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4月号 Rev 1.00
(2024年3月分)

2024
3

Created by Cyber Intelligence Group

今月のハイライト

「Operation Chronos」後のLockBitにみえる状況変化

LockBitランサムウェア攻撃グループは、2019年頃からその名を世界に知らしめており、ランサムウェア攻撃グループとしては最も長い歴史を持つ。
2024年2月20日の日本時間未明、法執行機関の共同作戦「Operation Chronos」によってLockBitのサーバーが押収され、彼らのリークサイトはダウンした。しかし、2月25日頃には新しいリークサイトやミラーサイトが複数登場し、まもなくLockBitの活動は再開された。
2月に101件だった掲載数は、3月も94件に上り、LockBitの勢いは一見すると衰え知らずのように受け止められる。しかし調査の結果、「OperationChronos」後の暴露に当たる3月の94件のリークのうち、38件は過去にLockBitが掲載したものであることが判明、実質的に新規となる掲載数は56件であった。このような状況から彼らがリークサイト掲載数を誇張し、組織の健全さを装っていると捉える見方もできる。

また、注目すべき別の観点として、新規掲載されたそれら56件の中で7件がAlphV/BlackCat（以下、AlphV）によって既に掲載された被害組織名と重複していることが判明した点も挙げられる。

> AlphVは2023年12月にLockBitと同じく法執行機関によってリークサイトがダウンさせられたものの、まもなくミラーサイトで活動を継続。その後、2024年3月初旬に突如リークサイトが法執行機関の押収を主張する表示に変わり、その後アクセス不能となった。
> この件については法執行機関が関与を否定した上、同期間に、AlphVのアフィリエイトの一員と主張する者が、AlphVに身代金2200万ドルを持ち逃げされたと暴露する騒ぎがあり、“出口詐欺”が疑われている。

現時点でAlphVの関係者がLockBitに合流したのかを断言することはできないが、LockBitはAlphVのリークサイトがダウンされた2023年12月頃にハッカーフォーラム上でAlphVやその他攻撃グループのアフィリエイト、開発者を勧誘しており、「データのバックアップがあれば、LockBitリークサイトを通じて恐喝活動を継続できる」と発言しているのを確認している。
こうした背景からLockBitとAlphVの間になんらかの接点が生まれた可能性も否定できない状況が垣間見える。

また4月8日には、前述の身代金2200万ドルをAlphVに支払ったとされる米大手医療関連組織への攻撃声明がRansomhubのリークサイトに掲載されたことを確認。 その声明では「AlphVが身代金を持ち逃げしたが、データは我々が保有しており、被害組織との取引が成立しない場合は最高額で入札した者にデータを売却する」という主旨が述べられていることから、AlphVのアフィリエイトがRansomhubに被害組織情報を持ち込んだと考えられる。
一方で視点を変えて見ると、今回の状況は結果的に、本レポートのp.33で詳しく分析している、”異なる攻撃グループから複数回恐喝される多重被害”にも該当する事例となったことは興味深い。

なお、全攻撃グループのリークサイト掲載の総数を俯瞰して見てみると、従来まではLockBitやAlphVがその割合の多くを占め全体数を押し上げる形となっていたため、前述のLockBitやAlphVの動向を鑑みると3月は掲載総数が減少すると思われたが、実際には先月の394件に比べ407件に増加したという興味深い結果が明らかになった。
その内状としては、上記のとおりLockBitによる過去被害の再掲載という印象操作の影響などもある一方で、我々の調査の結果、BlackBasta、PLAY、Medusa、Ransomhubといったグループが先月に比べ掲載数を実際に大きく増やし全体数を引き上げたという状況も判明した。諸々のタイミングを考慮すると、LockBitやAlphVの混乱がアフィリエイトの内部移動などにより他グループの活動に影響をもたらしたとみれなくもない。そう考えるとLockBitがそうした内部混乱を悟られないよう掲載数を誇張し平静を装っている可能性なども憶測できてしまう状況にあるといえるだろう。

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。

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）

● 監視している攻撃グループ数：164グループ（※1）

※1 活動停止した攻撃グループを含む

→内2024年3月にリークサイト掲載を確認した攻撃グループ数：34件

● 監視中の攻撃グループ一覧

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

※ 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

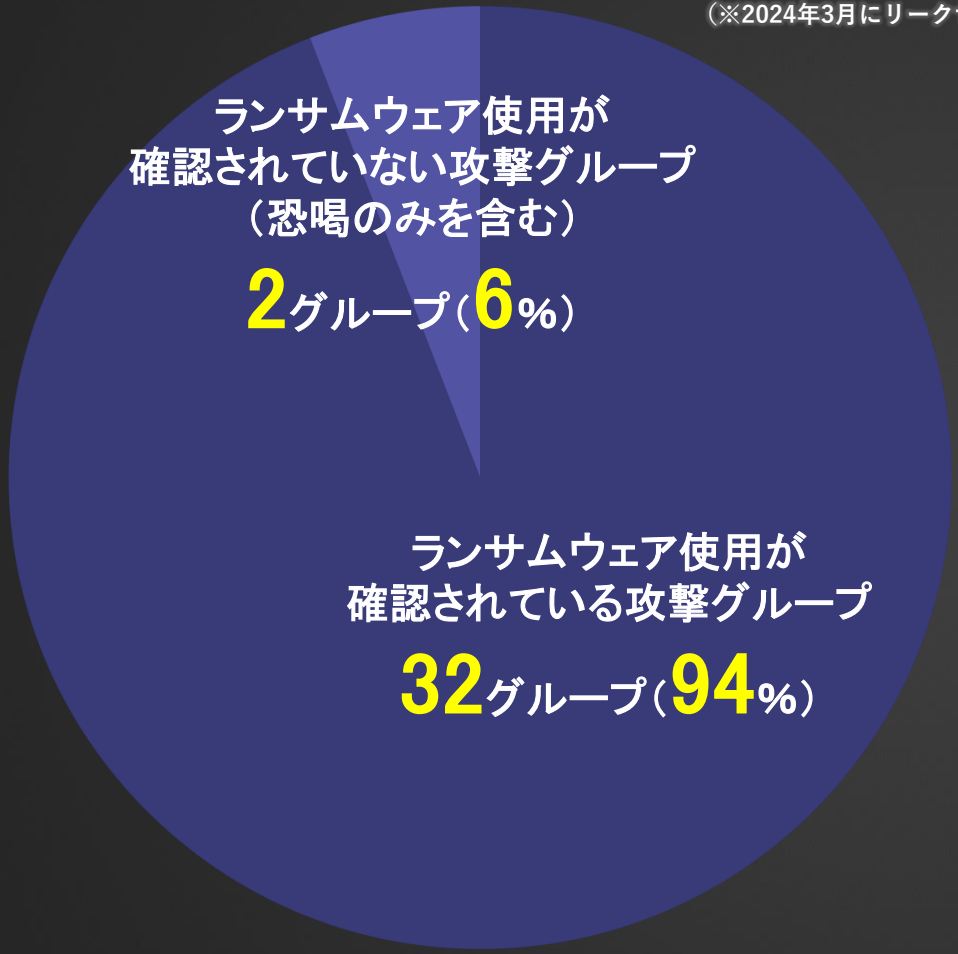
監視中のランサムウェア攻撃グループ情報（ランサムウェア使用の割合）

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3月）

（※2024年3月にリークサイト掲載を確認した攻撃グループ全34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3月に活動中である事が確認された全34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

Know your enemy.
Defense leadership.®

2024

3

年間 統計

（全世界）

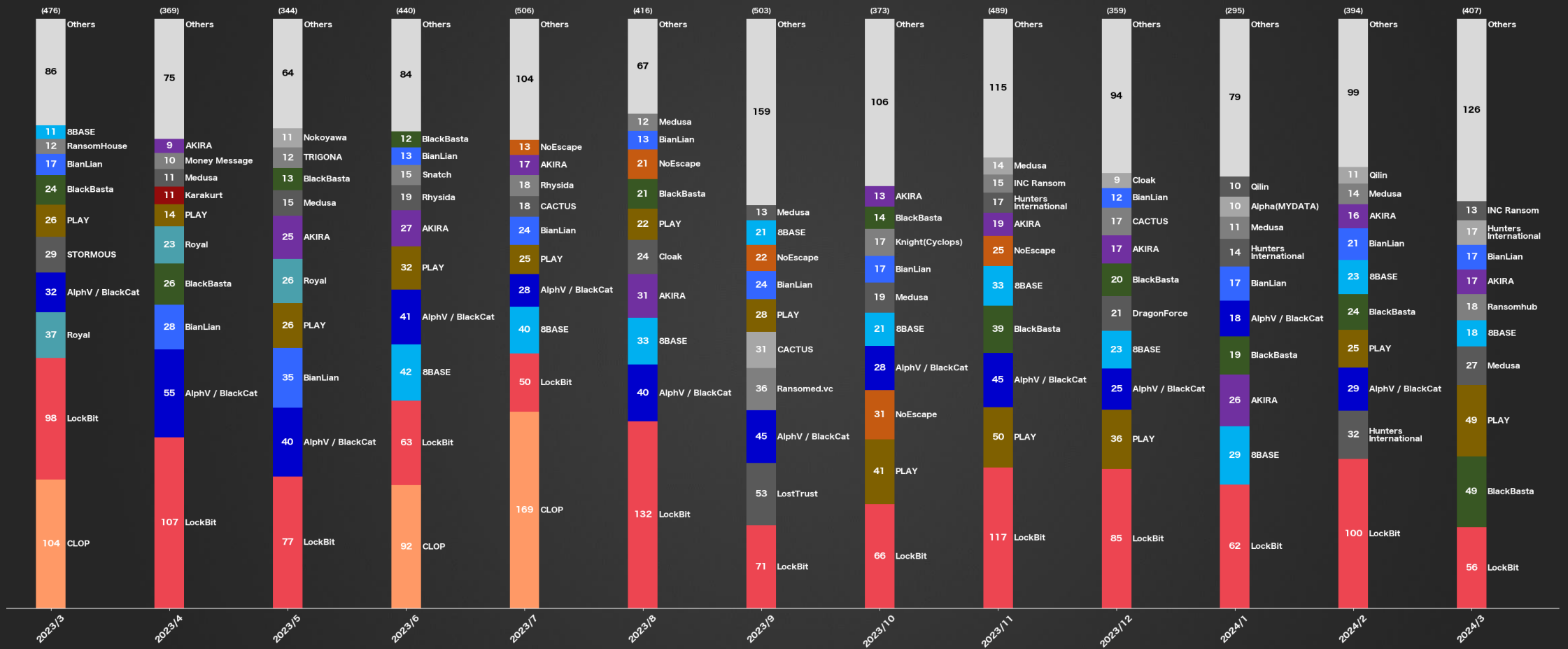
※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
　（日本にフォーカスした一部の表／グラフのみ、公表や報道から判明した数を加味し集計）
※ 国内被害組織に関する各種データについては、海外拠点（支社／関連会社）を含む。
※ 業種分類や集計方法を含む本レポートの各データ（値）はMBSD独自の観測および集計結果となる。
※ これらはあくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
※ ごく一部のランサムウェアの使用が明確に確認されていな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

M|B|S|D 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3月～2024年3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.

攻撃グループ 月別統計

（全世界）

（過去3ヶ月分）

2024

3

※ 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

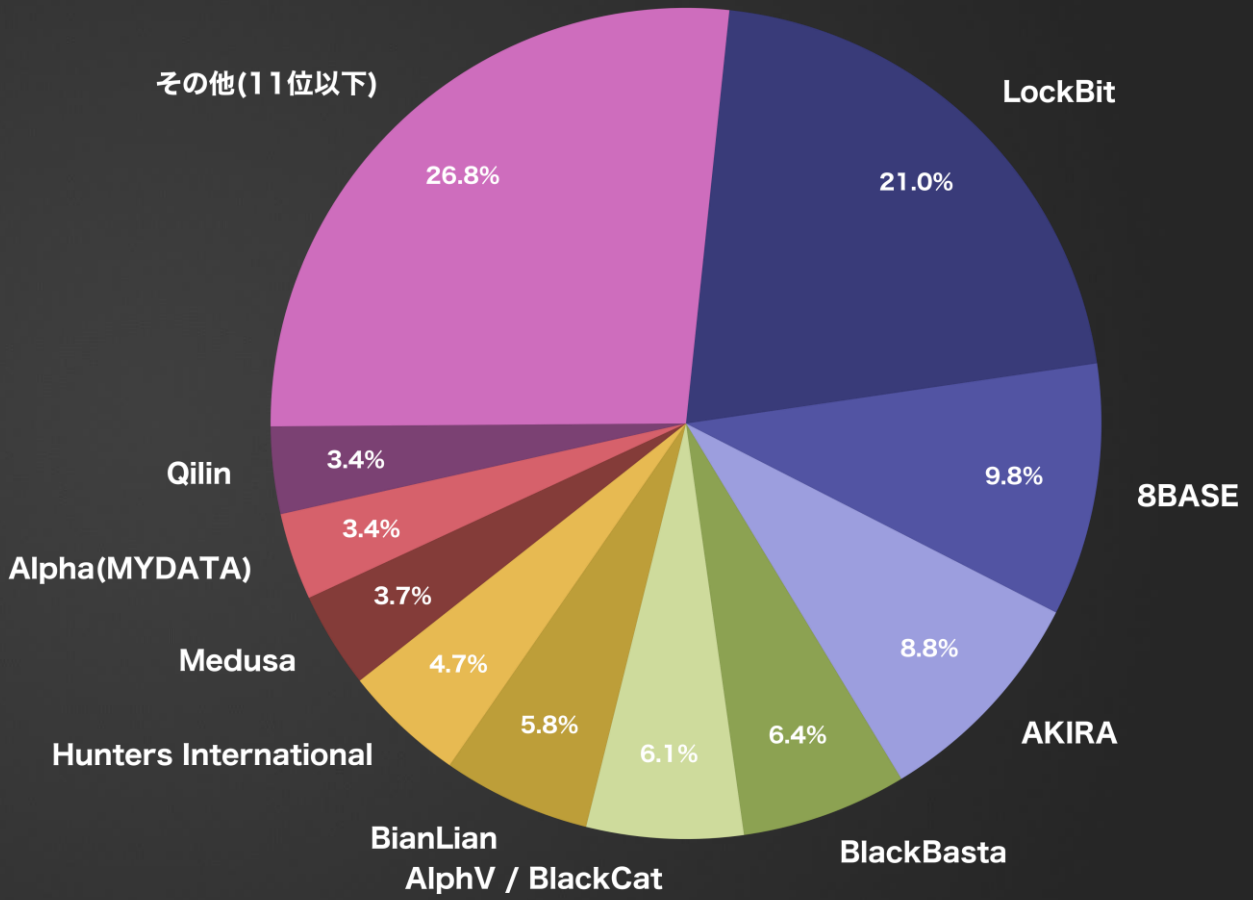
Know your enemy.
Defense leadership.®

● 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	21.0	- 23
8BASE	29	9.8	+ 6
AKIRA	26	8.8	+ 9
BlackBasta	19	6.4	- 1
AlphV / BlackCat	18	6.1	- 7
BianLian	17	5.8	+ 5
Hunters International	14	4.7	+ 8
Medusa	11	3.7	+ 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

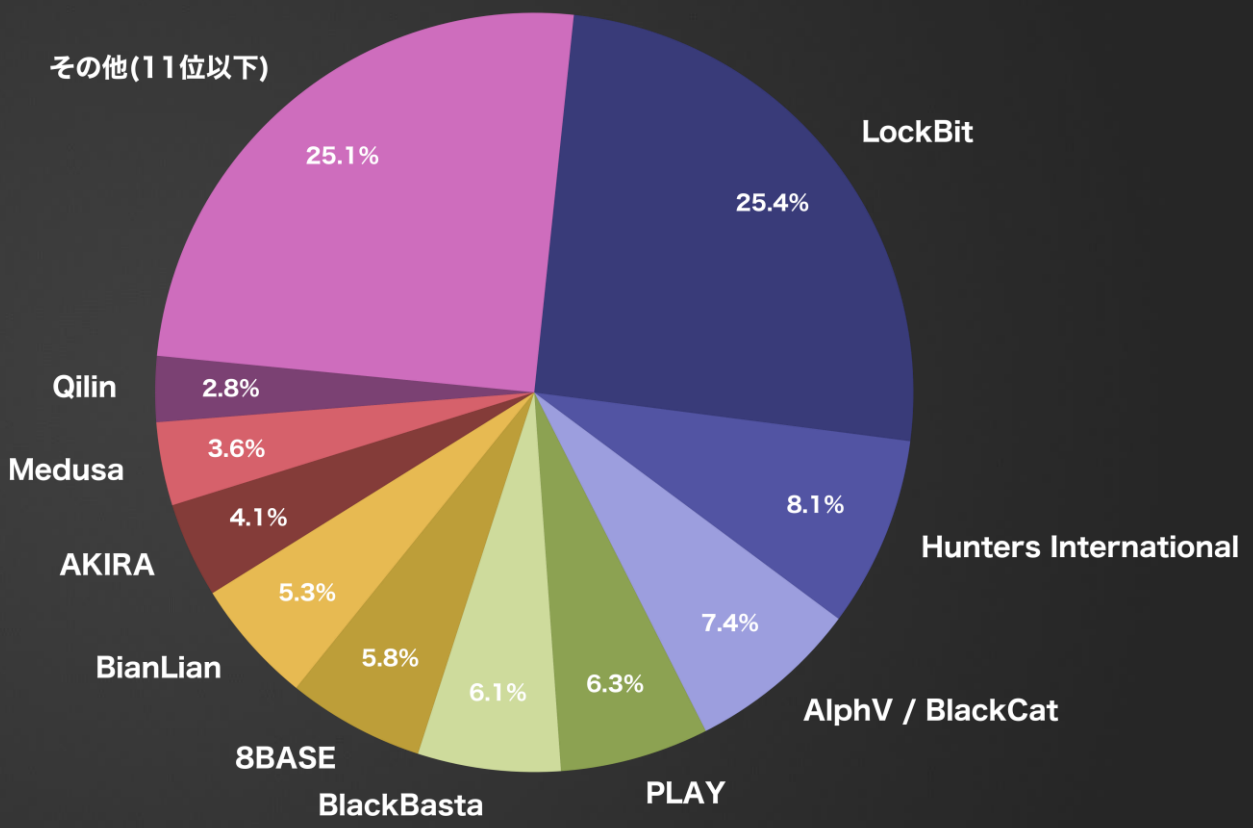
Know your enemy.
Defense leadership.®

● 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	25.4	+ 38
Hunters International	32	8.1	+ 18
AlphV / BlackCat	29	7.4	+ 11
PLAY	25	6.3	+ 20
BlackBasta	24	6.1	+ 5
8BASE	23	5.8	- 6
BianLian	21	5.3	+ 4
AKIRA	16	4.1	- 10
Medusa	14	3.6	+ 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

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

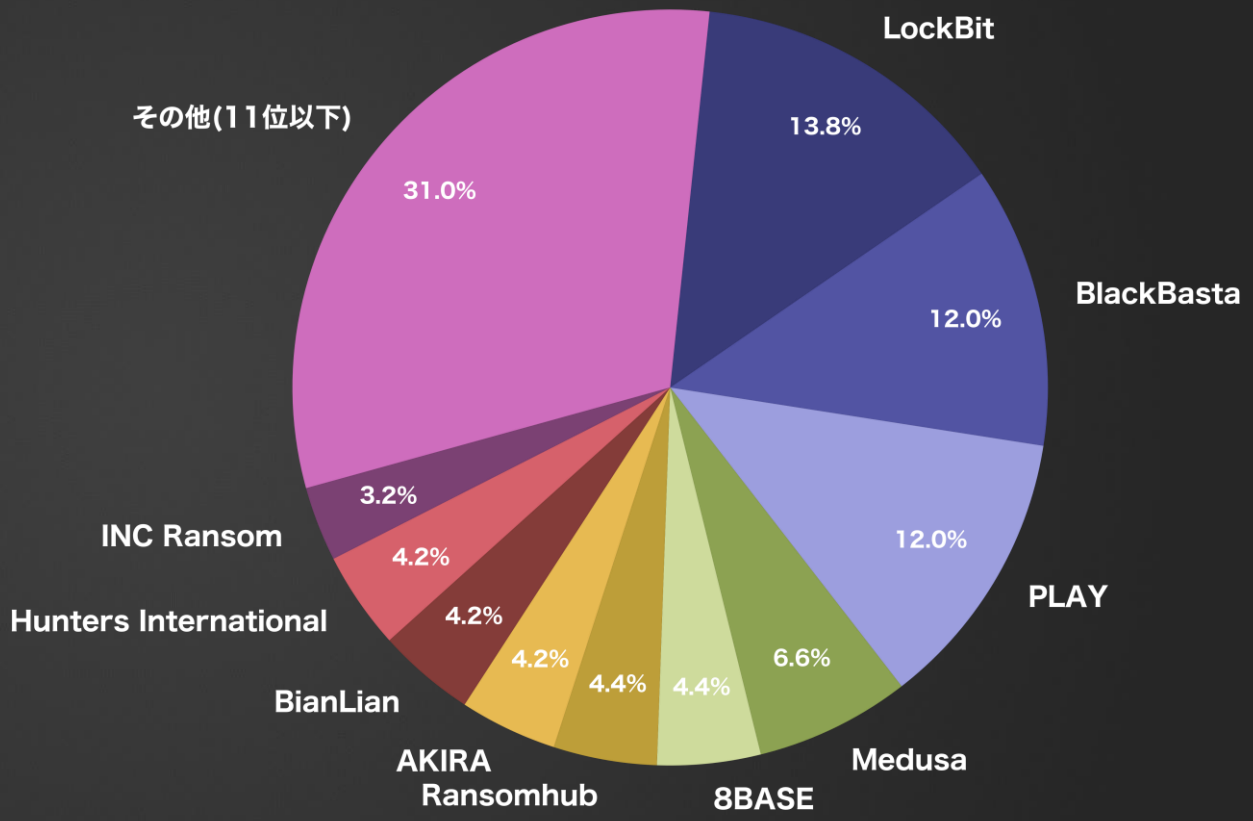
Know your enemy.
Defense leadership.

● 月別内訳 攻撃グループ TOP10 （2024年 3 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	56	13.8	- 44
BlackBasta	49	12.0	+ 25
PLAY	49	12.0	+ 24
Medusa	27	6.6	+ 13
8BASE	18	4.4	- 5
Ransomhub	18	4.4	+ 14
AKIRA	17	4.2	+ 1
BianLian	17	4.2	- 4
Hunters International	17	4.2	- 15
INC Ransom	13	3.2	+ 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

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

2024

3

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

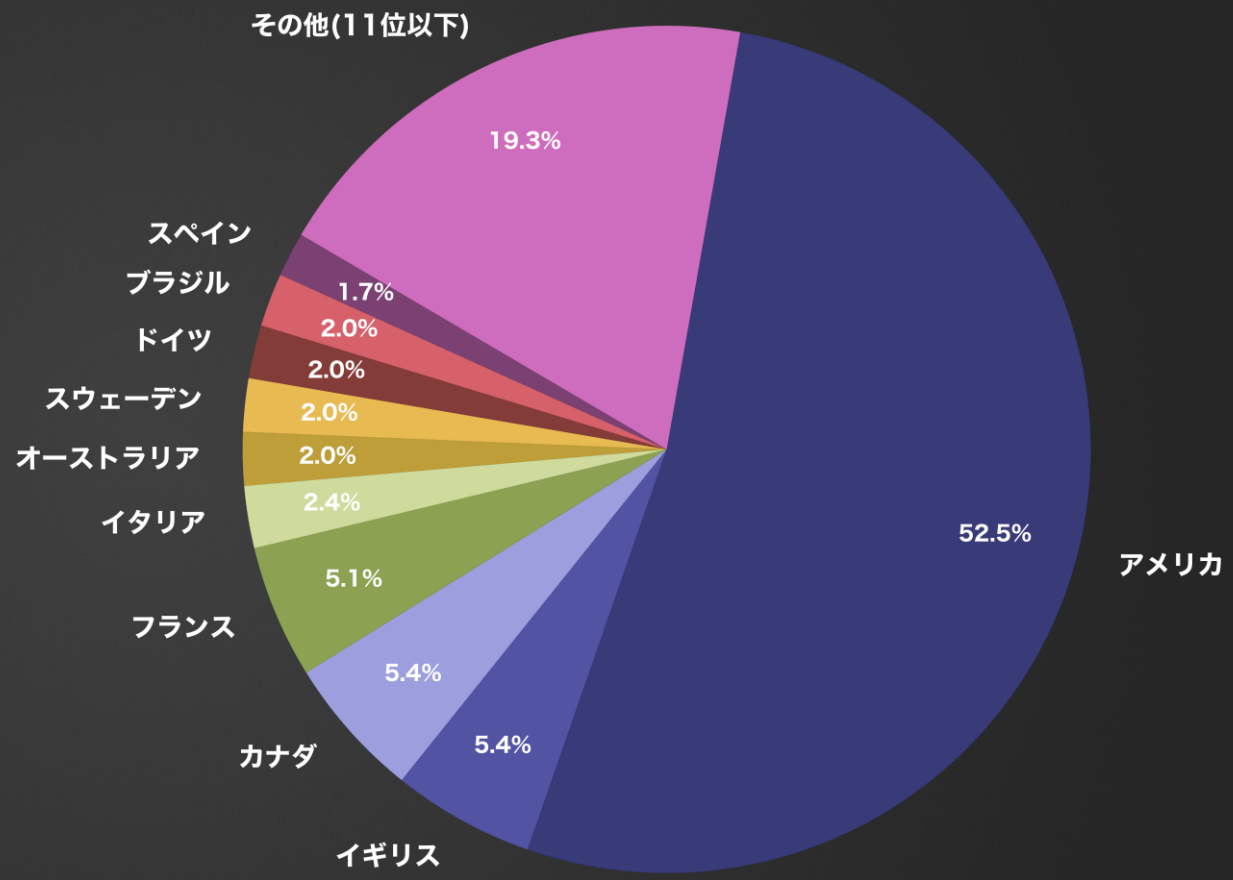
Know your enemy.
Defense leadership.®

● 月別内訳 被害国TOP10 （ 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	155	52.5	- 14
イギリス	16	5.4	- 8
カナダ	16	5.4	± 0
フランス	15	5.1	+ 5
イタリア	7	2.4	± 0
オーストラリア	6	2.0	- 1
スウェーデン	6	2.0	+ 3
ドイツ	6	2.0	- 12
ブラジル	6	2.0	+ 2
スペイン	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

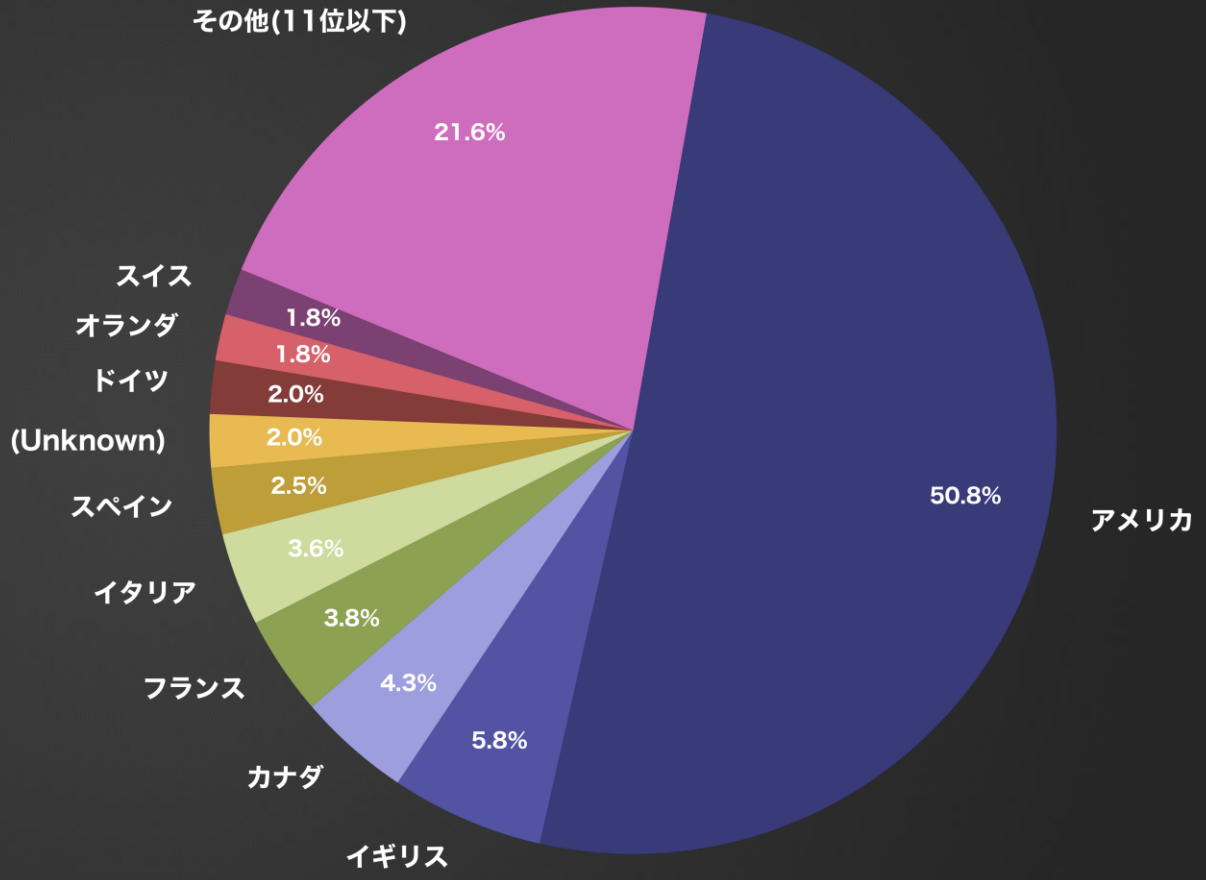
Know your enemy.
Defense leadership.

● 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	50.8	+ 45
イギリス	23	5.8	+ 7
カナダ	17	4.3	+ 1
フランス	15	3.8	± 0
イタリア	14	3.6	+ 7
スペイン	10	2.5	+ 5
(Unknown)	8	2.0	+ 7
ドイツ	8	2.0	+ 2
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

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

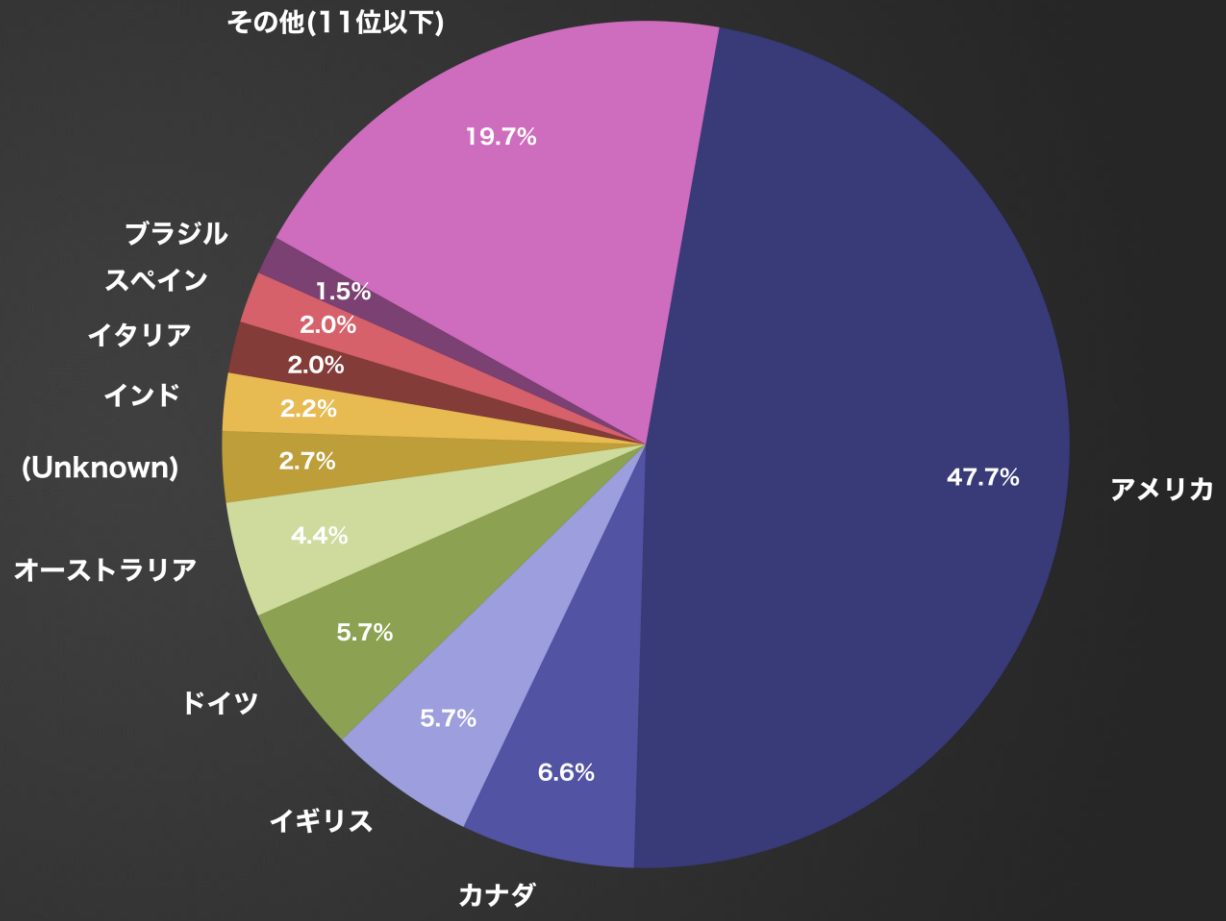
Know your enemy.
Defense leadership.®

● 月別内訳 被害国TOP10 （ 2024年 3 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	194	47.7	- 6
カナダ	27	6.6	+ 10
イギリス	23	5.7	± 0
ドイツ	23	5.7	+ 15
オーストラリア	18	4.4	+ 13
(Unknown)	11	2.7	+ 3
インド	9	2.2	+ 6
イタリア	8	2.0	- 6
スペイン	8	2.0	- 2
ブラジル	6	1.5	+ 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

3

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

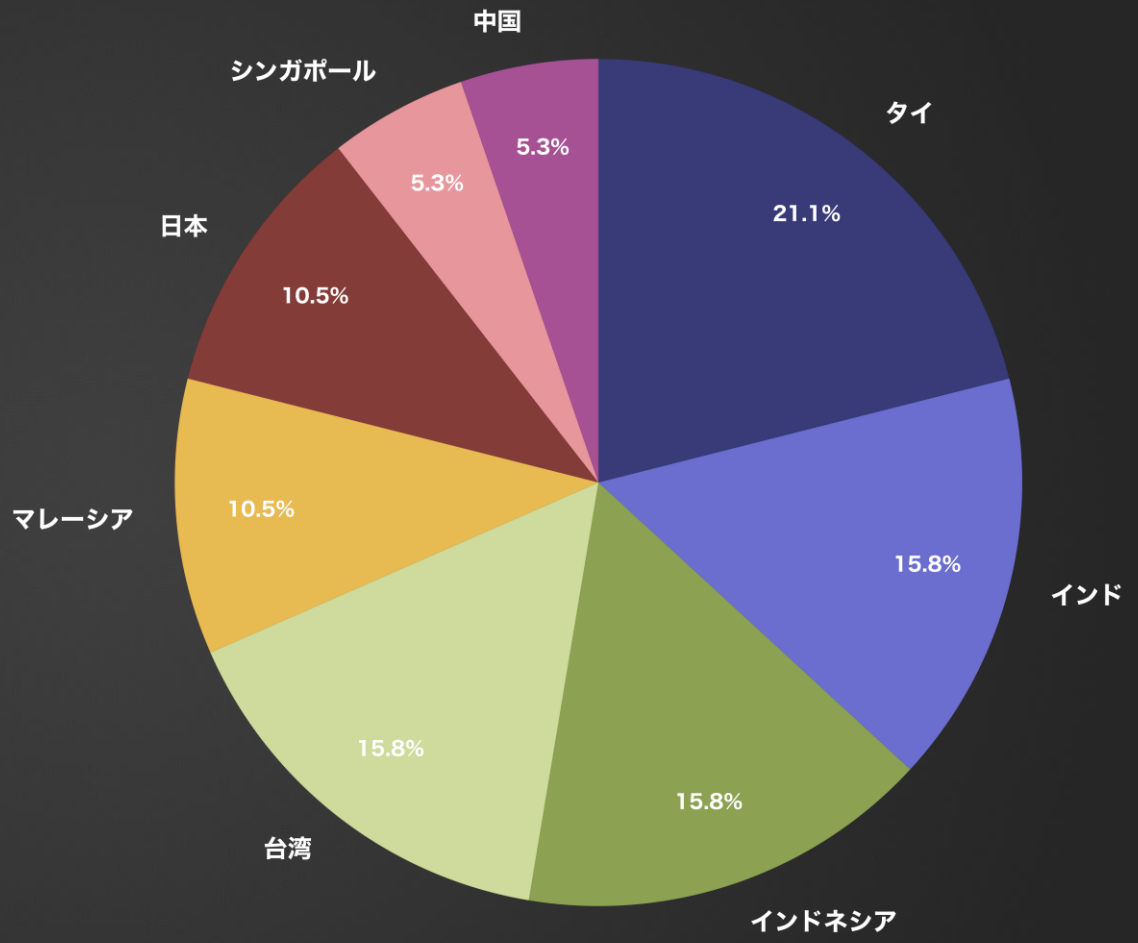
Know your enemy.
Defense leadership.

● 月別内訳 被害国TOP10 （ 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

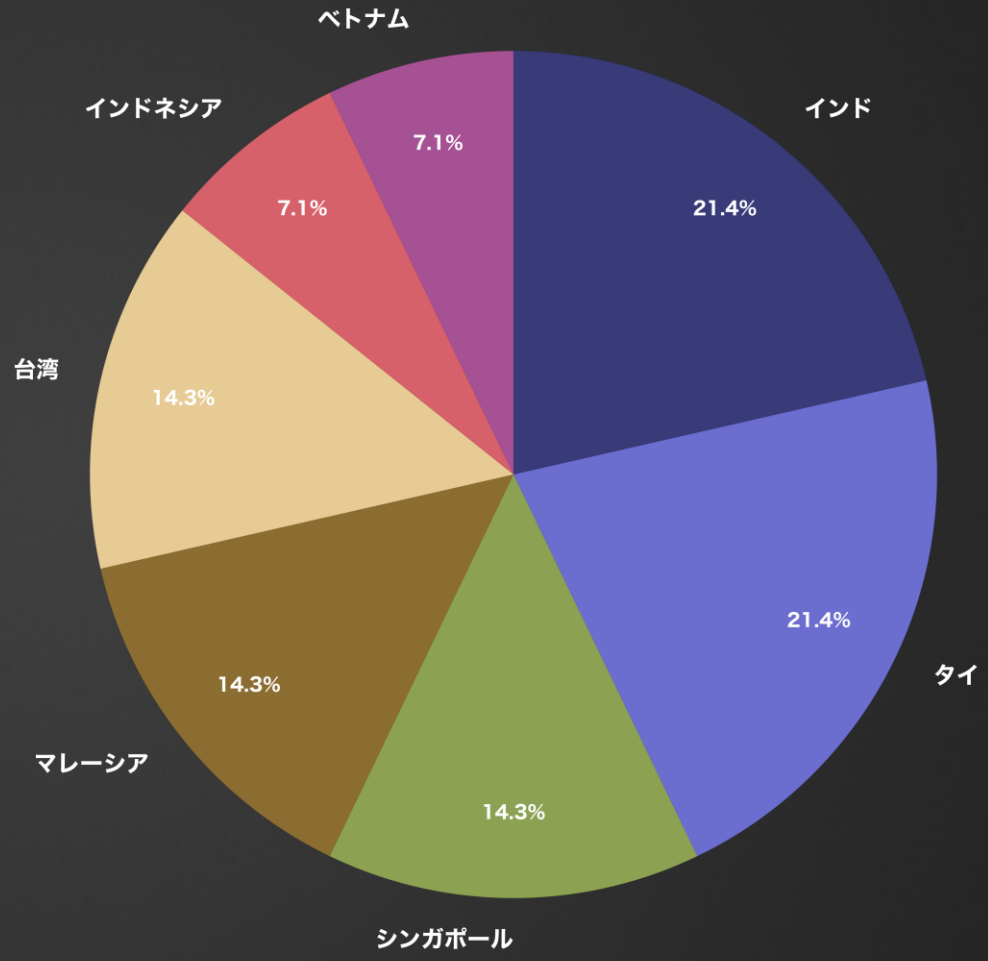
Know your enemy.
Defense leadership.®

● 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

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

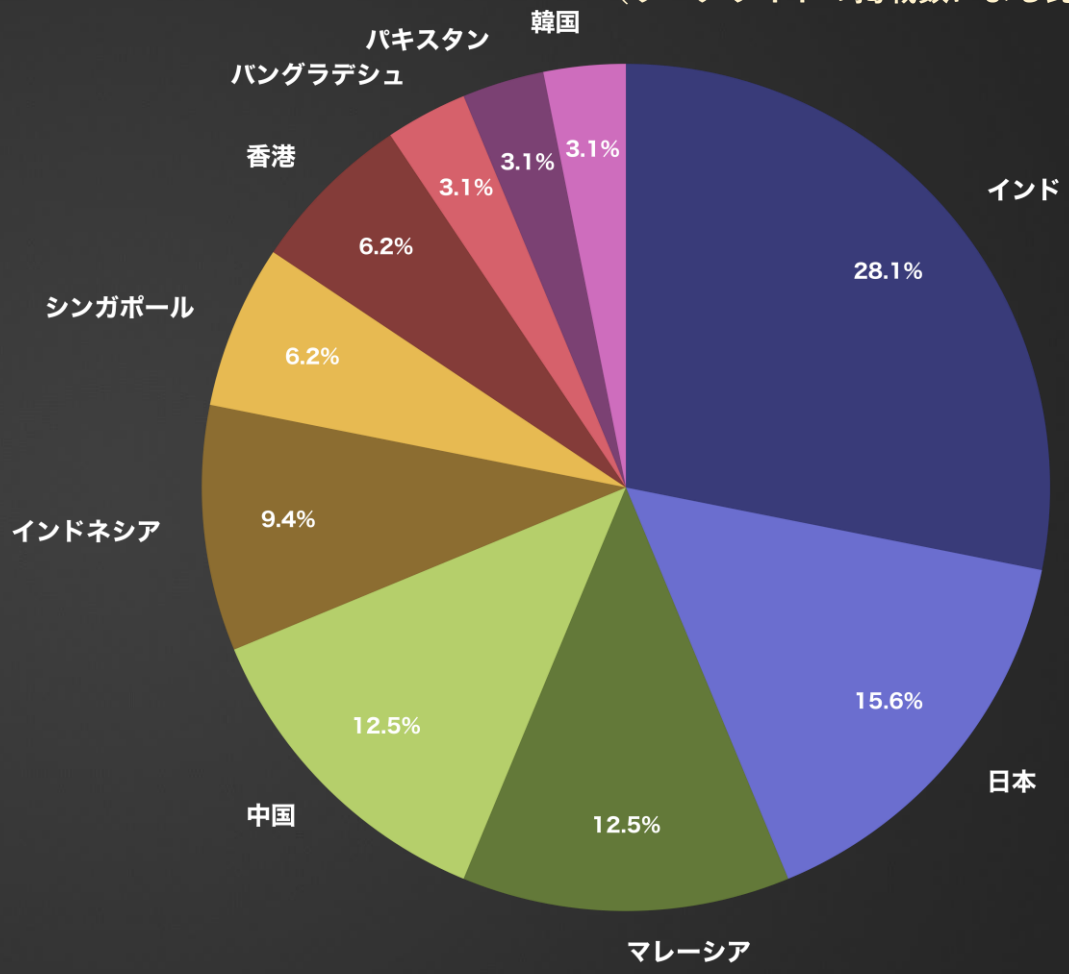
Know your enemy.
Defense leadership.

● 月別内訳 被害国TOP10 （ 2024年 3 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	9	28.1	+ 6
日本	5	15.6	+ 5
マレーシア	4	12.5	+ 2
中国	4	12.5	+ 4
インドネシア	3	9.4	+ 2
シンガポール	2	6.2	± 0
香港	2	6.2	+ 2
バングラデシュ	1	3.1	+ 1
パキスタン	1	3.1	+ 1
韓国	1	3.1	+ 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

3

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。

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

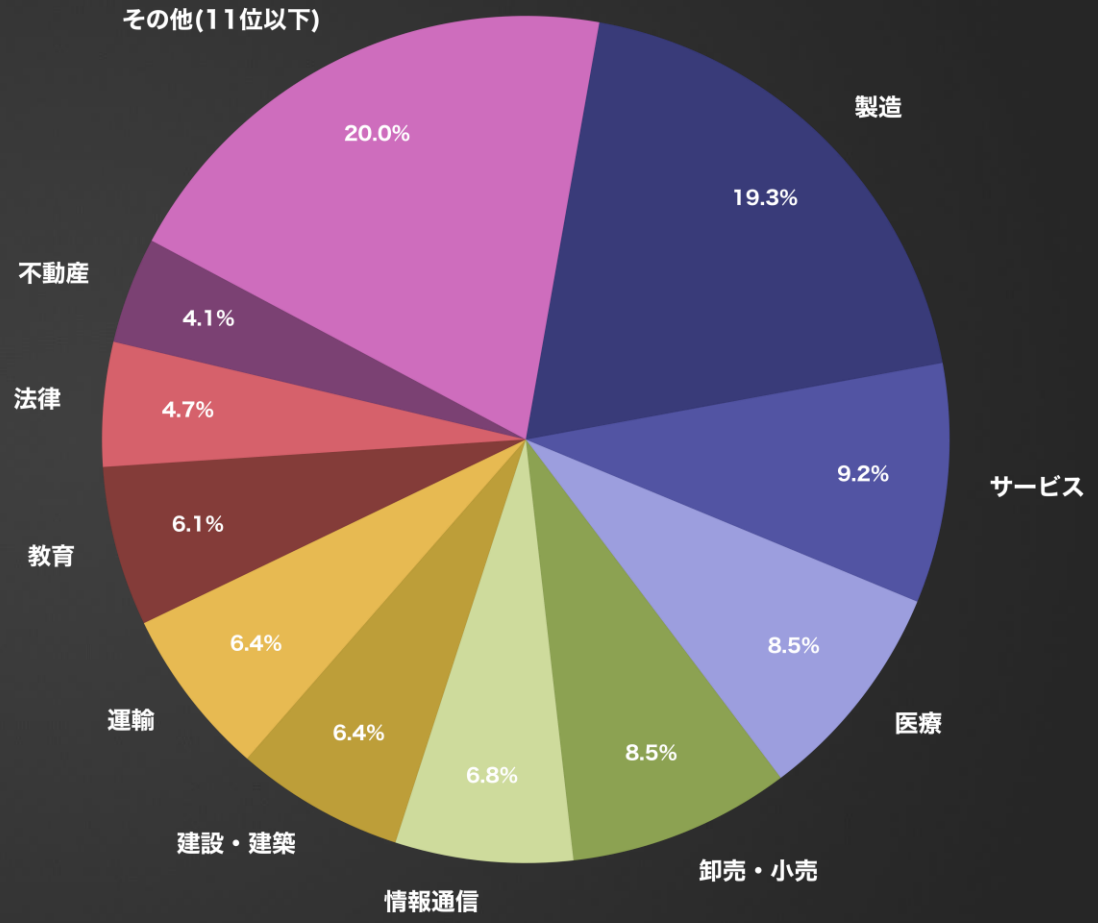
Know your enemy.
Defense leadership.

● 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	19.3	- 12
サービス	27	9.2	- 17
医療	25	8.5	- 6
卸売・小売	25	8.5	+ 5
情報通信	20	6.8	- 14
建設・建築	19	6.4	- 3
運輸	19	6.4	+ 9
教育	18	6.1	- 2
法律	14	4.7	- 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

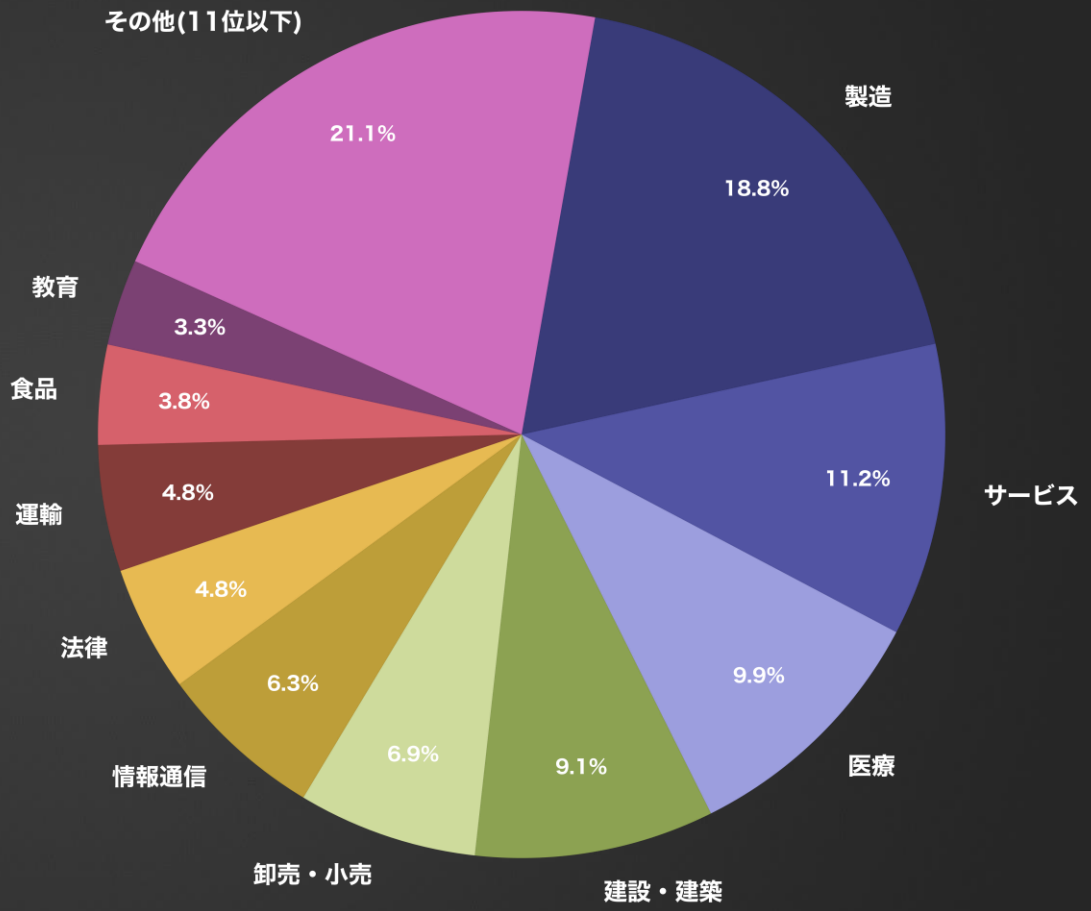
Know your enemy.
Defense leadership.

● 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	18.8	+ 17
サービス	44	11.2	+ 17
医療	39	9.9	+ 14
建設・建築	36	9.1	+ 17
卸売・小売	27	6.9	+ 2
情報通信	25	6.3	+ 5
法律	19	4.8	+ 5
運輸	19	4.8	± 0
食品	15	3.8	+ 3
教育	13	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）



※ 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

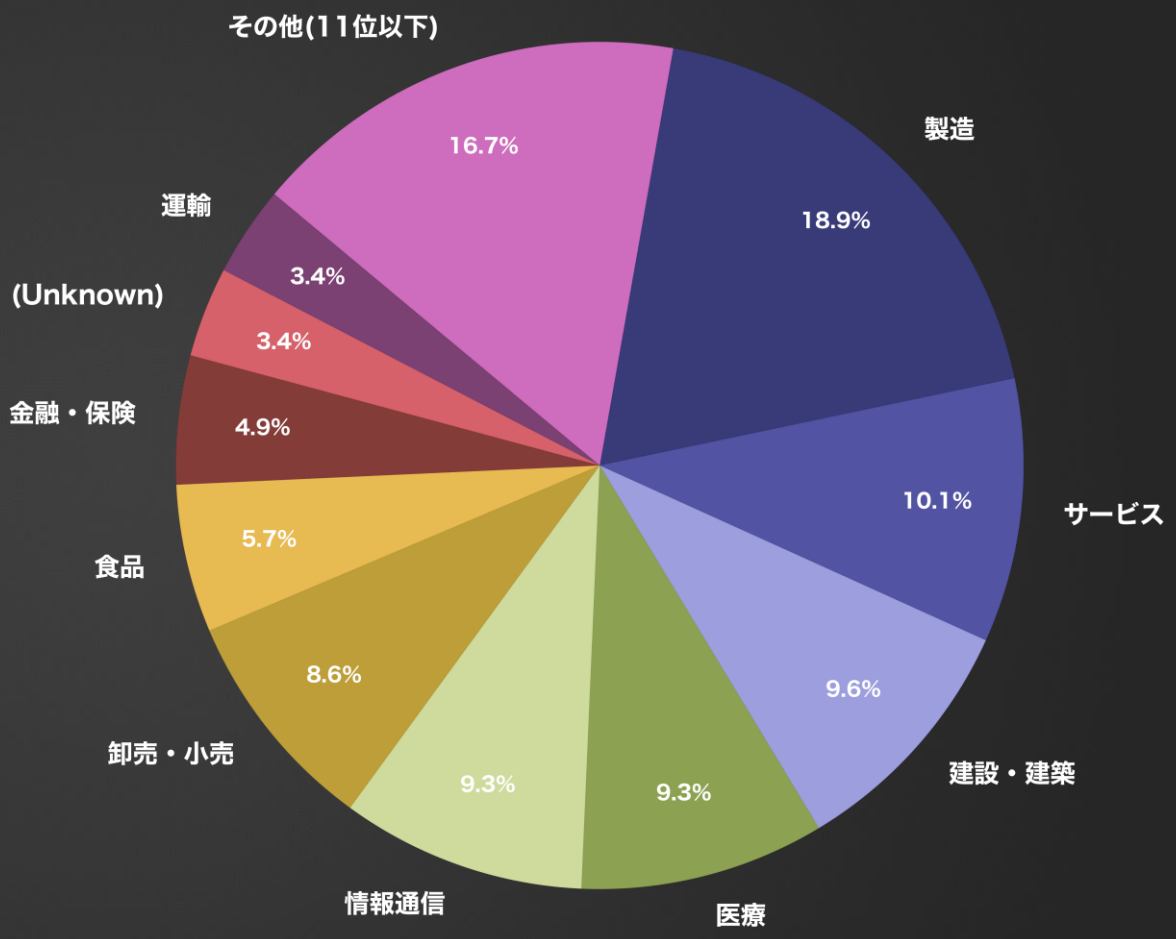
Know your enemy.
Defense leadership.®

● 月別内訳 業種 TOP10 （2024年 3 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	77	18.9	+ 2
サービス	41	10.1	- 3
建設・建築	39	9.6	+ 3
医療	38	9.3	- 1
情報通信	38	9.3	+ 13
卸売・小売	35	8.6	+ 8
食品	23	5.7	+ 8
金融・保険	20	4.9	+ 8
(Unknown)	14	3.4	+ 4
運輸	14	3.4	- 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）



※ 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

3

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.

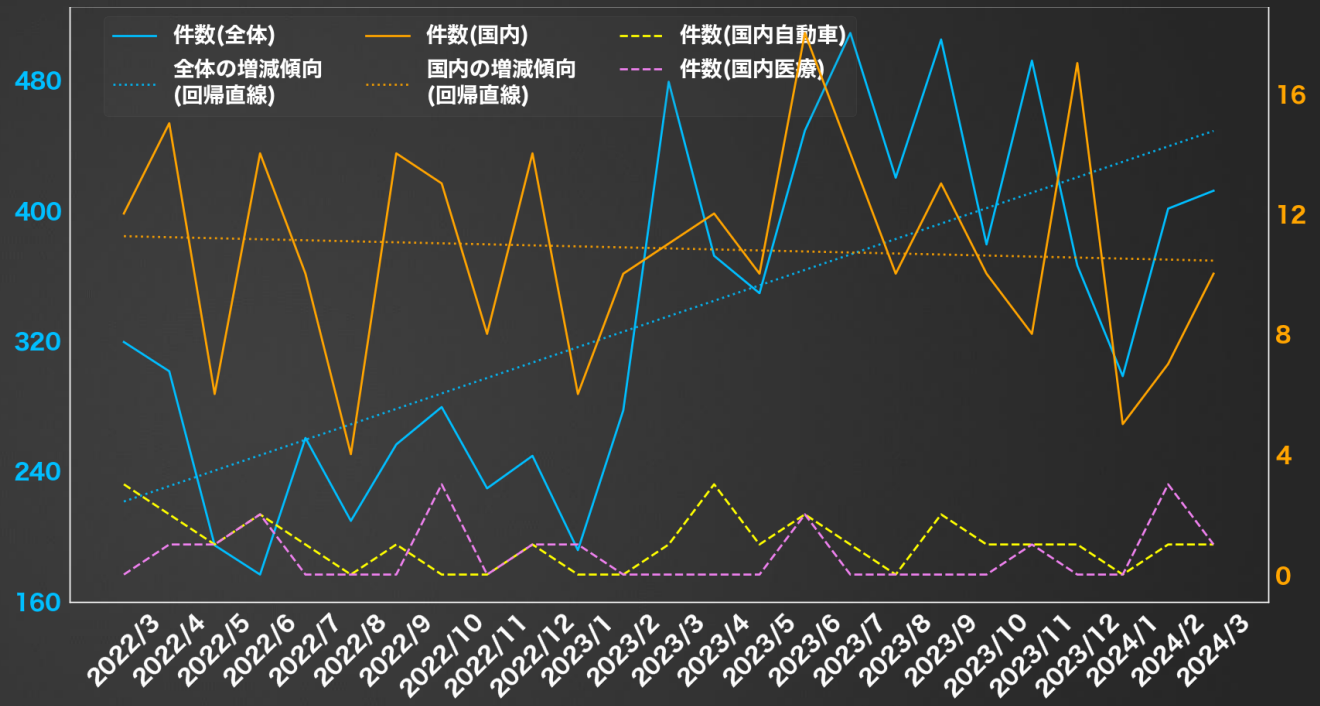
● 被害数の推移（2022年3月～2024年3月／全世界及び国内）(MBSD調べ)

※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)
2022/3	319	12	3	0
2022/4	301	15	2	1
2022/5	194	6	1	1
2022/6	176	14	2	2
2022/7	260	10	1	0
2022/8	209	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	449	18	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	298	5	0	0
2024/2	401	7	1	3
2024/3	412	10	1	1
合計	8371	271	26	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

Know your enemy.
Defense leadership.®

資本金別 月別統計
（国内）

2024

3

※ 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

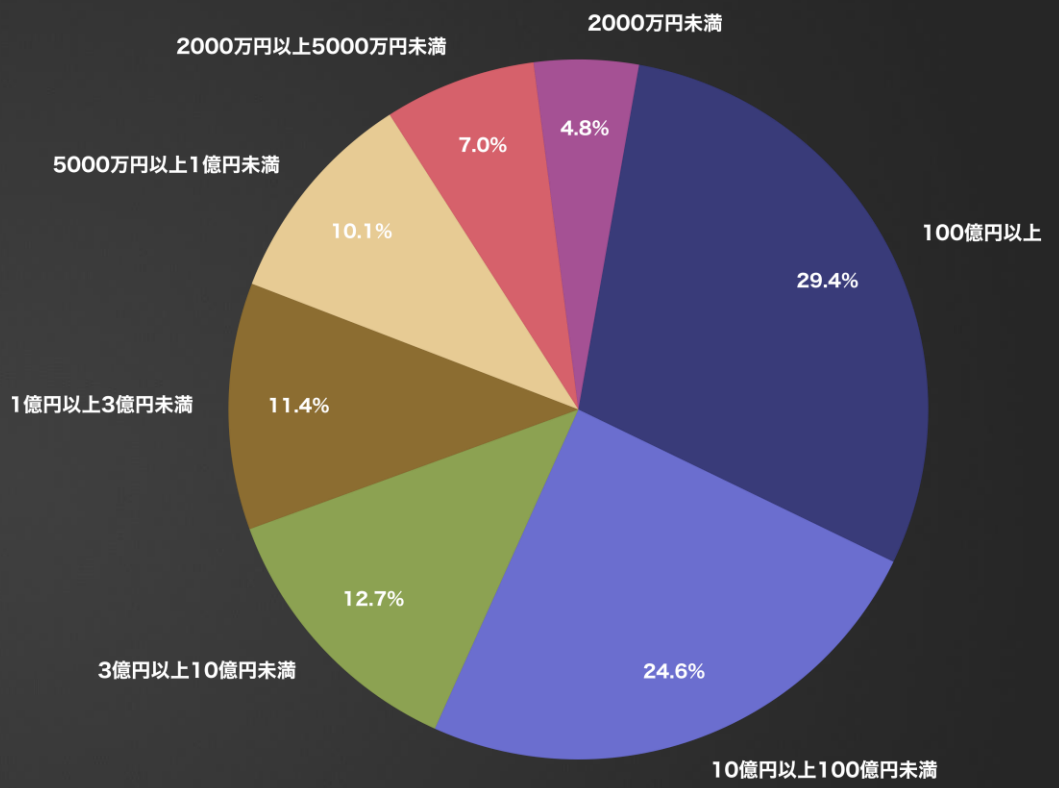
Know your enemy.
Defense leadership.

● 月別内訳 資本金別 （ 2022年3月～2024年3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	67	29.4
10億円以上100億円未満	56	24.6
3億円以上10億円未満	29	12.7
1億円以上3億円未満	26	11.4
5000万円以上1億円未満	23	10.1
2000万円以上5000万円未満	16	7.0
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：33.3%
・10億円未満が該当するとした場合：46.0%

（※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

3

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。

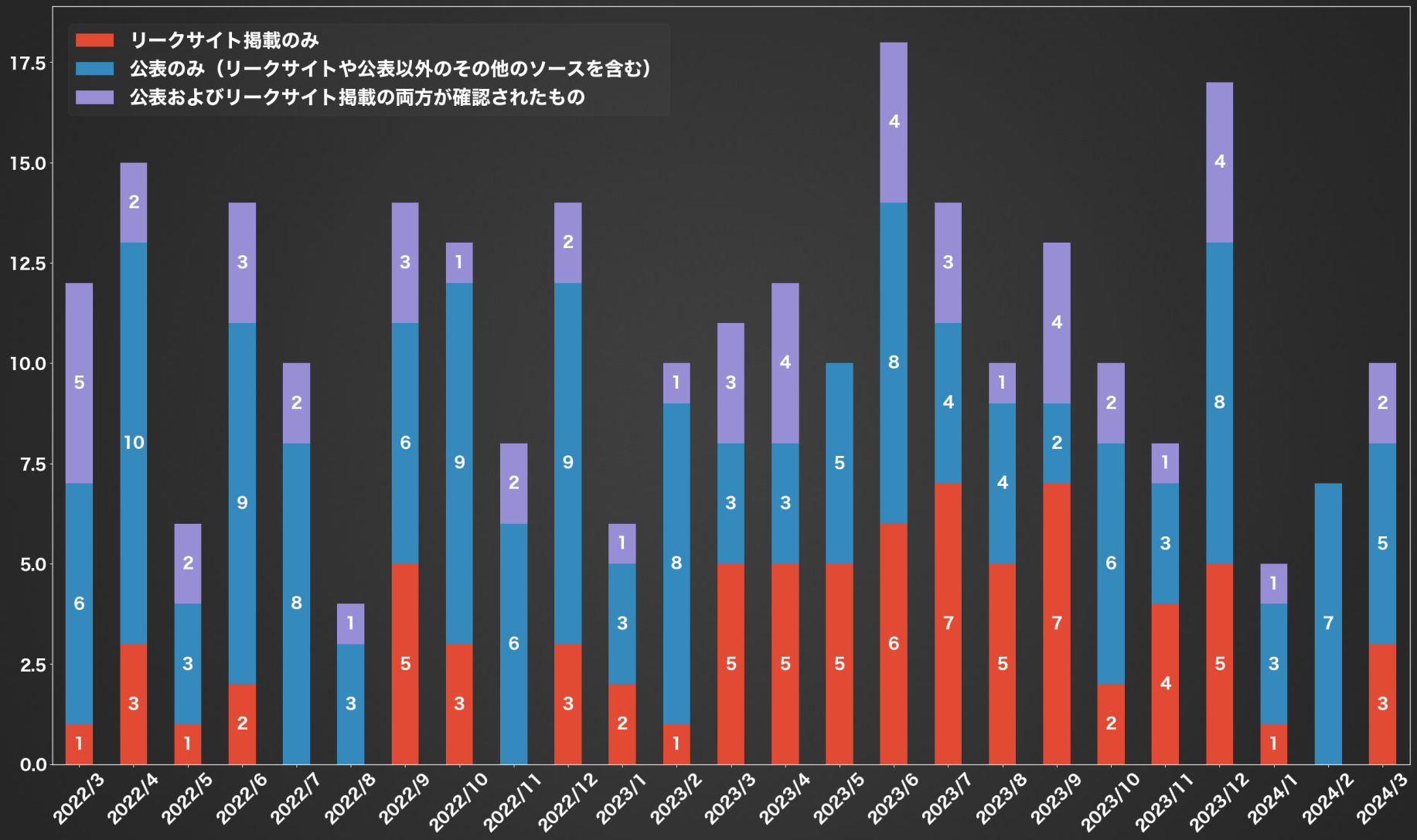
Created by Cyber Intelligence Group

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3月～2024年3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／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）

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

3

※ 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

MBSD 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3月～2024年3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
2023/3	(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	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
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

※ 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

MBSD 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3月～2024年3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	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)
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

被害月	攻撃グループ	業種概要
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)	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
2024/2	LockBit	自動車部品メーカー
2024/3	(Unknown)	放送事業会社
2024/3	(Unknown)	情報システムサービス会社
2024/3	(Unknown)	システム開発会社
2024/3	(Unknown)	建設関連事業会社
2024/3	LockBit	合成繊維製造会社
2024/3	LockBit	合成繊維製造会社
2024/3	AlphV / BlackCat	大手建設会社
2024/3	Medusa	大手電機メーカー(海外拠点)
2024/3	Hunters International	医療機器メーカー
2024/3	8BASE	自動車部品メーカー(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.®

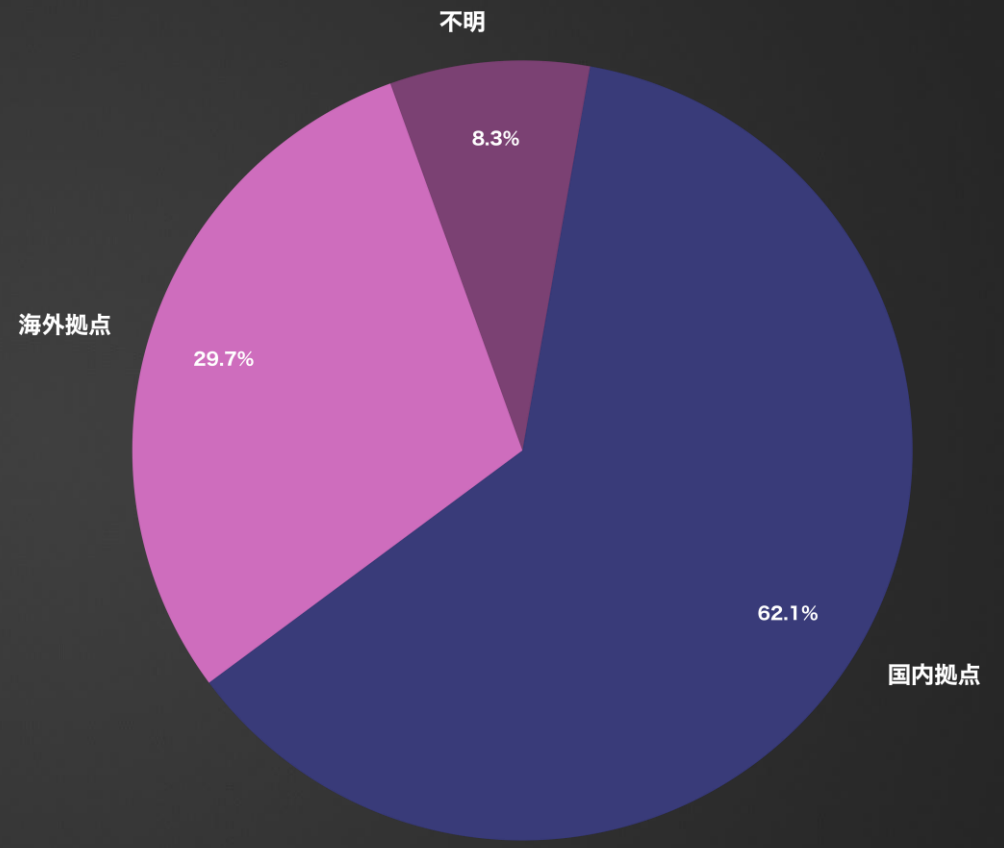
● 公となった国内被害組織における拠点割合（ 過去1年間／2023年3月～2024年3月）(MBSD調べ)

（※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	62.1
海外拠点	43	29.7
不明	12	8.3

▼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

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

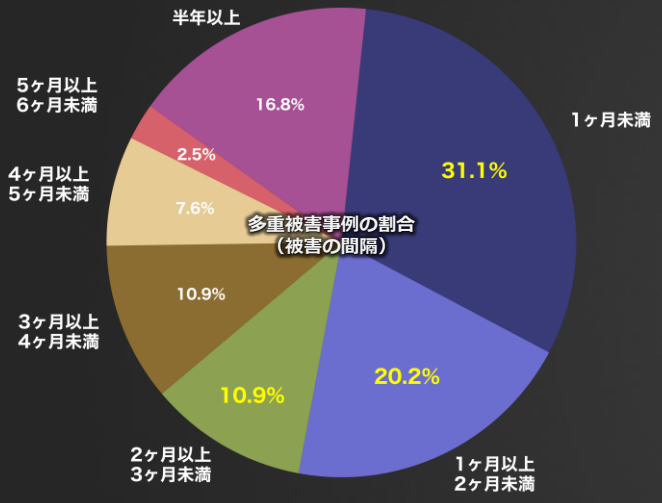
※多重被害：一度ランサムウェア攻撃の被害を受けた組織が異なる時期に異なる攻撃グループのリークサイトに再び掲載されるケース

多重被害に遭った被害組織の傾向と分析 （MBSD調べ）

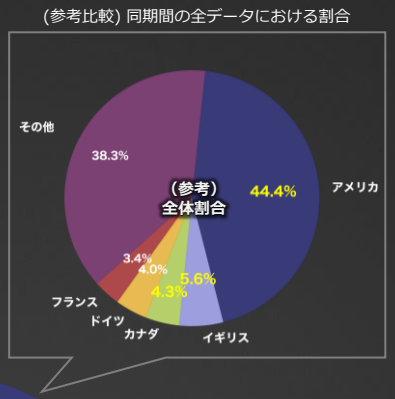
（過去2年間／2022年4月～2024年3月）

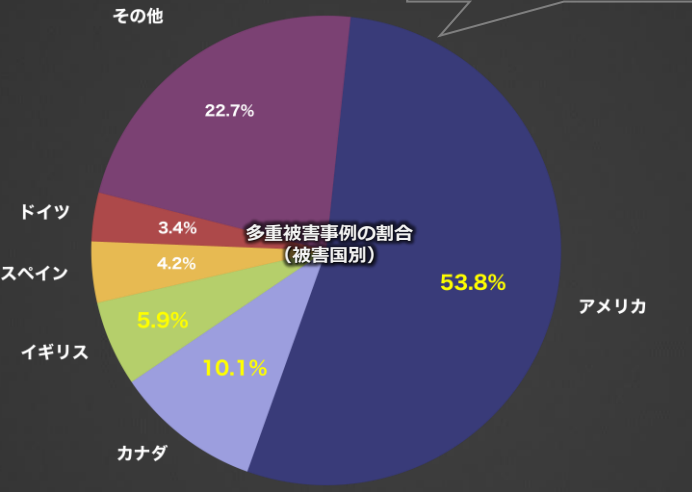
▼被害の間隔

（一度目の被害から二度目の被害までの間隔）

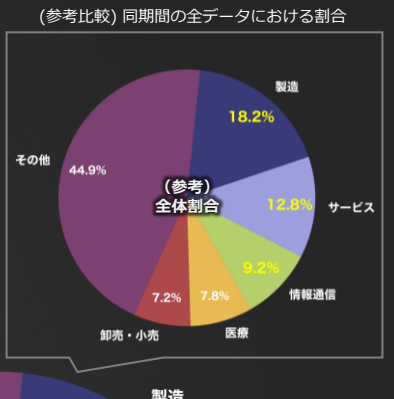


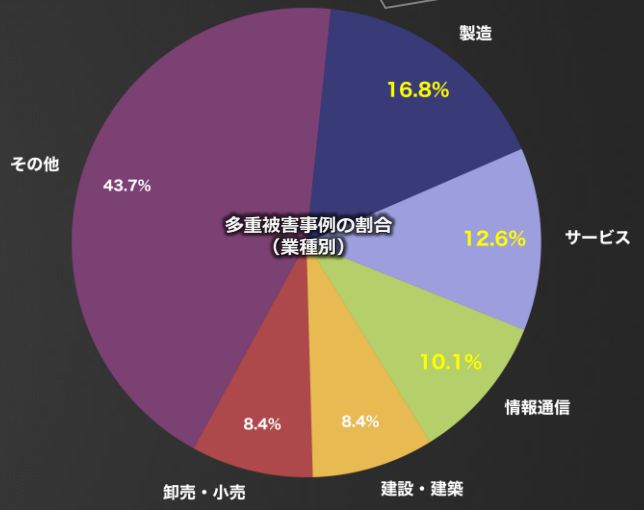
▼被害国別





▼業種別





▶多重被害に遭った組織数の累計：119件（全体8053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