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6月号 Rev 1.00
(2024年5月分)

2024
5

Created by Cyber Intelligence Group

今月のハイライト

「Operation Cronos」後も活動を継続するLockBitの現況

2024年2月、国際的な作戦である「Operation Cronos」によってLockBitが管理するサーバーの一部が押収された。
さらに押収されたリークサイト上で復号ツールが開発された旨やLockBit管理者（LockBitSuppまたはputinkrab）に関する情報公開を示唆する内容が掲載され、当初はLockBitを壊滅に追いやったとも思われた。しかしLockBitはすぐさま別の新たなリークサイトを立ち上げ、法執行機関に対する報復を示唆するような内容と共に活動継続を宣言した。
ただし、LockBitの活動に全く影響が無かったとは言い切れず、その後の動向は不安定さを露呈している。

3月は新たなリークサイトに96件の被害組織情報を掲載するも、その半数以上が過去に掲載した被害組織の再掲載であり、掲載数の水増しが疑われた。ところが4月の新規掲載数は24件となり、長い間トップクラスの掲載数を維持してきたLockBitは大幅に掲載数を減らすとともに、PLAYやHunters Internationalなどの比較的新しい攻撃グループにトップの座を譲っている。
5月に入り、法執行機関はLockBit管理者とされる人物の個人情報を公開し、資産凍結や渡航禁止などの制裁を加えるとともに起訴を公表。これに対し、LockBitSuppは情報の誤りを主張しているが、この発表の約二日後にはLockBitリークサイトに過去掲載情報を含む100件近くの被害組織情報が掲載された。これはLockBitSuppの個人情報公開に対する報復とも解釈でき、公開情報の信ぴょう性を高める結果となった。その後も継続的に掲載を続けたことで、結果的に5月における実質的なリークサイト新規掲載数は173件となり、過去二年間で最高を記録した。この勢いを維持するのか注視しているものの、一転して、6月の新規掲載数は6月25日時点で12件（テスト投稿や過去掲載除く）に留まる低水準となったことを確認している。活動が不安定になる前の2023年9月から2024年2月までの半年間の掲載数を集計してみると、各月1日～20日頃の平均掲載数は約60件であることから、月末時点での掲載数としては非常に少ないと言える。

「Operation Cronos」後にLockBitが信頼を失い、アフィリエイトなどの協力者が離散しているとの情報もあり、こうした背景と合わせて直近の活動状況を鑑みると、LockBitが不安定な状況下で活動を続けていることが窺い知れる。
しかし、仮にLockBitが解散したとしてもリブランドを行い活動を継続するケースや、協力者が他の攻撃グループに移籍して活動を継続するケースが考えられる。
また2月のサーバー押収時に、身代金を支払った被害組織の情報が削除されずに保管されていたことなどがわかっており、一度盗まれたデータが他の攻撃者の手に渡り再度恐喝に使用される可能性は決して低くない。これらから、首謀者の逮捕や攻撃グループの解散が一部に留まる限り、完全な解決とはならないことがわかる。
しかしながら少しでも被害組織を救済し、被害を抑えるべく現在もLockBitに対する捜査は継続されており、6月初旬にはFBIによって「現時点で7000以上の復号キーを保有し、被害組織のデータ復旧支援が可能」である旨が公表されている。サイバー犯罪者の徹底的な取り締まりや被害組織への支援体制の強化が、サイバー攻撃へのさらなる抑止力となることが期待される。

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。

監視中のランサムウェア攻撃グループ情報（拠点数と一覧）

● 当月監視対象の攻撃グループ数（※1）：177（※2）グループ

→当月リークサイト掲載の活動を確認した攻撃グループ数：43件

※1）レポート公開月に出現した攻撃グループは次月号に反映
※2）活動停止した攻撃グループを含む

● 当月監視対象の攻撃グループ一覧

（🔴：当月から新しく監視対象に加えた攻撃グループ）

0mega (Omega)
8BASE
ABYSS
AKIRA
AKO
Alpha (MYDATA)
AlphV (BlackCat)
Apos Security
APT73 (Eraleig)
🔴 ARCUS MEDIA
ArvinClub
Astro (Astra)
AtomSilo
Avaddon
AvosLocker
Axxes
Babuk
BianLian
BL0ODY (BLOODY)
Bl4ckt0r (BlackTor)
BlackBasta
BlackByte
BlackDolphin
BlackMatter
Blackout
BLACKSUIT
BLUESKY
BULLY
CACTUS
CHEERS
ChileLocker (Arcrypter)
CiphBit
CipherLocker
CL0P (CLOP)
Cloak
Conti
Cooming Project
CROSSLOCK
CryptBB
CRYPTNET
CryptOn
Cuba
Cyclops
DAGON
DAIXIN
dAn0n (danon)
Dark Angels
DARK VAULT
DARKBIT
DARKPOWER
DarkRace
DarkRypt
Darkside
~~Dispossessor~~ [Databroker]
Donex
Donut
DoppelPaymer
dotAdmin
DragonForce
Dunghill
eCh0raix (eChoraix)
El_Cometa
EMBARGO
Endurance
Entropy
Everest
🔴 FSOCIETY / FLOCKER
FSTeam
Grief
Groove
🔴 ~~HANDARA~~ [Hacktivist]
Haron
HelloGookie
Hitler (AGL0BGVYCG)
Hive
HolyGhost
Hotarus
HUNTERS INTERNATIONAL
ICEFIRE
INC Ransom
Insane
Karakurt
Karma
KILLSEC
Knight
La Piovra
LAMBDA
LAPSUS$
LILITH
LockBit
Lorenz
LostTrust
LV
MADCAT
MALAS
MalekTeam
MALLOX
MBC
Medusa
MEOW
Metaencryptor
Midas
Mindware
~~Mogilevich~~ [fraud]
MOISHA
Money Message
Monti
Mount Locker
N3tw0rm (NetWorm)
N4UGHTYSEC (NAUGHTYSEC)
Nefilim
Nevada
NightSky
NoEscape
Nokoyawa
NONAME [2023年確認]
NONAME (VFOKX)
Onyx
Pandora
Pay2Key
Payload.bin
PLAY
Prometheus
PUTIN TEAM
Pysa / Mespinoza
Qilin (Agenda)
QIULONG
Quantum
RA GROUP
RA WORLD
RABBIT HOLE
Ragnar Locker
Ragnarok
Rancoz
Ransom Cartel
Ransom Corp
Ransom EXX
Ransomed.vc
RansomHouse
ransomhub
Ransomware Blog
Ranzy
Raznatovic
Red Ransomware Group (Red CryptoApp)
RedAlert (N13V)
Relic
Revil (Sodinokibi)
Rhysida
ROOK
Royal
Rransom
Sabbath (54bb47h)
shaoleaks
SIEGEDSEC
SLUG
Snatch
Solidbit
Space Bears
Sparta
Spook
STORMOUS
Sugar
Suncrypt
SynACK
ThreeAM (3AM)
TRIGONA
TRISEC
🔴 Underground
UnSafe
V IS VENDETTA
Vice Society
VSOP
WEREWOLVES
x001xs
XING Team
Yanluowang
Zeon
🔴 Zero Tolerance

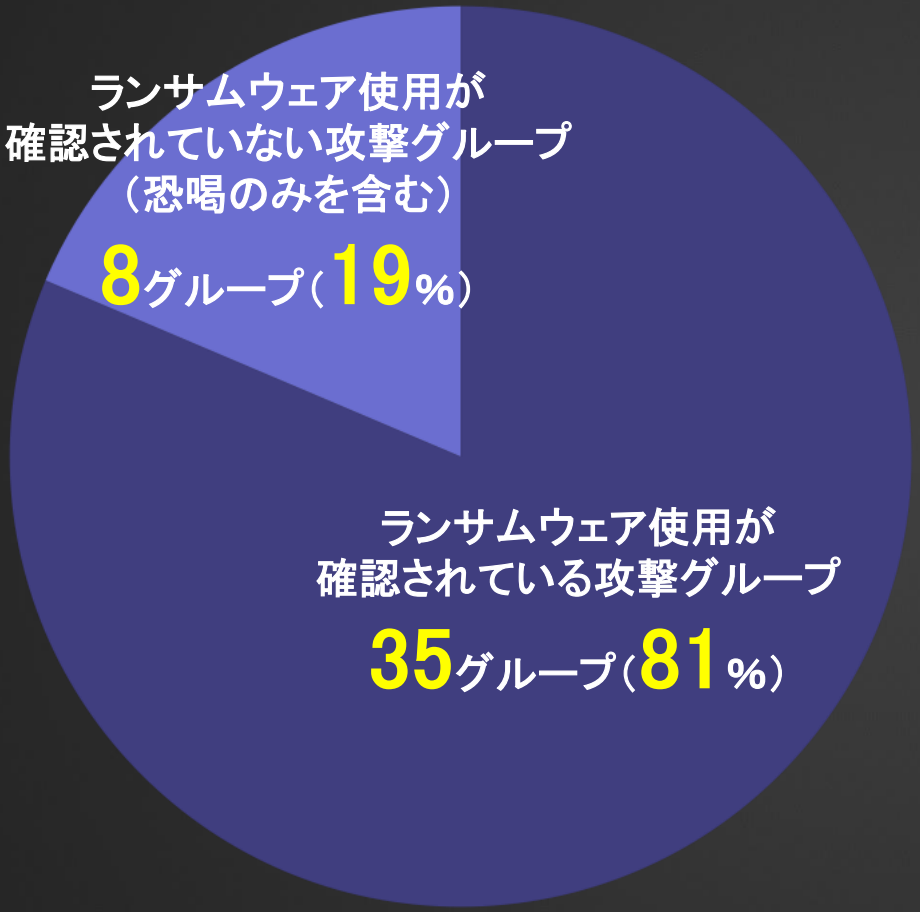
※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
（日本にフォーカスした一部の表／グラフのみ、公表や報道から判明した数を加味し集計）
※ 国内被害組織に関する各種データについては、海外拠点（支社／関連会社）を含む。
※ 業種分類や集計方法を含む本レポートの各データ（値）はMBSD独自の観測および集計結果となる。
※ これらはあくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
※ ごく一部のランサムウェアの使用が明確に確認されていない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

Know your enemy. Defense leadership.®

● 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5月）

（※2024年5月にリークサイト掲載を確認した攻撃グループ全43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5月に活動中である事が確認された全43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。

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

2024

5

年間 統計

（全世界）

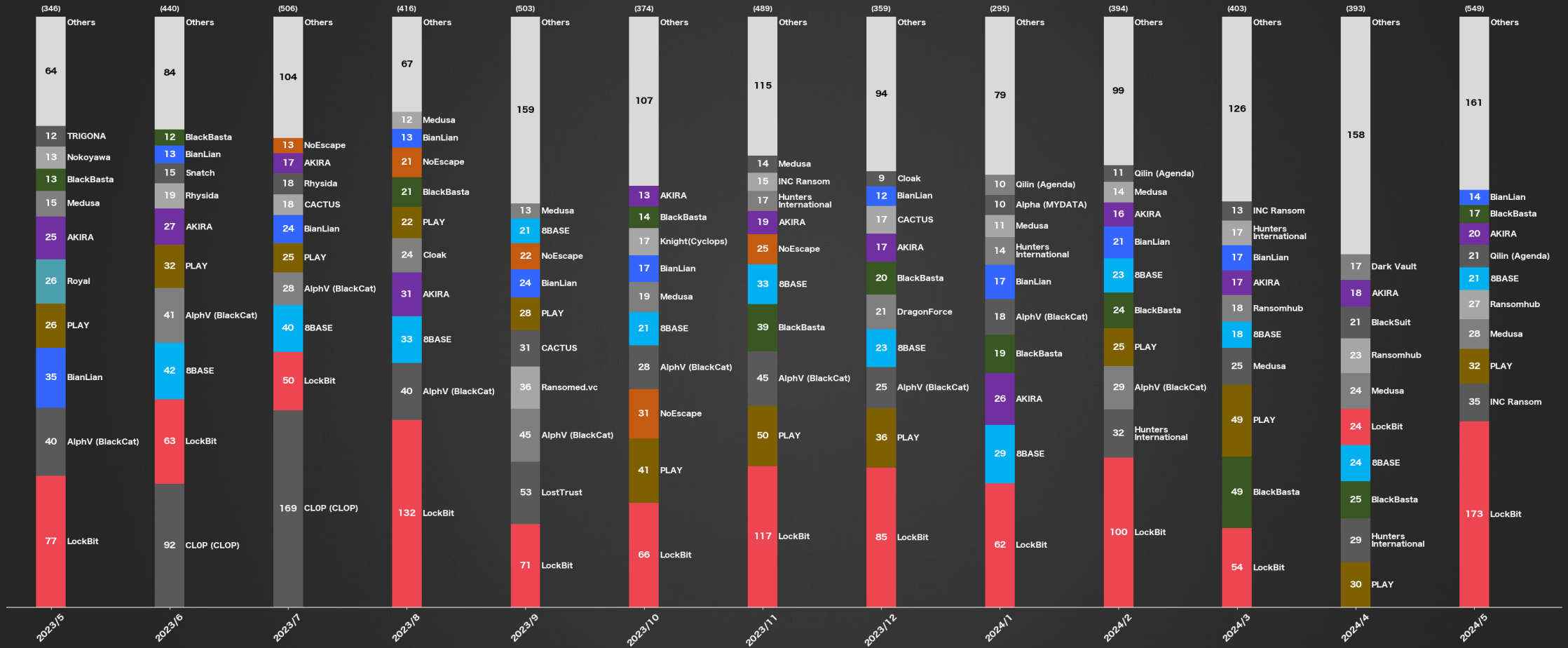
※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
（日本にフォーカスした一部の表／グラフのみ、公表や報道から判明した数を加味し集計）
※ 国内被害組織に関する各種データについては、海外拠点（支社／関連会社）を含む。
※ 業種分類や集計方法を含む本レポートの各データ（値）はMBSD独自の観測および集計結果となる。
※ これらはあくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
※ ごく一部のランサムウェアの使用が明確に確認されていない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

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5月～2024年5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

5

※ 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 － ②

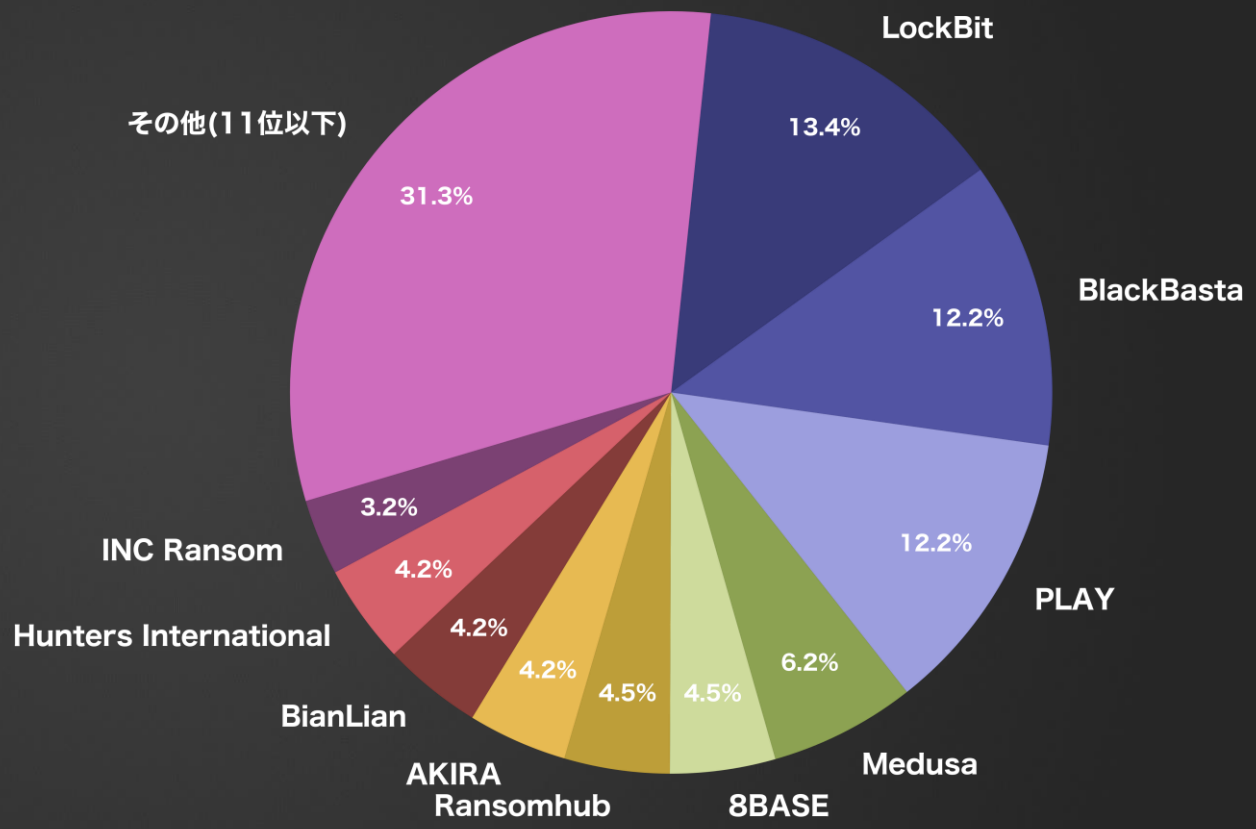
Know your enemy.
Defense leadership.

● 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	54	13.4	- 46
BlackBasta	49	12.2	+ 25
PLAY	49	12.2	+ 24
Medusa	25	6.2	+ 11
8BASE	18	4.5	- 5
Ransomhub	18	4.5	+ 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

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ③

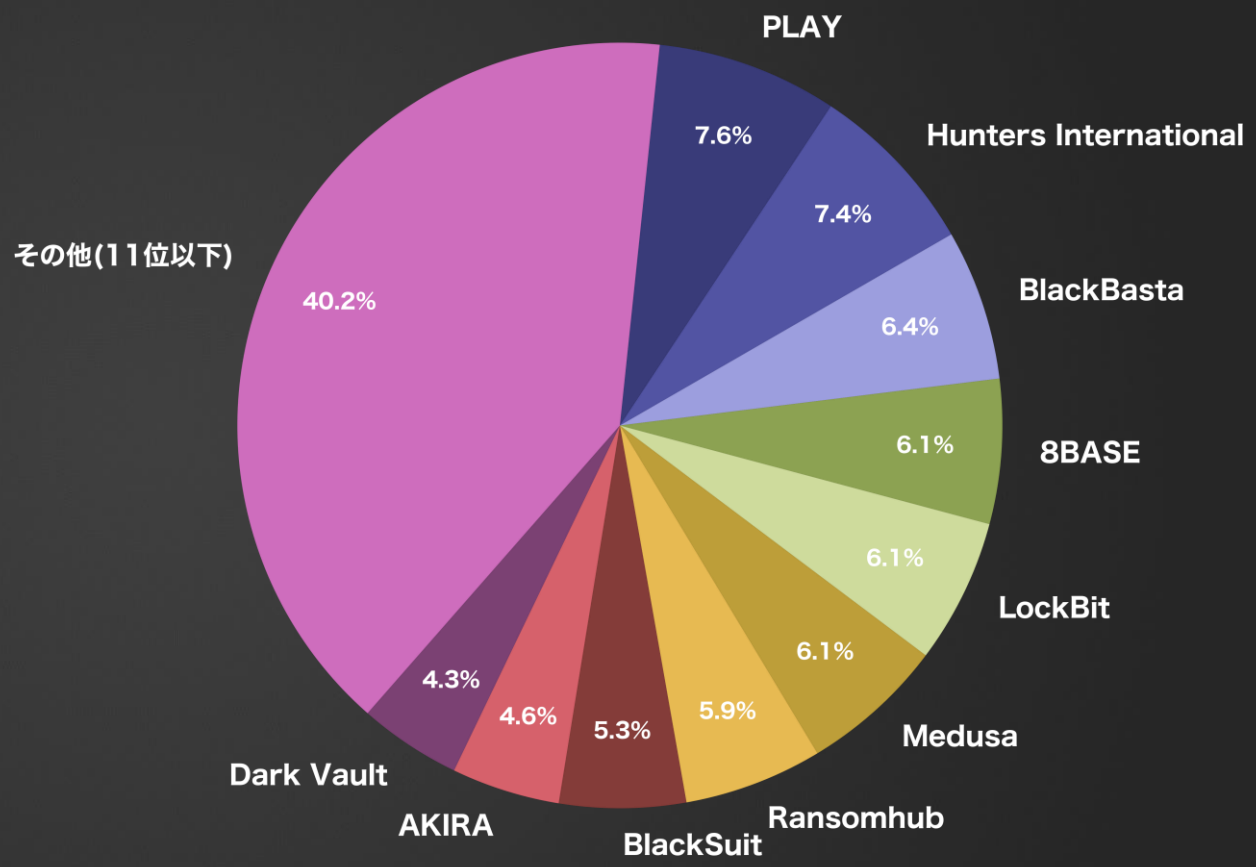
Know your enemy.
Defense leadership.®

● 月別内訳 攻撃グループ TOP10 （2024年 4 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)
PLAY	30	7.6	- 19
Hunters International	29	7.4	+ 12
BlackBasta	25	6.4	- 24
8BASE	24	6.1	+ 6
LockBit	24	6.1	- 30
Medusa	24	6.1	- 1
Ransomhub	23	5.9	+ 5
BlackSuit	21	5.3	+ 13
AKIRA	18	4.6	+ 1
Dark Vault	17	4.3	+ 17

▼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

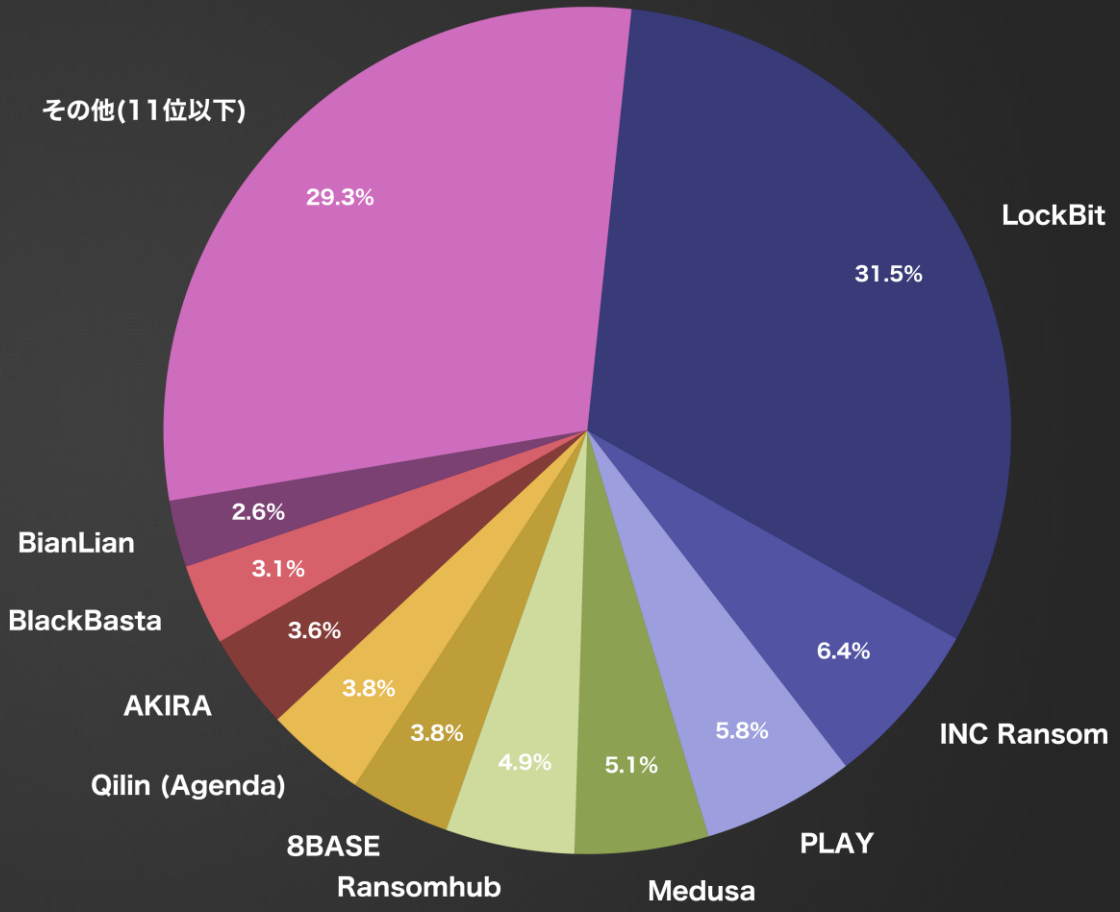
Know your enemy.
Defense leadership.®

● 月別内訳 攻撃グループ TOP10 （2024年 5 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	173	31.5	+ 149
INC Ransom	35	6.4	+ 19
PLAY	32	5.8	+ 2
Medusa	28	5.1	+ 4
Ransomhub	27	4.9	+ 4
8BASE	21	3.8	- 3
Qilin (Agenda)	21	3.8	+ 9
AKIRA	20	3.6	+ 2
BlackBasta	17	3.1	- 8
BianLian	14	2.6	+ 2

▼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

5

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 － ⑤

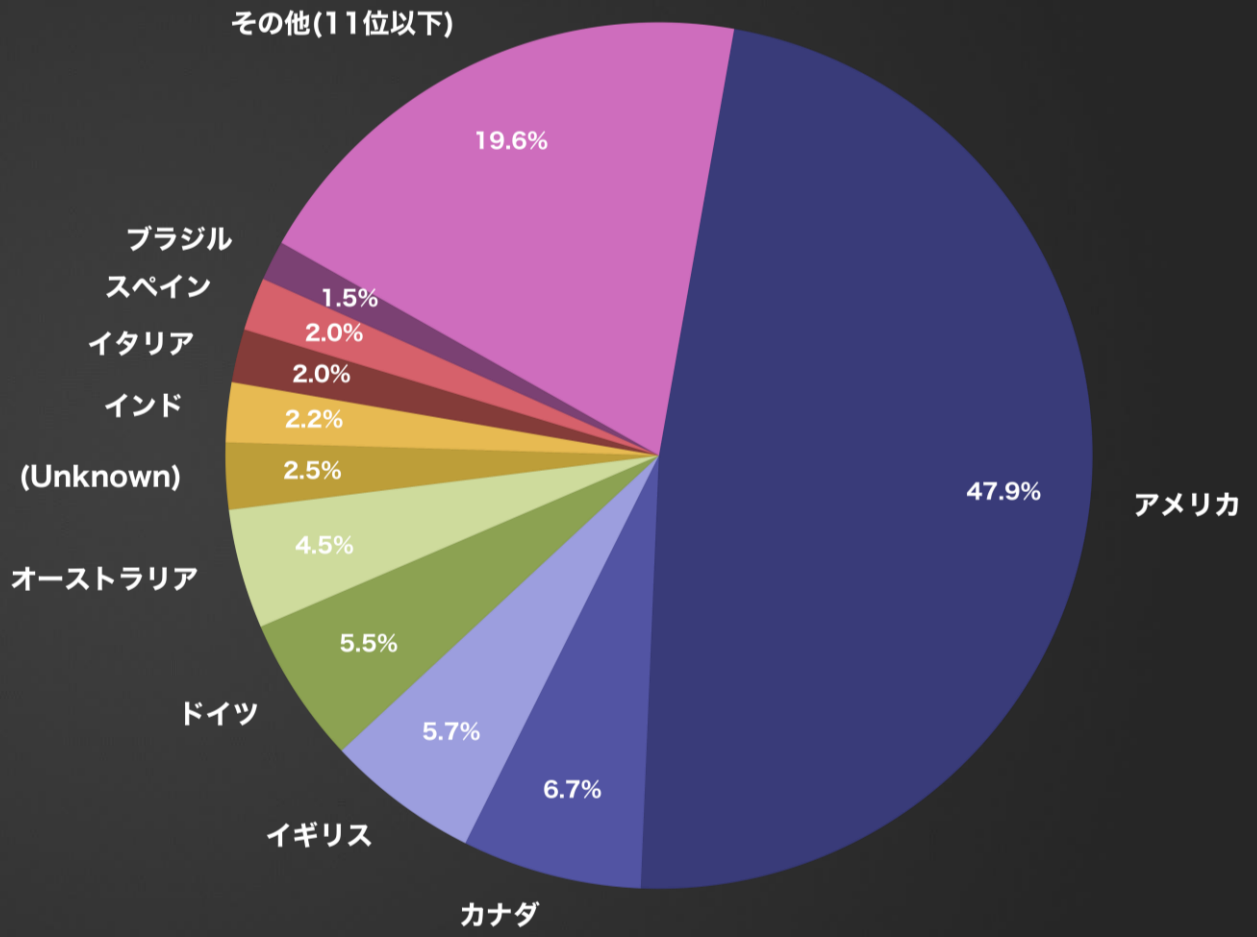
MBSD Know your enemy. Defense leadership.®

● 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	193	47.9	- 7
カナダ	27	6.7	+ 10
イギリス	23	5.7	± 0
ドイツ	22	5.5	+ 14
オーストラリア	18	4.5	+ 13
(Unknown)	10	2.5	+ 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

暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑥

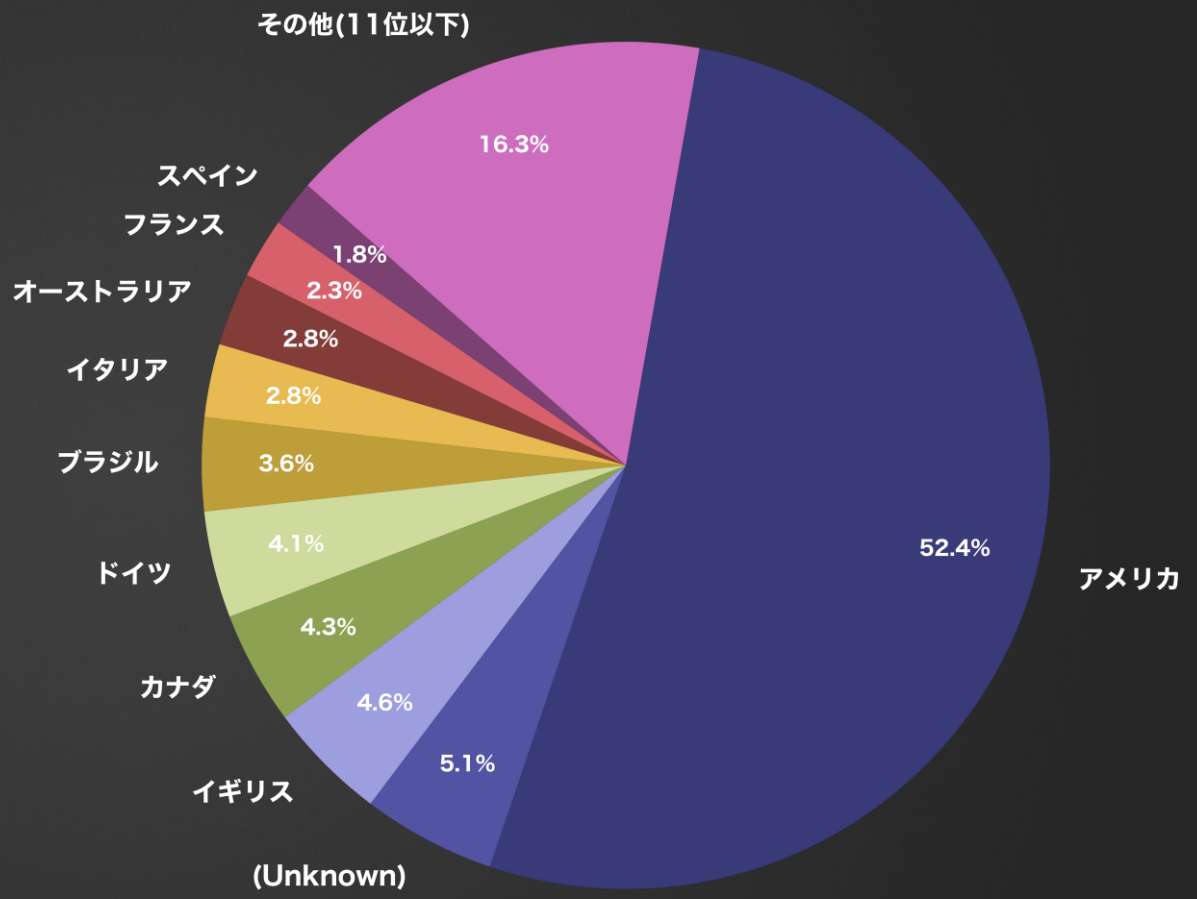
Know your enemy.
Defense leadership.

● 月別内訳 被害国TOP10 （ 2024年 4 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	206	52.4	+ 13
(Unknown)	20	5.1	+ 10
イギリス	18	4.6	- 5
カナダ	17	4.3	- 10
ドイツ	16	4.1	- 6
ブラジル	14	3.6	+ 8
イタリア	11	2.8	+ 3
オーストラリア	11	2.8	- 7
フランス	9	2.3	+ 8
スペイン	7	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

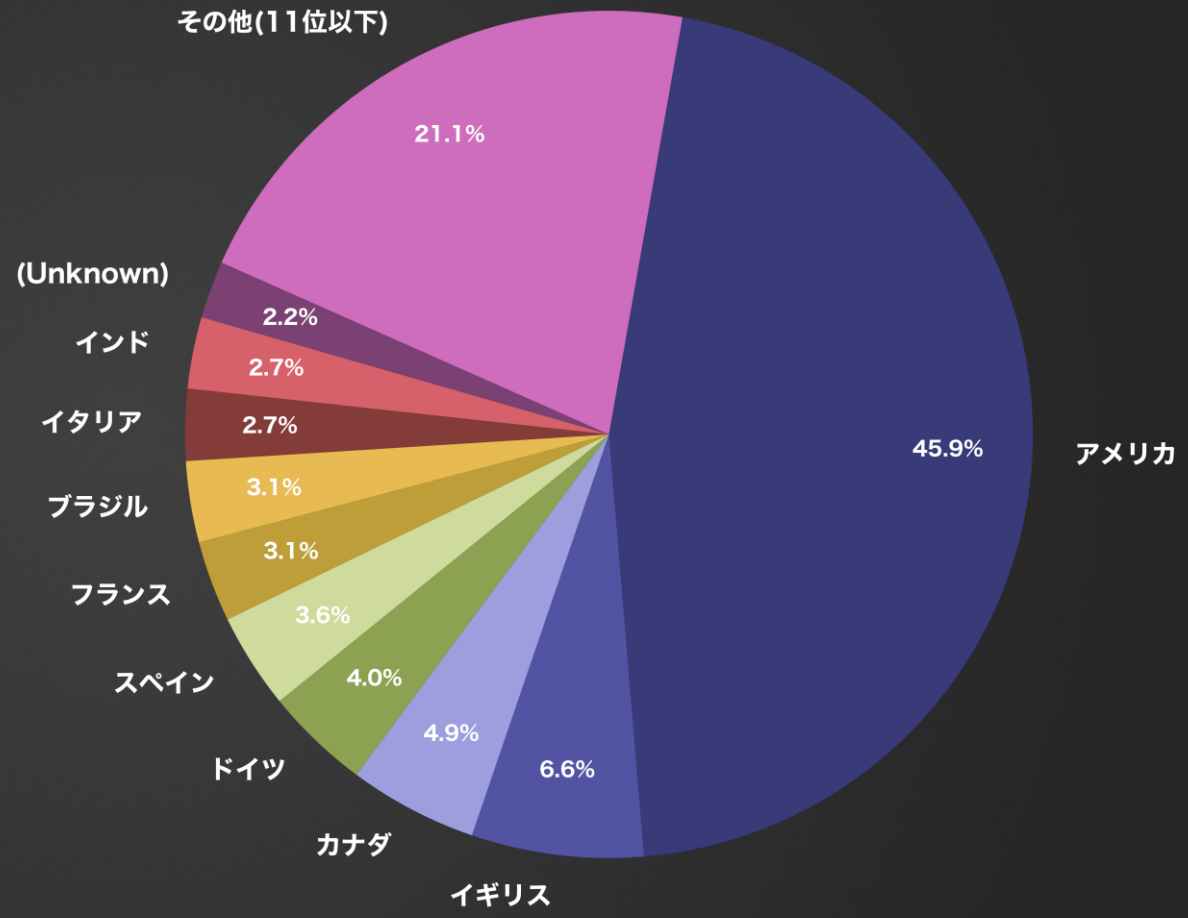
Know your enemy.
Defense leadership.®

● 月別内訳 被害国TOP10 （ 2024年 5 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	252	45.9	+ 46
イギリス	36	6.6	+ 18
カナダ	27	4.9	+ 10
ドイツ	22	4.0	+ 6
スペイン	20	3.6	+ 13
フランス	17	3.1	+ 8
ブラジル	17	3.1	+ 3
イタリア	15	2.7	+ 4
インド	15	2.7	+ 9
(Unknown)	12	2.2	- 8

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



※ 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

5

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 － ⑧

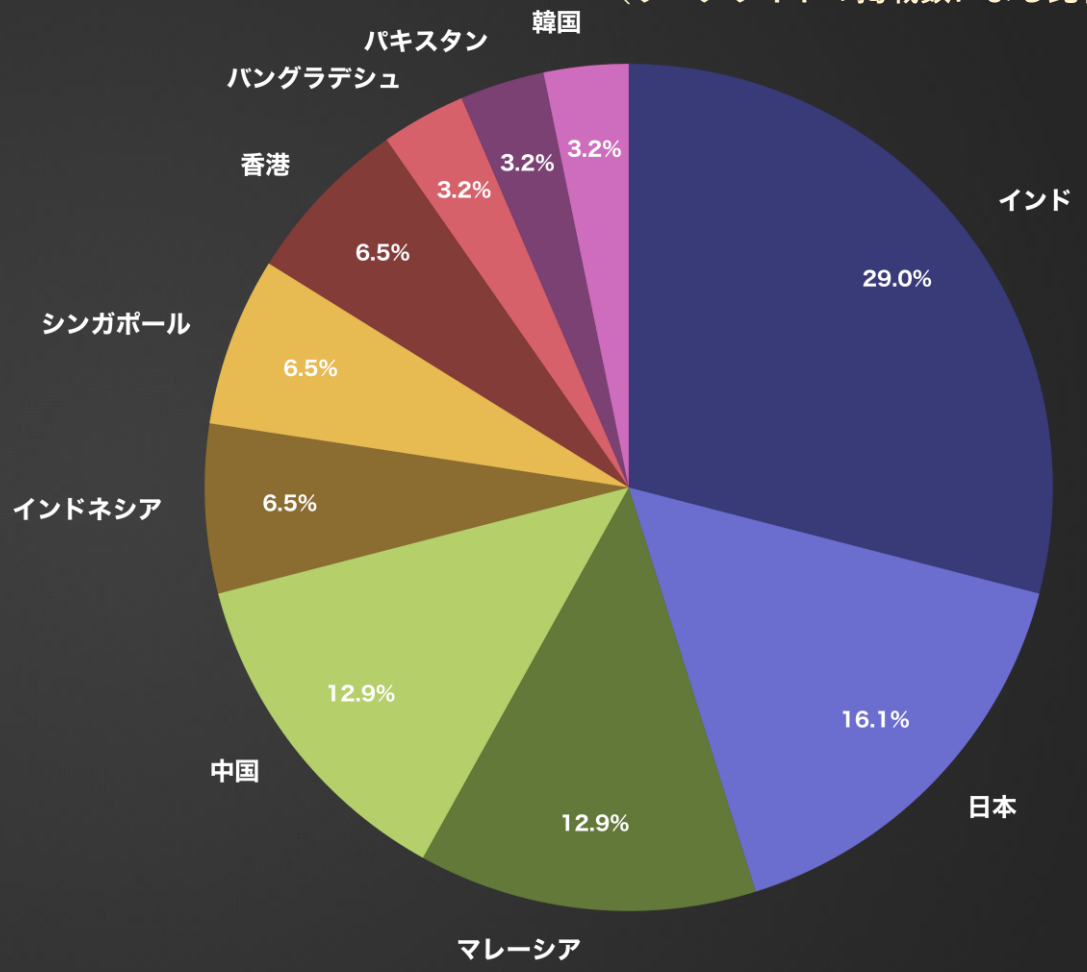
Know your enemy.
Defense leadership.®

● 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	29.0	+ 6
日本	5	16.1	+ 4
マレーシア	4	12.9	+ 2
中国	4	12.9	+ 4
インドネシア	2	6.5	+ 1
シンガポール	2	6.5	± 0
香港	2	6.5	+ 2
バングラデシュ	1	3.2	+ 1
パキスタン	1	3.2	+ 1
韓国	1	3.2	+ 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 － ⑨

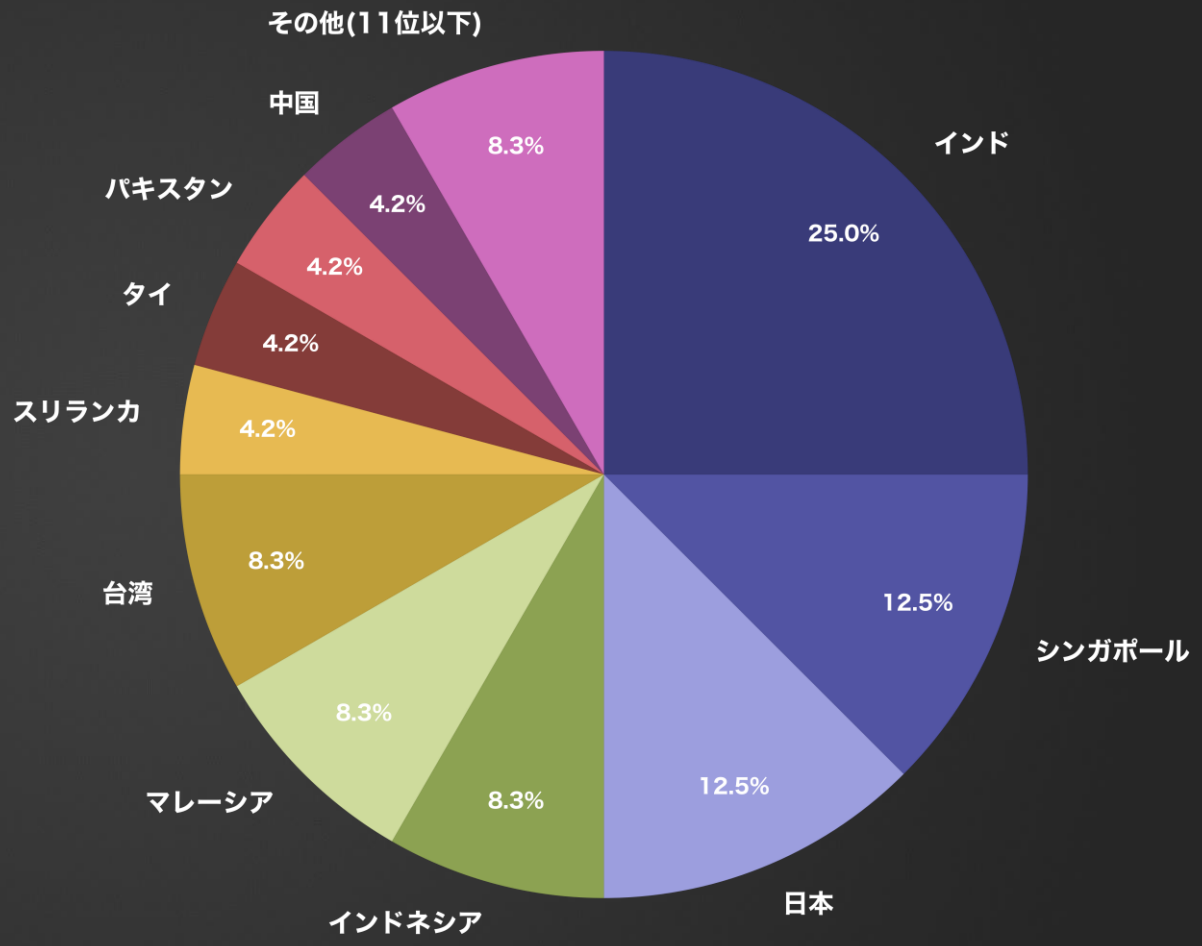
Know your enemy.
Defense leadership.

● 月別内訳 被害国TOP10 （ 2024年 4 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	6	25.0	- 3
シンガポール	3	12.5	+ 1
日本	3	12.5	- 2
インドネシア	2	8.3	± 0
マレーシア	2	8.3	- 2
台湾	2	8.3	+ 2
スリランカ	1	4.2	+ 1
タイ	1	4.2	+ 1
パキスタン	1	4.2	± 0
中国	1	4.2	- 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

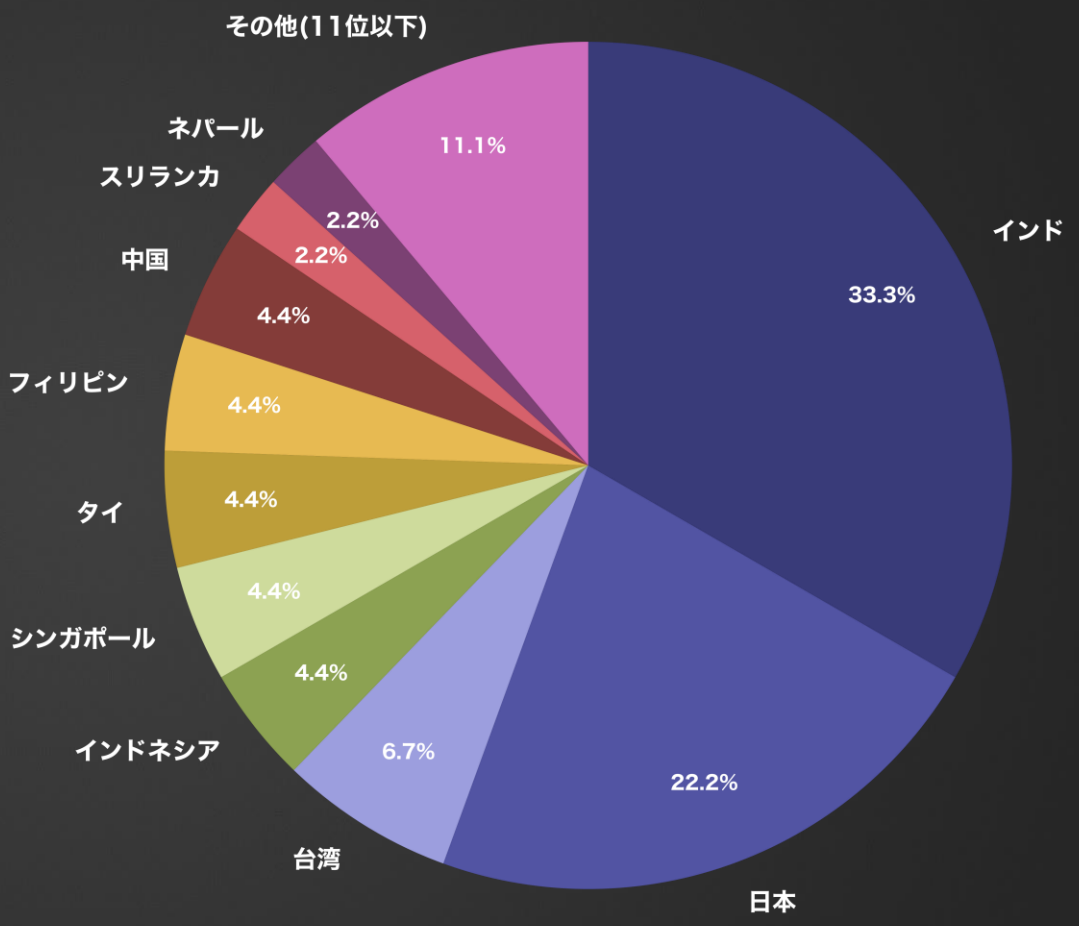
Know your enemy.
Defense leadership.

● 月別内訳 被害国TOP10 （ 2024年 5 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	15	33.3	+ 9
日本	10	22.2	+ 7
台湾	3	6.7	+ 1
インドネシア	2	4.4	± 0
シンガポール	2	4.4	- 1
タイ	2	4.4	+ 1
フィリピン	2	4.4	+ 2
中国	2	4.4	+ 1
スリランカ	1	2.2	± 0
ネパール	1	2.2	+ 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

5

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 － ⑪

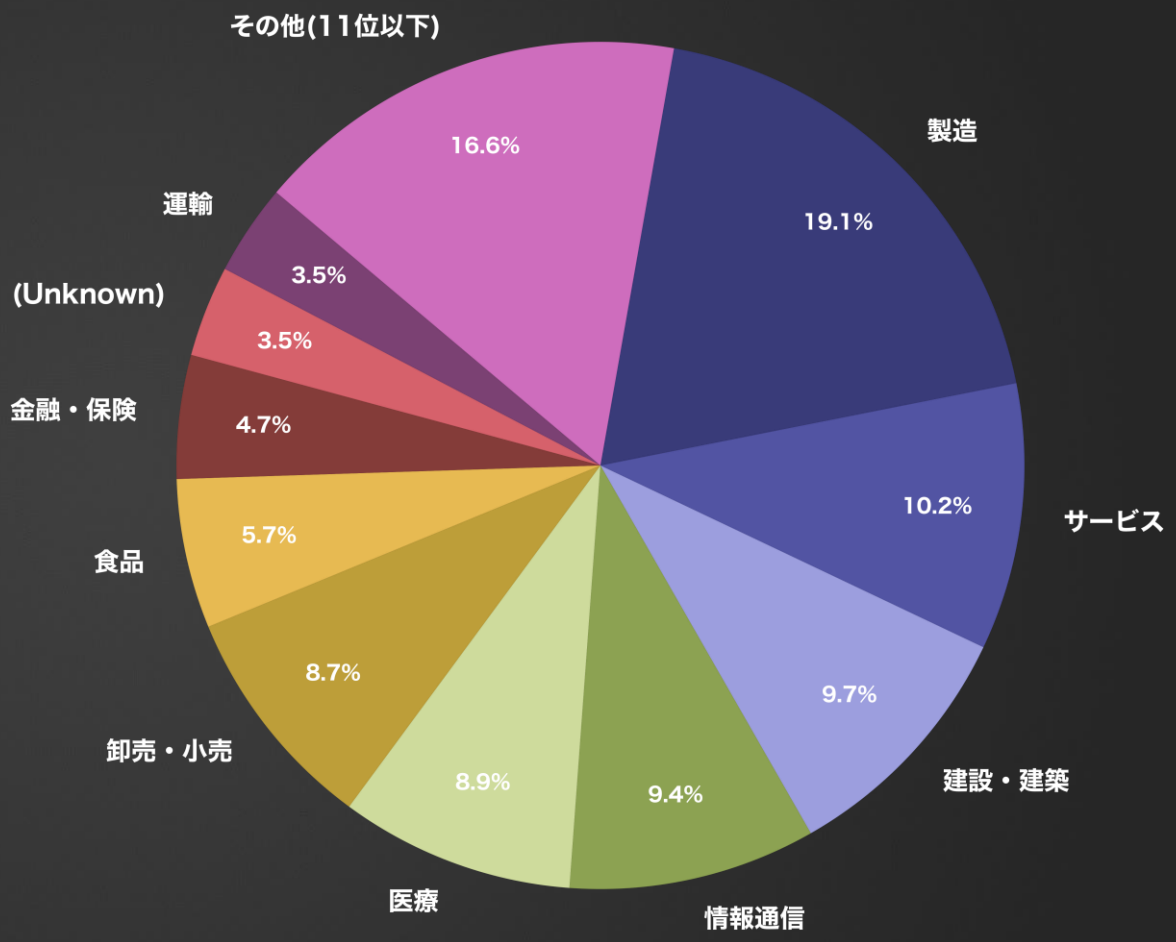
Know your enemy.
Defense leadership.

● 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	19.1	+ 1
サービス	41	10.2	- 3
建設・建築	39	9.7	+ 3
情報通信	38	9.4	+ 13
医療	36	8.9	- 3
卸売・小売	35	8.7	+ 8
食品	23	5.7	+ 8
金融・保険	19	4.7	+ 7
(Unknown)	14	3.5	+ 5
運輸	14	3.5	- 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 － ⑫

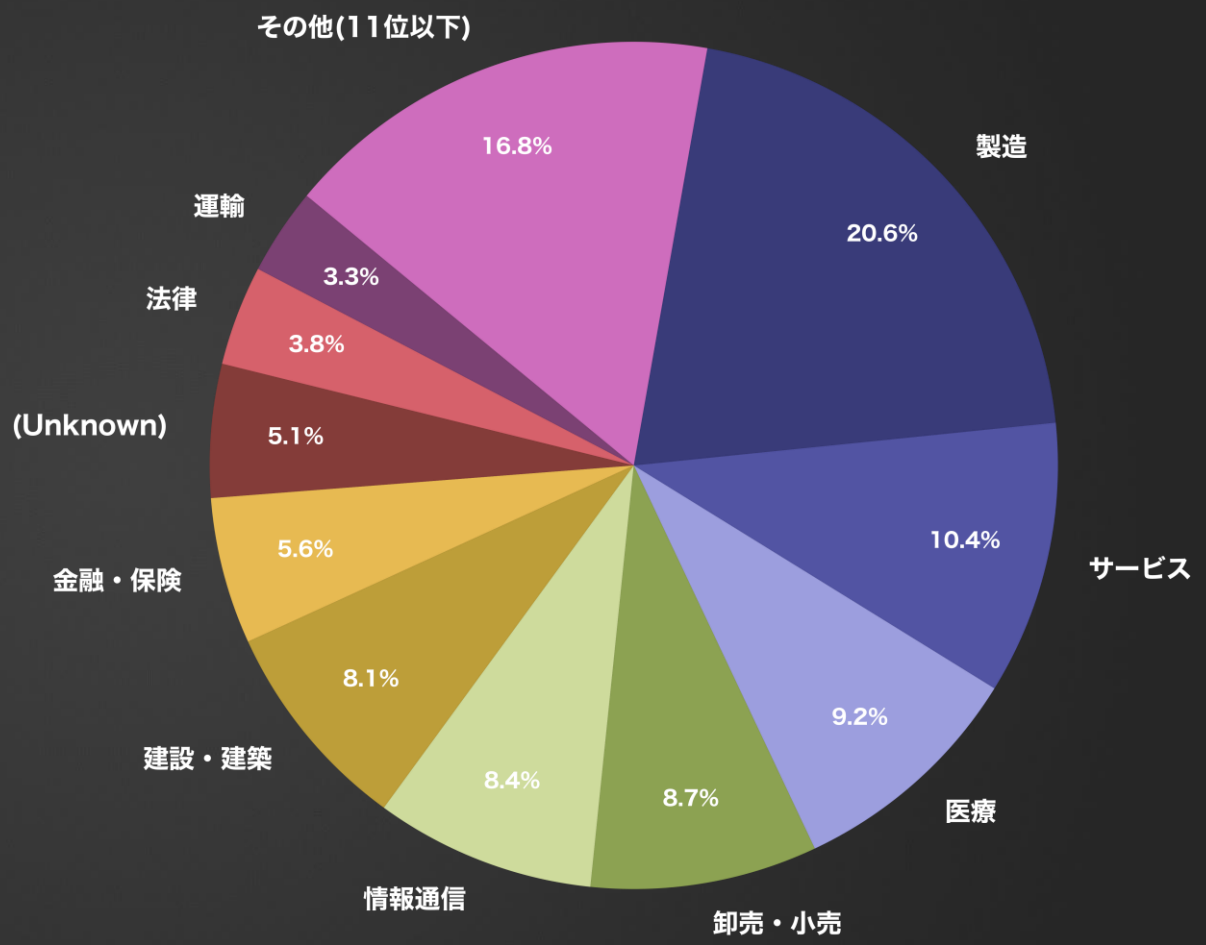
Know your enemy.
Defense leadership.

● 月別内訳 業種 TOP10 （2024年 4 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	81	20.6	+ 4
サービス	41	10.4	± 0
医療	36	9.2	± 0
卸売・小売	34	8.7	- 1
情報通信	33	8.4	- 5
建設・建築	32	8.1	- 7
金融・保険	22	5.6	+ 3
(Unknown)	20	5.1	+ 6
法律	15	3.8	+ 2
運輸	13	3.3	- 1

▼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

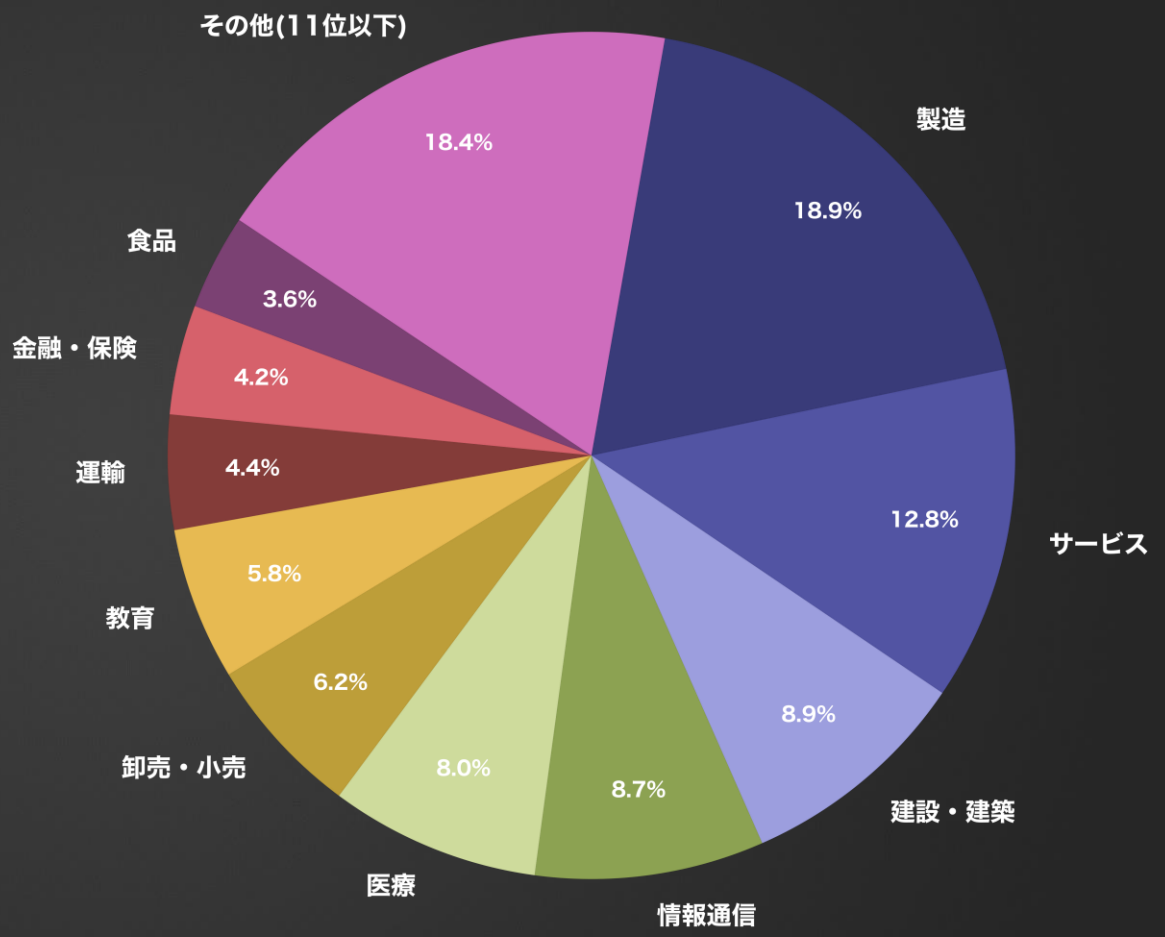
Know your enemy.
Defense leadership.®

● 月別内訳 業種 TOP10 （2024年 5 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	104	18.9	+ 23
サービス	70	12.8	+ 29
建設・建築	49	8.9	+ 17
情報通信	48	8.7	+ 15
医療	44	8.0	+ 8
卸売・小売	34	6.2	± 0
教育	32	5.8	+ 21
運輸	24	4.4	+ 11
金融・保険	23	4.2	+ 1
食品	20	3.6	+ 15

▼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

5

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.

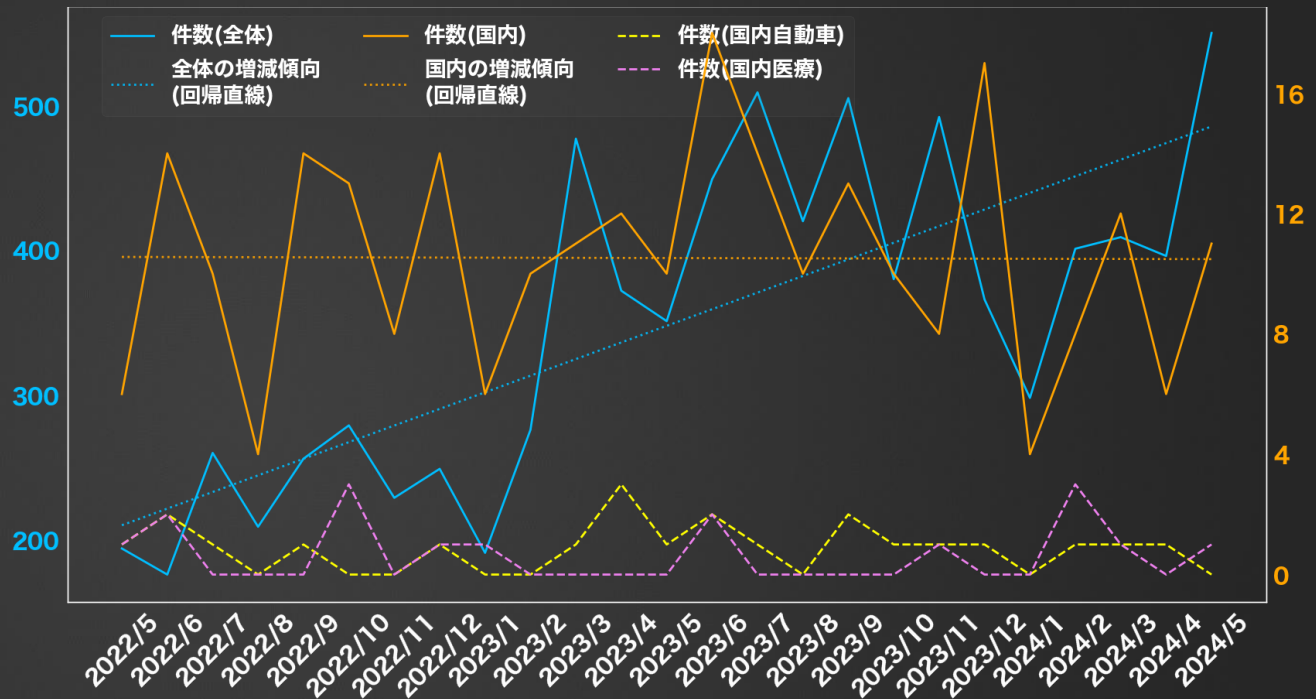
● 被害数の推移（ 2022年5月～2024年5月／全世界及び国内 ）(MBSD調べ)

※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)
2022/5	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	276	10	0	0
2023/3	477	11	1	0
2023/4	372	12	3	0
2023/5	351	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	380	10	1	0
2023/11	492	8	1	1
2023/12	366	17	1	0
2024/1	298	4	0	0
2024/2	401	8	1	3
2024/3	409	12	1	1
2024/4	396	6	1	0
2024/5	550	11	0	1
合計	8694	263	22	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

5

※ 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

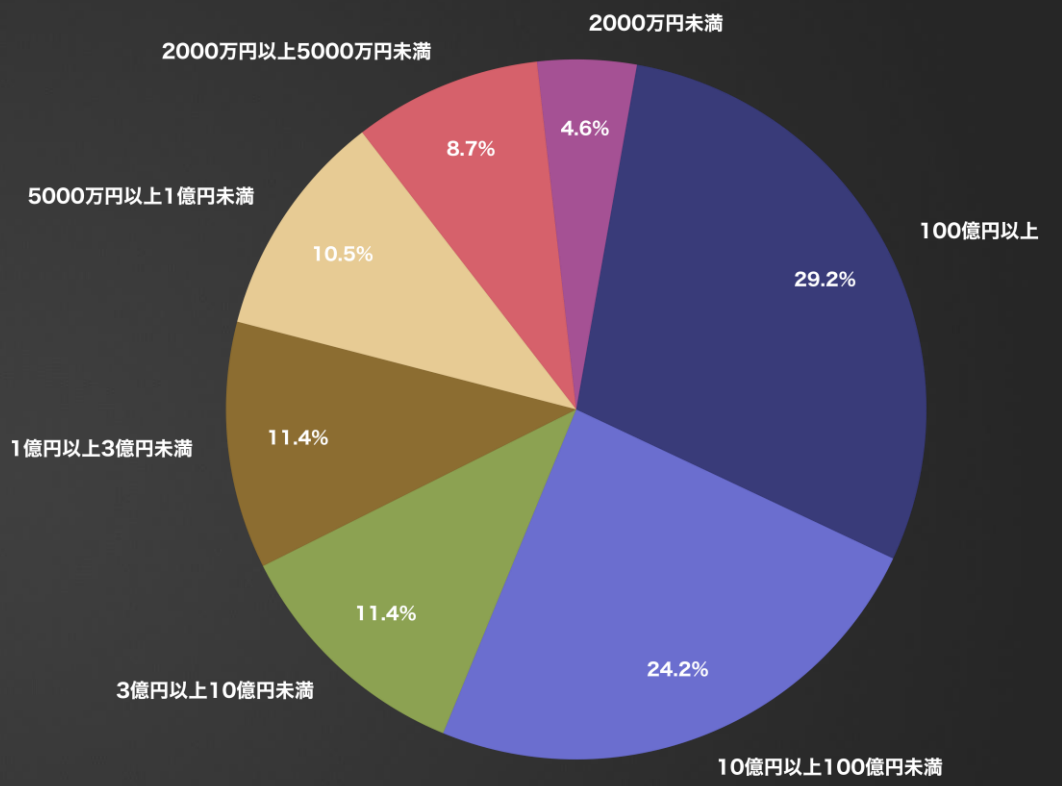
Know your enemy.
Defense leadership.

● 月別内訳 資本金別 （ 2022年5月～2024年5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	64	29.2
10億円以上100億円未満	53	24.2
3億円以上10億円未満	25	11.4
1億円以上3億円未満	25	11.4
5000万円以上1億円未満	23	10.5
2000万円以上5000万円未満	19	8.7
2000万円未満	10	4.6

▼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：35.2%
・10億円未満が該当するとした場合：46.6%

（※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

5

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。

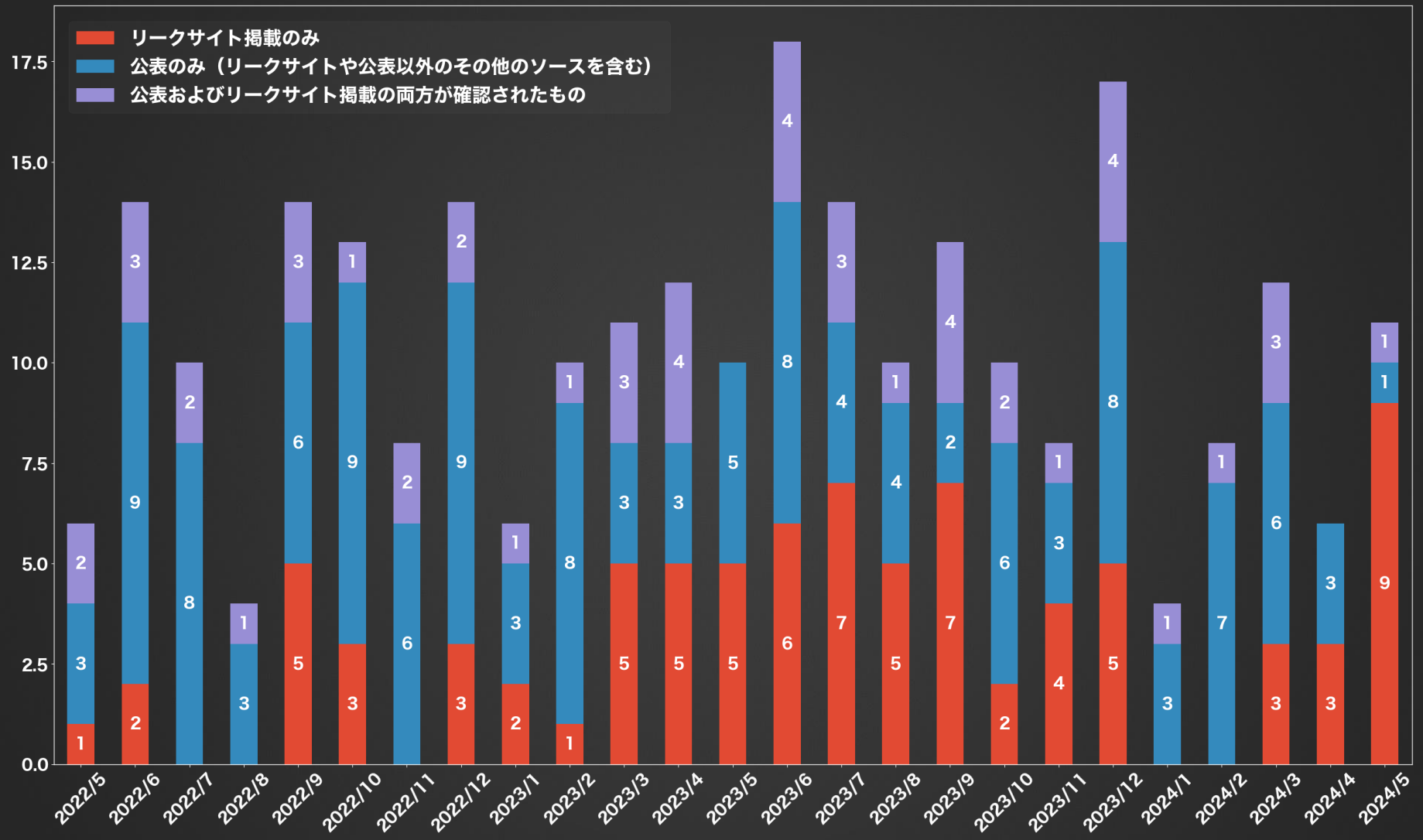
Created by Cyber Intelligence Group

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5月～2024年5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

5

※ 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5月～2024年5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
2023/5	(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	CL0P (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 (Agenda)	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	CL0P (CLOP)	総合エレクトロニクスメーカー(海外拠点)
2023/7	CL0P (CLOP)	総合画像機器メーカー(海外拠点)
2023/7	CL0P (CLOP)	大手飲料メーカー(海外拠点)
2023/7	CL0P (CLOP)	たばこ製造販売会社(海外拠点)
2023/7	CL0P (CLOP)	大手電気機器メーカー(海外拠点)
2023/7	CL0P (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	CL0P (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 (Agenda)	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)
2023/12	(Unknown)	大手出版社
2023/12	(Unknown)	地方自治体

※ 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 － 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5月～2024年5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
2023/12	(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	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	化学メーカー
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)	商工会議所
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	CL0P (CLOP)	大手文房具メーカー(海外拠点)
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)
2024/4	(Unknown)	繊維製品サプライヤー
2024/4	(Unknown)	電子機器サプライヤー
2024/4	LockBit	アクセサリーパーツメーカー
2024/4	STORMOUS	大手電機メーカー(海外拠点)
2024/4	Hunters International	大手自動車メーカー(海外拠点)
2024/4	8BASE	電子部品メーカー
2024/5	(Unknown)	地方独立行政法人
2024/5	LockBit	製紙会社(海外拠点)
2024/5	LockBit	ITサービス会社(海外拠点)
2024/5	Hunters International	音響関連機器メーカー(海外拠点)
2024/5	8BASE	ITサービス会社
2024/5	8BASE	協同組合
2024/5	8BASE	OAサプライ用品メーカー
2024/5	8BASE	農業機械販売会社
2024/5	8BASE	税理士法人
2024/5	Ransomhub	ソフトウェア企業
2024/5	RansomHouse	建築部品メーカー

※ 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）

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.®

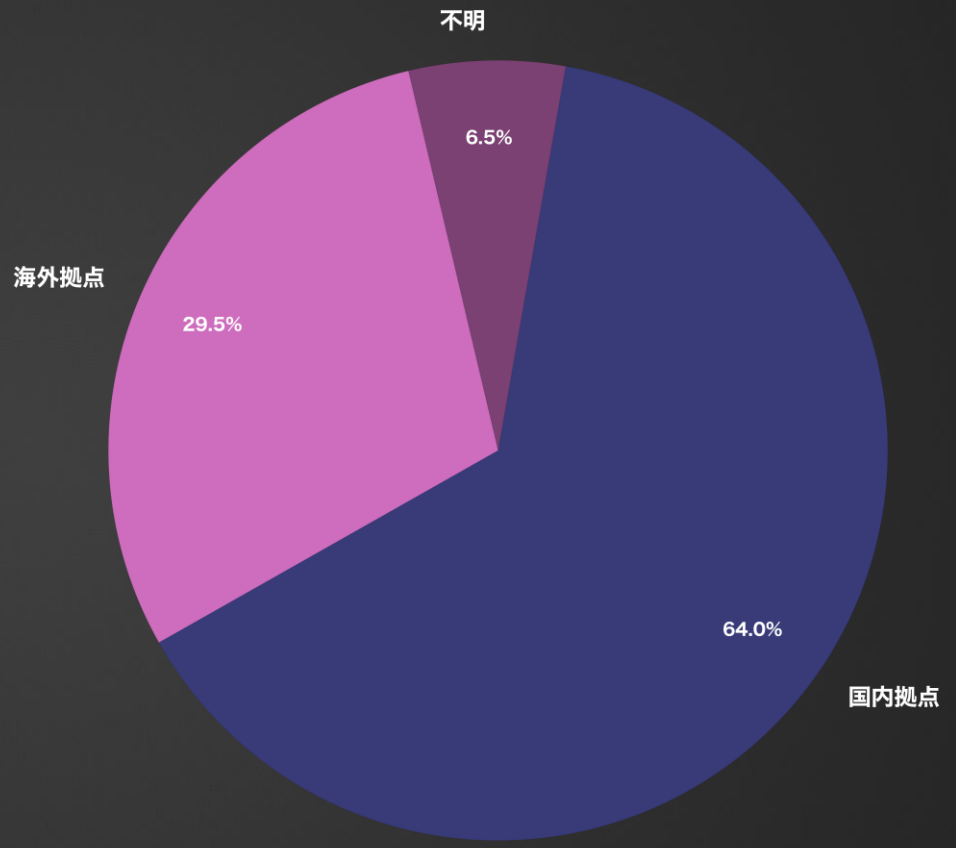
● 公となった国内被害組織における拠点割合（ 過去1年間／2023年5月～2024年5月）(MBSD調べ)

（※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	89	64.0
海外拠点	41	29.5
不明	9	6.5

▼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。

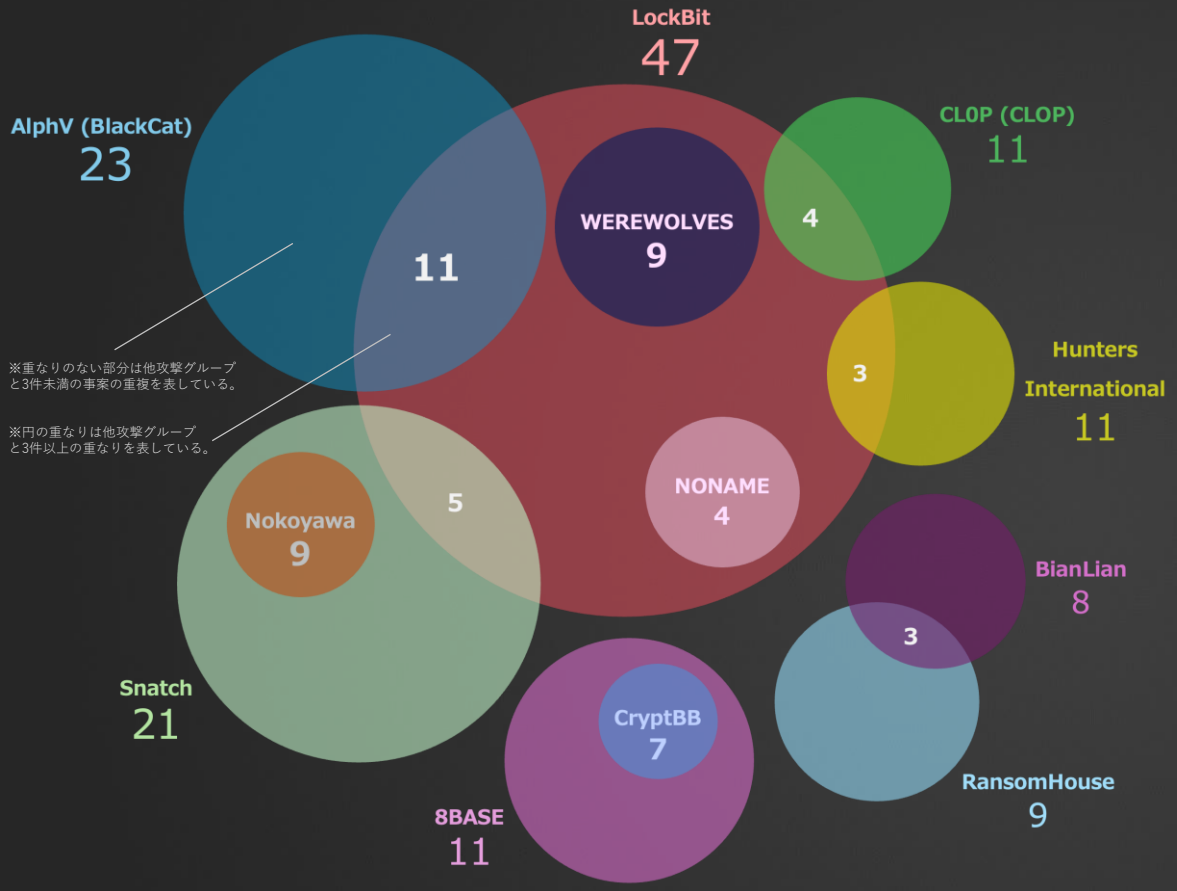
Created by Cyber Intelligence Group

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.

繰り返し暴露された事案数の集計と攻撃グループ間の関係性 (MBSD調べ)

（過去2年間／2022年6月～2024年5月／累計132件）



※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

ランサムウェア攻撃の被害の中には、データを盗まれたのちにリークサイトで暴露され、さらに異なる攻撃グループのリークサイトなどから二度三度と繰り返し暴露されるケースがある。
つまり言い換えると、ランサムウェア攻撃の被害組織の中には、複数回にわたってリークサイトに情報が掲載される「多重被害」に遭う組織が存在する。

近年の有名な事例としては、AlphV (BlackCat)の被害に遭い身代金を支払った被害組織の情報をアフィリエイトが他の攻撃グループに持ち込み、その被害組織を再度脅迫したケースなどが挙げられる。
これは攻撃グループの内部で起きた報酬支払いに関する内輪揉めが原因であるが、多重被害の原因は多岐にわたる。

例えば
- 被害後の対策不足による再侵入
- 攻撃グループ間の連携によるデータの横流し
- 攻撃グループによる他グループのリークサイトやハッカーフォーラムからのデータ盗用
- 攻撃グループメンバーやアフィリエイトによるデータの持ち出し

などが理由の一部として挙げられる。

一度盗まれたデータの流用を完全に防ぐことは困難だが、複数回の侵入による多重被害は、インシデント発生時の適切な対応とその後の対策により、防御の可能性を大幅に高めることができる。
ランサムウェア被害発生を想定し、有事の際に冷静な対応ができるよう、対策のための情報の一つとして多重被害の実態を把握しておくことも重要である。

※ 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 － ⑳

Know your enemy.
Defense leadership.®

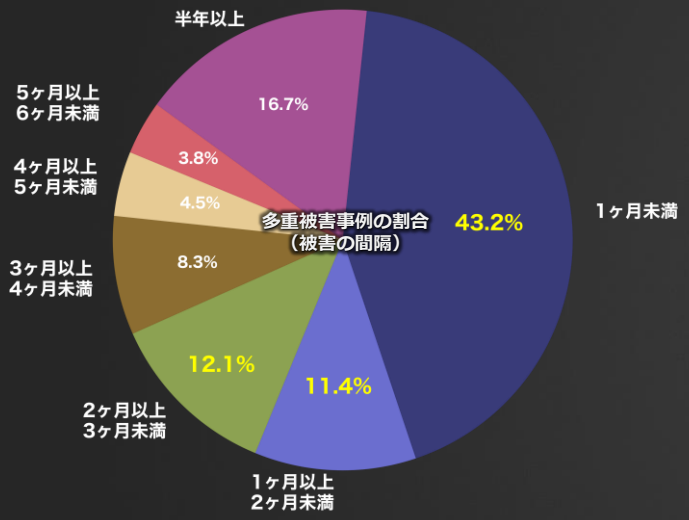
※多重被害：一度ランサムウェア攻撃の被害を受けた組織が異なる時期に異なる攻撃グループのリークサイトに再び掲載されるケース

多重被害に遭った被害組織の傾向と分析 （MBSD調べ）

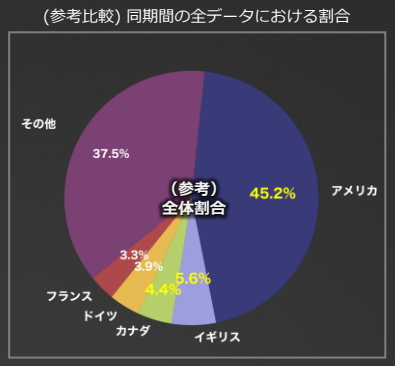
（過去2年間／2022年6月～2024年5月）

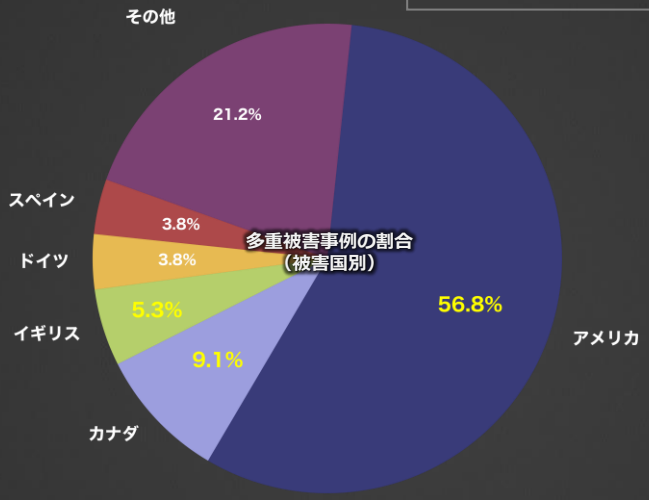
▼被害の間隔

（一度目の被害から二度目の被害までの間隔）

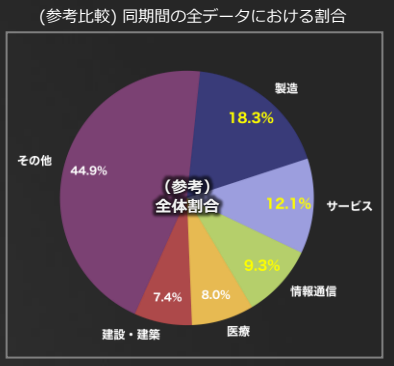


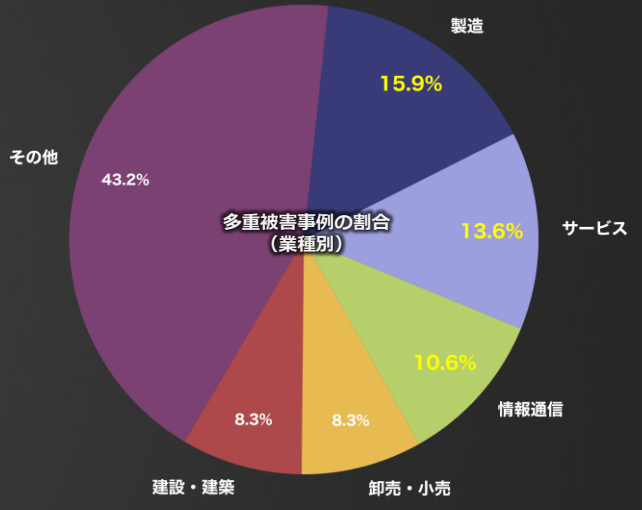
▼被害国別





▼業種別





▶多重被害に遭った組織数の累計：132件（全体8511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。これら多重被害の事例には日本関連の組織も含まれており、一度侵入されデータ窃取されれば、いかなる組織でも多重被害に遭う可能性がある事を示す。
こうした被害を防ぐためには、日頃からの対策に加え万が一ランサムウェアの被害に遭っても身代金を支払わない（脅せば支払う組織であると認知されてしまう）ことや、繰り返しの侵入を防ぐために侵入経路の徹底的な洗い出し等の事後対応・再発防止策の実施が不可欠である。

※ 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