19	4.8	+ 5
運輸	19	4.8	± 0
食品	15	3.8	+ 4
(Unknown)	14	3.5	+ 13

▼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。

Created by Cyber Intelligence Group

Know your enemy.
Defense leadership.®

2024

2

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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑭

Know your enemy.
Defense leadership.

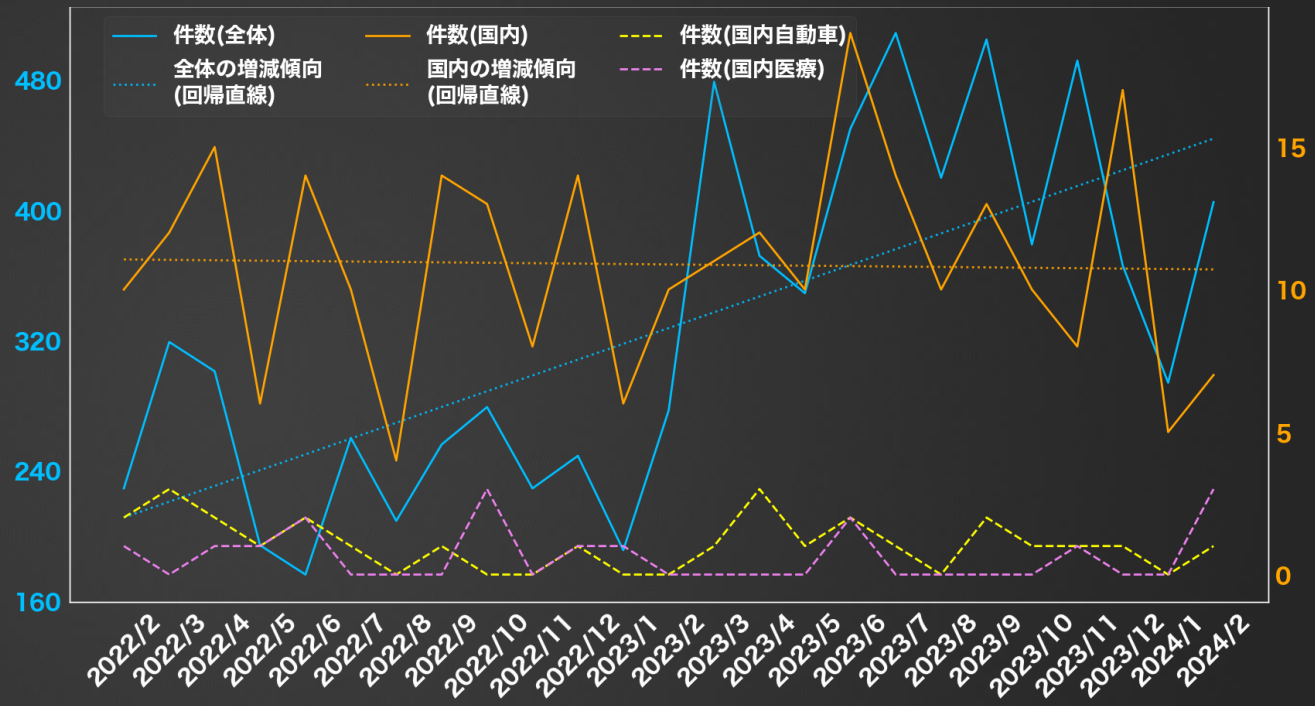
● 被害数の推移（2022年2月～2024年2月／全世界及び国内）(MBSD調べ)

※件数(国内)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)
2022/2	229	10	2	1
2022/3	319	12	3	0
2022/4	301	15	2	1
2022/5	194	6	1	1
2022/6	155	14	2	2
2022/7	260	10	1	0
2022/8	184	4	0	0
2022/9	256	14	1	0
2022/10	279	13	0	3
2022/11	229	8	0	0
2022/12	249	14	1	1
2023/1	191	6	0	1
2023/2	277	10	0	0
2023/3	479	11	1	0
2023/4	372	12	3	0
2023/5	349	10	1	0
2023/6	450	19	2	2
2023/7	509	14	1	0
2023/8	420	10	0	0
2023/9	505	13	2	0
2023/10	379	10	1	0
2023/11	492	8	1	1
2023/12	366	17	1	0
2024/1	294	5	0	0
2024/2	405	7	1	3
合計	8143	272	27	16

▼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。

Created by Cyber Intelligence Group

M|B|S|D Know your enemy. Defense leadership.

2024

2

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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑮

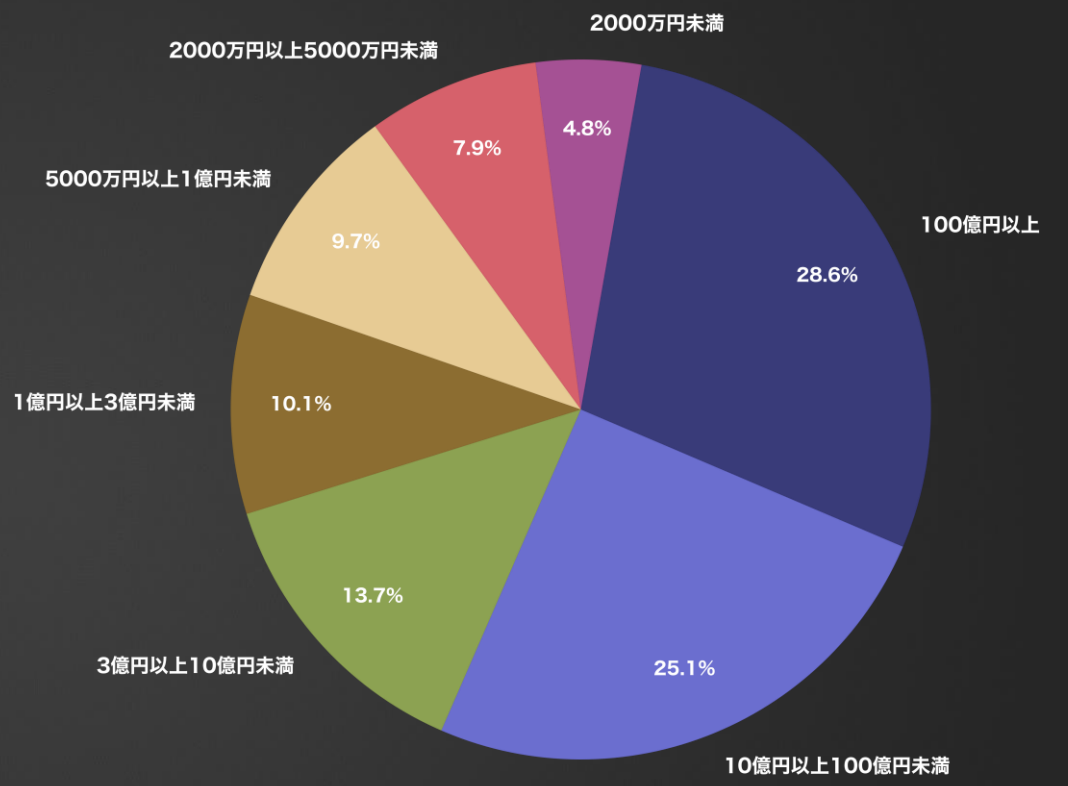
Know your enemy.
Defense leadership.

● 月別内訳 資本金別 （ 2022年2月～2024年2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

資本金	件数	割合(%)
100億円以上	65	28.6
10億円以上100億円未満	57	25.1
3億円以上10億円未満	31	13.7
1億円以上3億円未満	23	10.1
5000万円以上1億円未満	22	9.7
2000万円以上5000万円未満	18	7.9
2000万円未満	11	4.8

▼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）



▼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：32.5%
・10億円未満が該当するとした場合：46.2%

（※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）

※ 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。

Created by Cyber Intelligence Group

Know your enemy.
Defense leadership.®

2024

2

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。

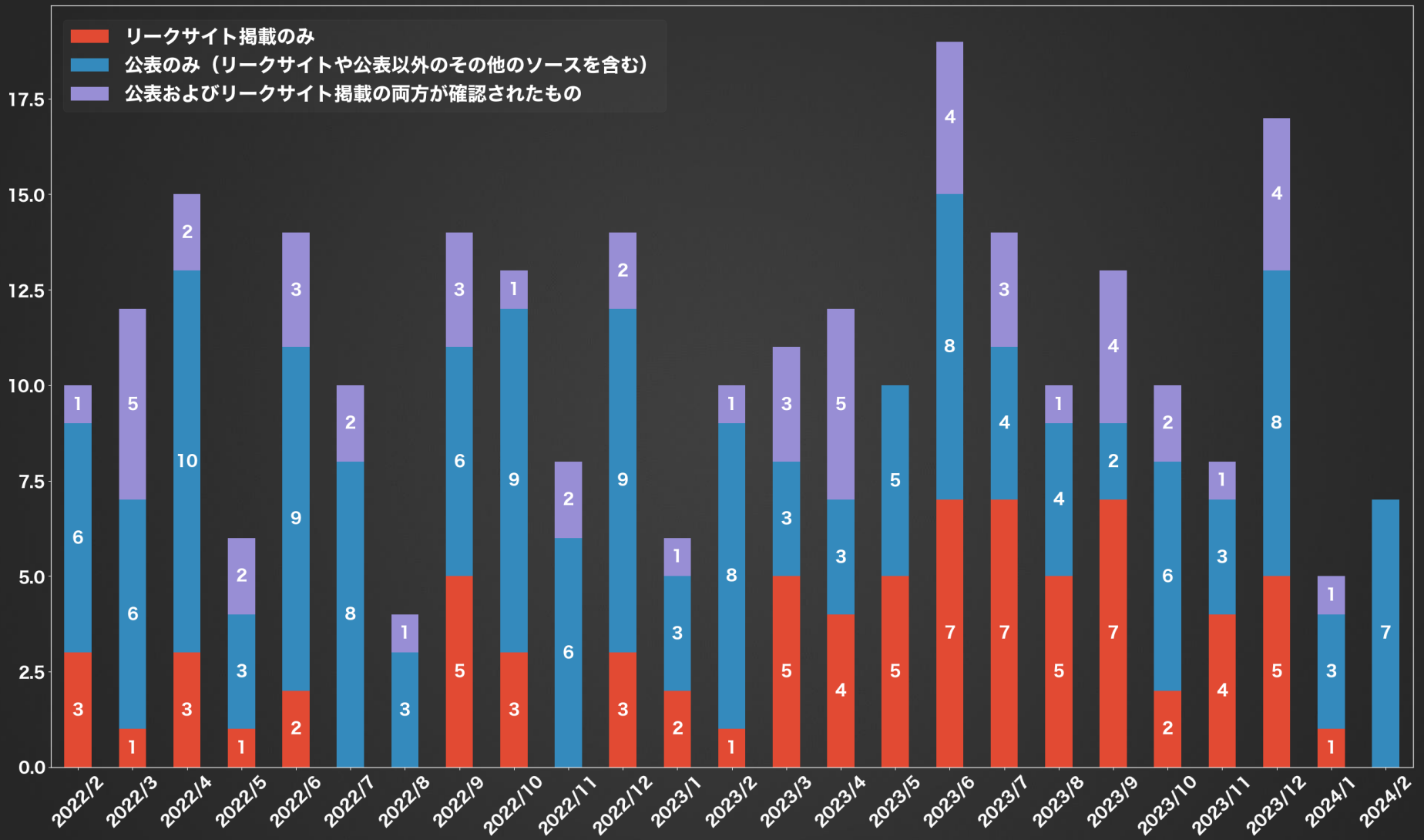
Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑯

Know your enemy.
Defense leadership.®

● 公表割合 月別内訳 （2022年2月～2024年2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



（※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。

Created by Cyber Intelligence Group

Know your enemy.
Defense leadership.®

公となった国内被害組織 概要一覧

2024

2

※ 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。

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑰

M|B|S|D® Know your enemy. Defense leadership.®

公となった国内被害組織概要一覧（過去1年間／2023年2月～2024年2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
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
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)	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	LockBit	自動車部品メーカー(海外拠点)
2023/5	LockBit	デザイン事務所
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)	インテリア販売会社
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	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)	化粧品メーカー
2023/7	(Unknown)	大手信販会社
2023/7	(Unknown)	学校法人
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)
2023/7	CLOP	たばこ製造販売会社(海外拠点)
2023/7	CLOP	大手電気機器メーカー(海外拠点)
2023/7	CLOP	自動車部品メーカー(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	PLAY	大手生活用品メーカー(海外拠点)
2023/7	NoEscape	土木建設会社
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

※ 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。

（※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）

Created by Cyber Intelligence Group

暴露型ランサムウェア攻撃統計CIGマンスリーレポート – ⑰

Know your enemy.
Defense leadership.®

公となった国内被害組織概要一覧（過去1年間／2023年2月～2024年2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
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
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)	国立大学
2023/10	(Unknown)	制御機器メーカー
2023/10	(Unknown)	小売店経営会社
2023/10	AlphV / BlackCat	大手専門商社
2023/10	PLAY	眼鏡メーカー
2023/10	NoEscape	自動車部品メーカー
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	畜産機器メーカー
2023/11	AlphV / BlackCat	大手電子部品メーカー
2023/11	Medusa	金融サービス会社(海外拠点)
2023/11	Hunters International	大手機械部品メーカー
2023/11	INC Ransom	大手輸送用機器メーカー(海外拠点)

被害月	攻撃グループ	業種概要
2023/12	(Unknown)	大手出版社
2023/12	(Unknown)	地方自治体
2023/12	(Unknown)	IoTサービス会社
2023/12	(Unknown)	地域事業
2023/12	(Unknown)	レジャー用品販売
2023/12	(Unknown)	一般社団法人
2023/12	(Unknown)	システムコンサルティング会社
2023/12	(Unknown)	地方新聞社
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	BlackBasta	大手ガラス製品メーカー(海外拠点)
2023/12	DragonForce	大手食品メーカー(海外拠点)
2024/1	(Unknown)	漁網総合メーカー
2024/1	(Unknown)	建設機材サービス
2024/1	LockBit	化学メーカー
2024/1	LockBit	包装用品メーカー
2024/1	LockBit	公益財団法人
2024/2	(Unknown)	医療関連製品卸売業
2024/2	(Unknown)	自動車部品メーカー
2024/2	(Unknown)	医療検査機関
2024/2	(Unknown)	ITサービス会社
2024/2	(Unknown)	総合商店運営
2024/2	(Unknown)	医療機関
2024/2	(Unknown)	物流サービス会社

※ 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。

（※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）

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑱

Know your enemy.
Defense leadership.®

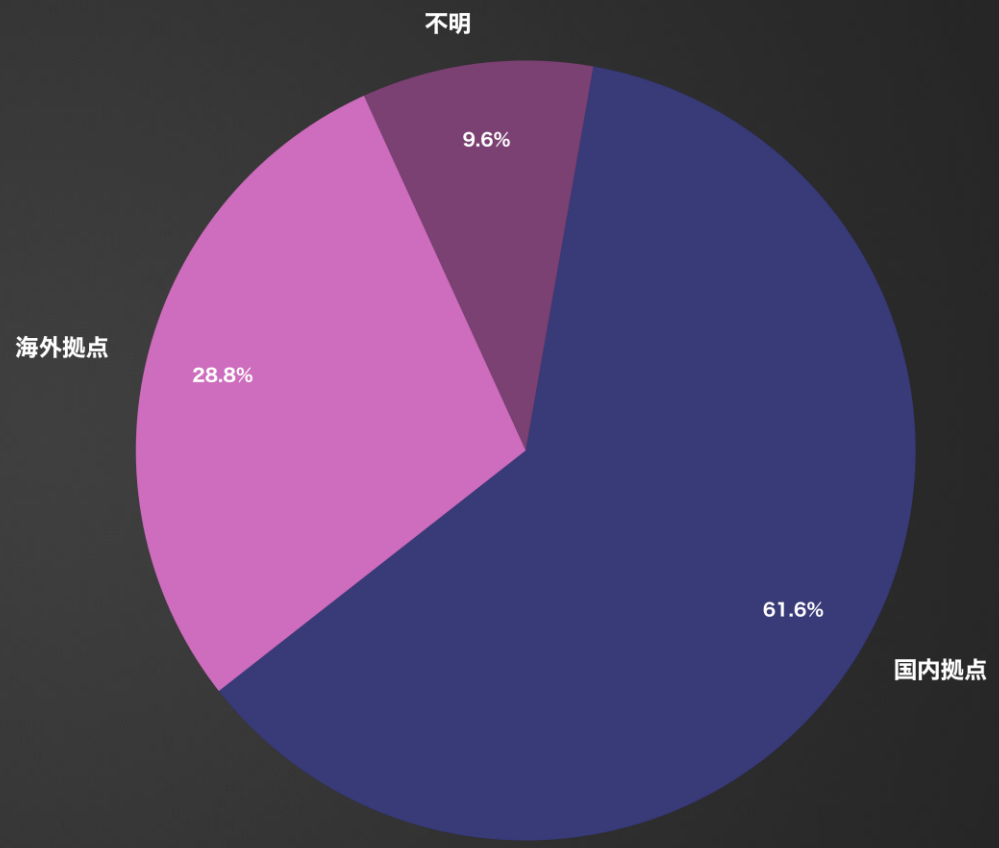
● 公となった国内被害組織における拠点割合（ 過去1年間／2023年2月～2024年2月）(MBSD調べ)

（※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）

※
「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	90	61.6
海外拠点	42	28.8
不明	14	9.6

▼ランサムウェア攻撃を受けた日本関連組織の拠点別割合



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

※ 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。

Created by Cyber Intelligence Group

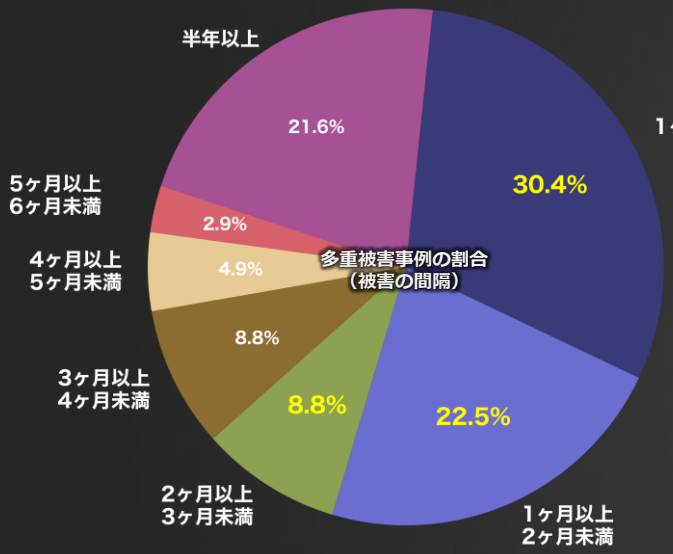
暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑲

Know your enemy.
Defense leadership.®

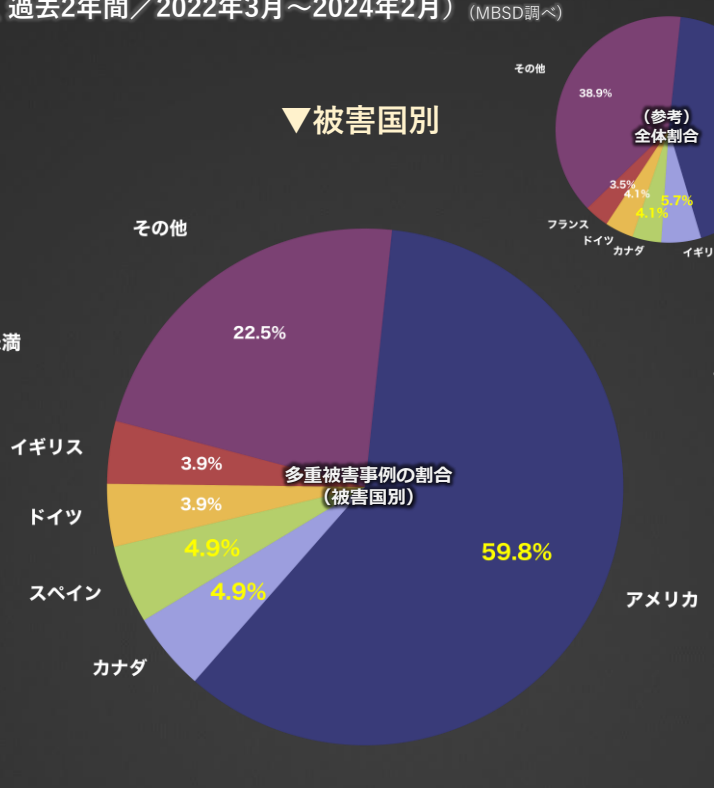
※多重被害：一度ランサムウェア攻撃の被害を受けた組織が異なる時期に異なる攻撃グループのリークサイトに再び掲載されるケース

多重被害に遭った被害組織の傾向と分析（過去2年間／2022年3月～2024年2月）(MBSD調べ)

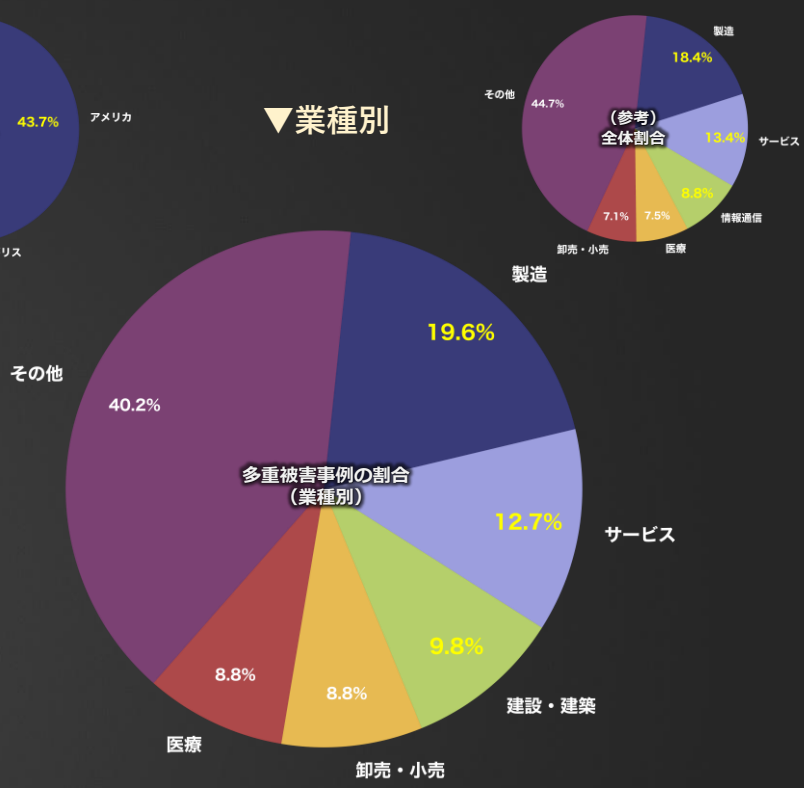
▼被害の間隔
（一度目の被害から二度目の被害までの間隔）



▼被害国別



▼業種別



▶多重被害に遭った組織数の累計：101件（全体7960件中）

※異なる攻撃グループによるリークサイトへの掲載件数を元に算出

全体母数からの割合は少ないものの、一度ランサムウェア攻撃を受けた被害組織は、異なる時期に異なる攻撃グループによって再びリークサイトへ掲載される被害を繰り返す場合があり、中には３回以上被害に遭うケースもある。これは事後対応が不十分で再び侵入されるケースや、流出した暴露データが裏で共有・拡散され繰り返し脅されるケースなどの背景があると考えられる。
被害国や業種の観点ではほぼ全体割合の縮図となっているものの、最も注目すべきは繰り返される「被害の間隔」であり、実に50%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あ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。

※ 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。

Created by Cyber Intelligence Group

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

Created by Cyber Intelligence Group