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5月号 Rev 1.01
(2024年4月分)

2024
4

更新履歴

Rev 1.01 (2024年8月15日)：「今月のハイライト」内、 Dispossessorに関する情報の更新。

Created by Cyber Intelligence Group

今月のハイライト

LockBitの活動減少と新興グループの台頭

LockBitランサムウェア攻撃グループの2024年4月におけるリークサイト新規掲載数は、過去1年間の月平均80件以上から大幅に減少し、過去最低水準である24件となった。2024年2月に複数の国が協力して実行した「Operation Cronos」によってサーバーの一部を押収された後、LockBitはすぐさま別のリークサイトを立ち上げ活動を継続していた。
3月は94件の掲載するも、その多くは過去に掲載した被害組織の再掲載であり、実質的な掲載数は56件となるなど減少傾向が予測できる結果となっていた。過去には増減を繰り返しながらも、長期に渡ってトップクラスの掲載数を維持していたことを考慮すると、今月の大幅な減少によるトップ交代は特に印象的である。
一方、4月の攻撃グループ全体のリークサイト掲載数は、LockBitの掲載数減少にもかかわらず、前月の405件から393件とわずかな減少にとどまった。今月の掲載数は最多であるPLAYでも30件と比較的少なく、多くの攻撃グループが活発に活動している状況がうかがえる。
また、4月には立て続けに8つの新たな攻撃グループの活動拠点（リークサイト）が確認された。LockBit配下で活動していたアフィリエイトの内部移動がどこまで関与するかは不明だが、これには、LockBitリークサイトと記載内容に多くの類似点が見られる「Apt73 (Eraleig)」や、リークサイトのデザインがLockBitと類似している「Red Ransomware Group」、「Dark Vault」、「Dispossessor」が含まれる。さらには医療関連業種を中心に攻撃する「QIULONG」や、「RaaS」を「Ransomware-as-a-Service」ではなく“Recovery-as-a-Service”、「ランサムウェア」を”Secure Data Protector”と記載するといった、表現の節々に自らの活動を正当化する言動が特徴的な「Apos Security」など、新しい観点で攻撃を行う攻撃グループも出現しており、これら新興攻撃グループの活動も全体の掲載数が微減にとどまった要因といえるであろう。

さらに、2024年2月に押収されたのちオフラインとなっていたリークサイトが5月に入り再びオンラインになり、LockBit首謀者に関する情報などが公開されたことを確認。また同じタイミングで、法執行機関が該当人物を起訴したと発表。この点については、次号にて詳細な解説を予定している。

Dispossessorによる他グループからの情報盗用と心理的圧力を利用した恐喝の可能性

「Dispossessor」は2024年2月に活動拠点が確認された攻撃グループ（※2024年8月追記：2024年8月12日の押収に際しFBIが公表(※1)した情報によれば活動開始は2023年8月）であり、リークサイト上でアフィリエイトに対するルールを掲載するなど自らをランサムウェア攻撃グループであると主張している。リークサイトに300件以上の被害組織情報を掲載し、出現当初はそのデザインの類似性や掲載された被害組織情報などから、LockBitのリブランド先である可能性や模倣犯である可能性が指摘されていた。
ところがDispossessorが掲載した被害組織情報を詳細に分析した結果、大半が他の攻撃グループが過去に掲載したものであることが判明。 LockBitのみならず、8Base、CLOP、Snatch、NOKOYAWA、Hunters Internationalなど多岐にわたる攻撃グループが掲載した攻撃声明と重複していた。 他グループとの重複を計測すると4月は327件中320件であり、残る7件も出所は実質的に不明である。そのため、Dispossessor は自ら攻撃を仕掛けるグループですらない可能性があり、他グループの攻撃を転載し便乗詐欺を行っているという見方もできる。
一方、もし該当の7件が独自の攻撃であった場合、Dispossessorが主張どおりランサムウェア攻撃グループであるという可能性も残る。その場合は、他の複数のランサムウェア攻撃グループが公表した攻撃情報を転載することで掲載数を実態よりも大きく水増しし、より力のある攻撃グループのように見せかけ、被害組織に心理的な圧力をかけることで恐喝を優位に進める目的があると見ることもできる。

（※1）https://www.fbi.gov/contact-us/field-offices/cleveland/news/international-investigation-leads-to-shutdown-of-ransomware-group

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。

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（拠点数と一覧）

MBSD Know your enemy. Defense leadership.®

● 当月監視対象の攻撃グループ数（※1）：172グループ（※2）

→当月リークサイト掲載の活動を確認した攻撃グループ数：41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）

8BASE
ABYSS
AKIRA
AKO
Alpha(MYDATA)
AlphV / BlackCat
● Apos Security
● APT73 (Eraleig)
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
● dAn0n
DARK VAULT
DarkAngels
DARKBIT
DARKPOWER
DarkRace
DarkRypt
Darkside
● Dispossessor
Donex
Donut
DoppelPaymer
dotAdmin
DragonForce
Dunghill
eCh0raix
El_Cometa
● EMBARGO
Endurance
Entropy
Everest
FSTeam
Grief
Groove
Haron
● HelloGookie (HelloKitty)
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
● QIULONG
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 Group
RedAlert (N13V)
Relic
Revil (Sodinokibi)
Rhysida
ROOK
Royal
Rransom
Sabbath (54bb47h)
shaoleaks
SIEGEDSEC
SLUG
Snatch
Solidbit
● SpaceBears
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。

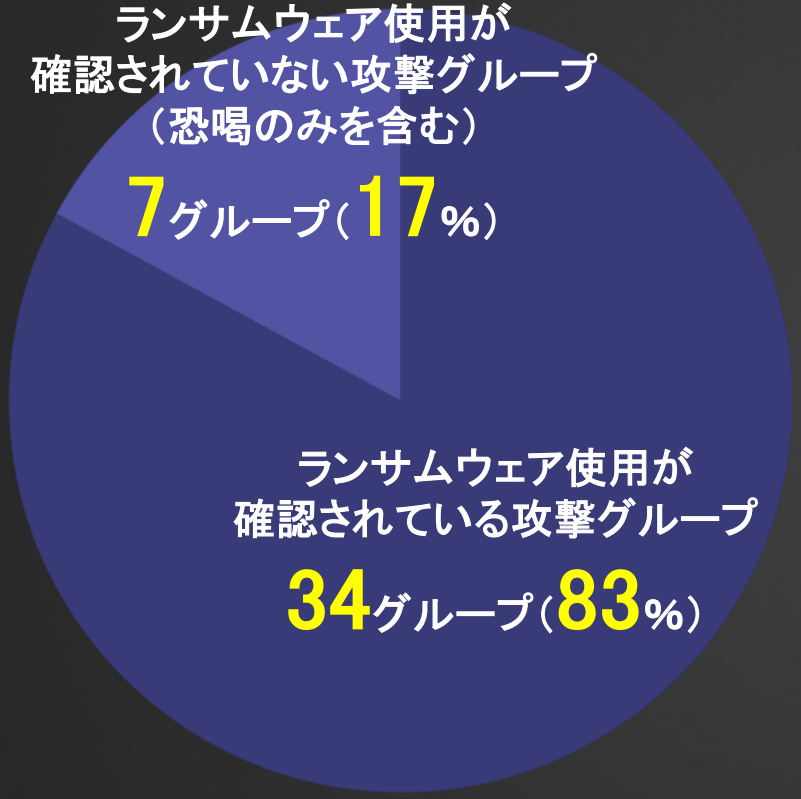
Created by Cyber Intelligence Group

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4月）

（※2024年4月にリークサイト掲載を確認した攻撃グループ全41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4月に活動中である事が確認された全41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

4

年間 統計

（全世界）

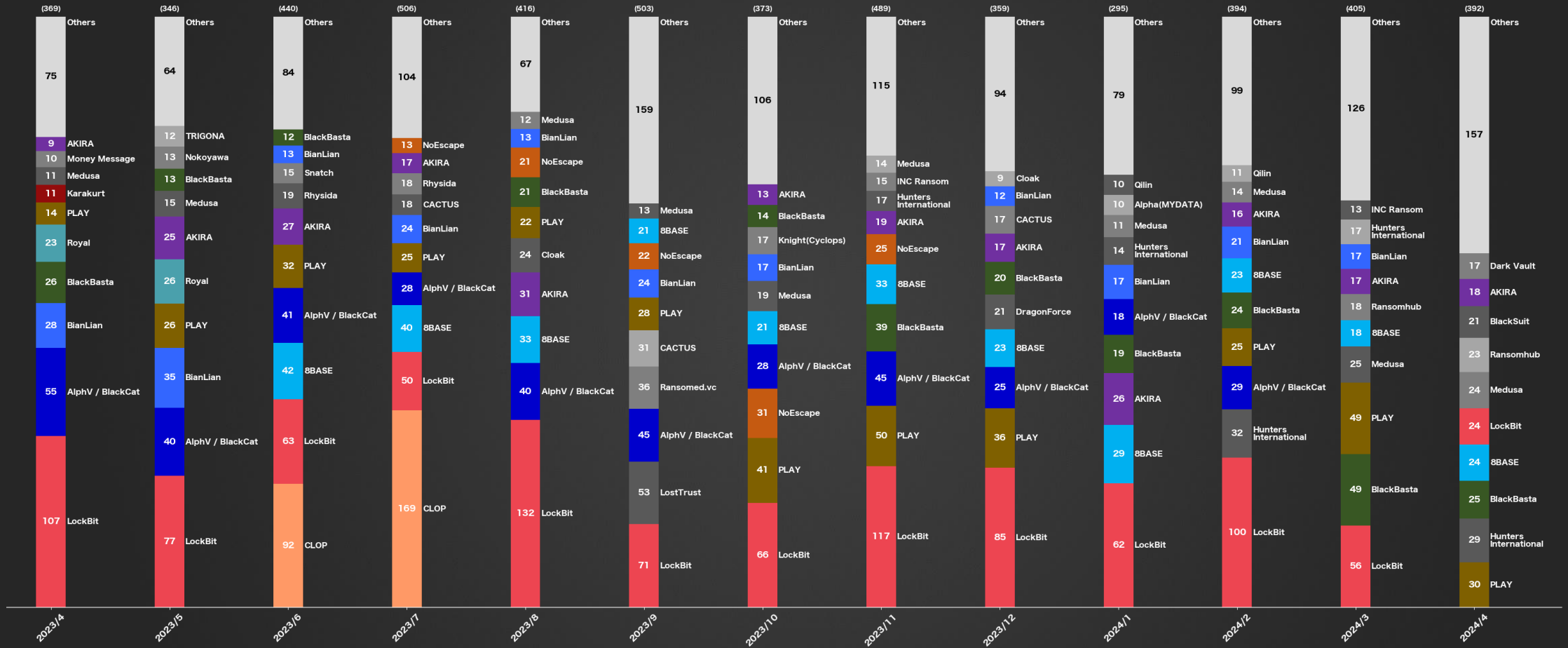
※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
　（日本にフォーカスした一部の表／グラフのみ、公表や報道から判明した数を加味し集計）
※ 国内被害組織に関する各種データについては、海外拠点（支社／関連会社）を含む。
※ 業種分類や集計方法を含む本レポートの各データ（値）はMBSD独自の観測および集計結果となる。
※ これらはあくまで公に把握できた攻撃数の集計結果であり、実被害数はさらに多いものと想定される。
※ 攻撃日が判明している場合は攻撃日、不明な場合はリークサイト等への掲載日や記載日を元に集計している。
※ ごく一部のランサムウェアの使用が明確に確認されていない暴露＆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4月～2024年4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

Know your enemy.
Defense leadership.®

2024

4

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 － ②

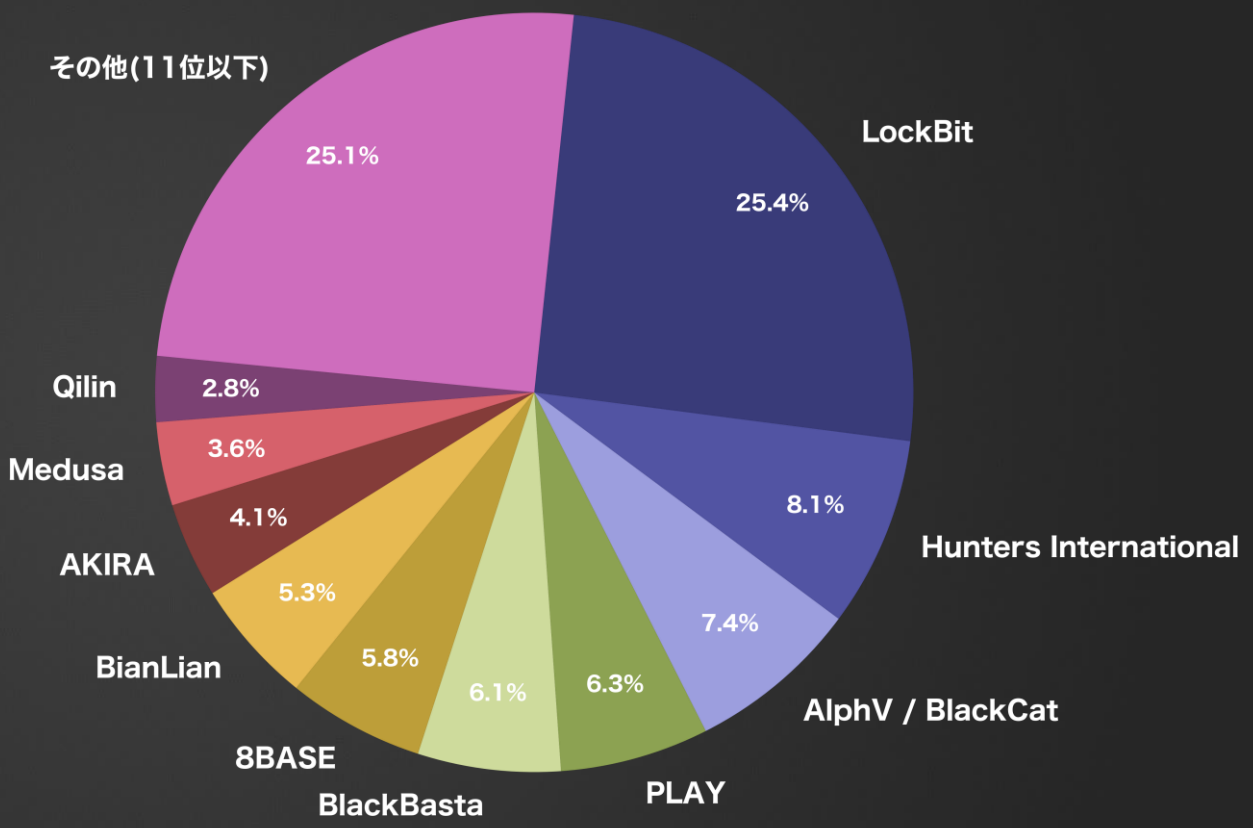
Know your enemy.
Defense leadership.®

● 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 － ③

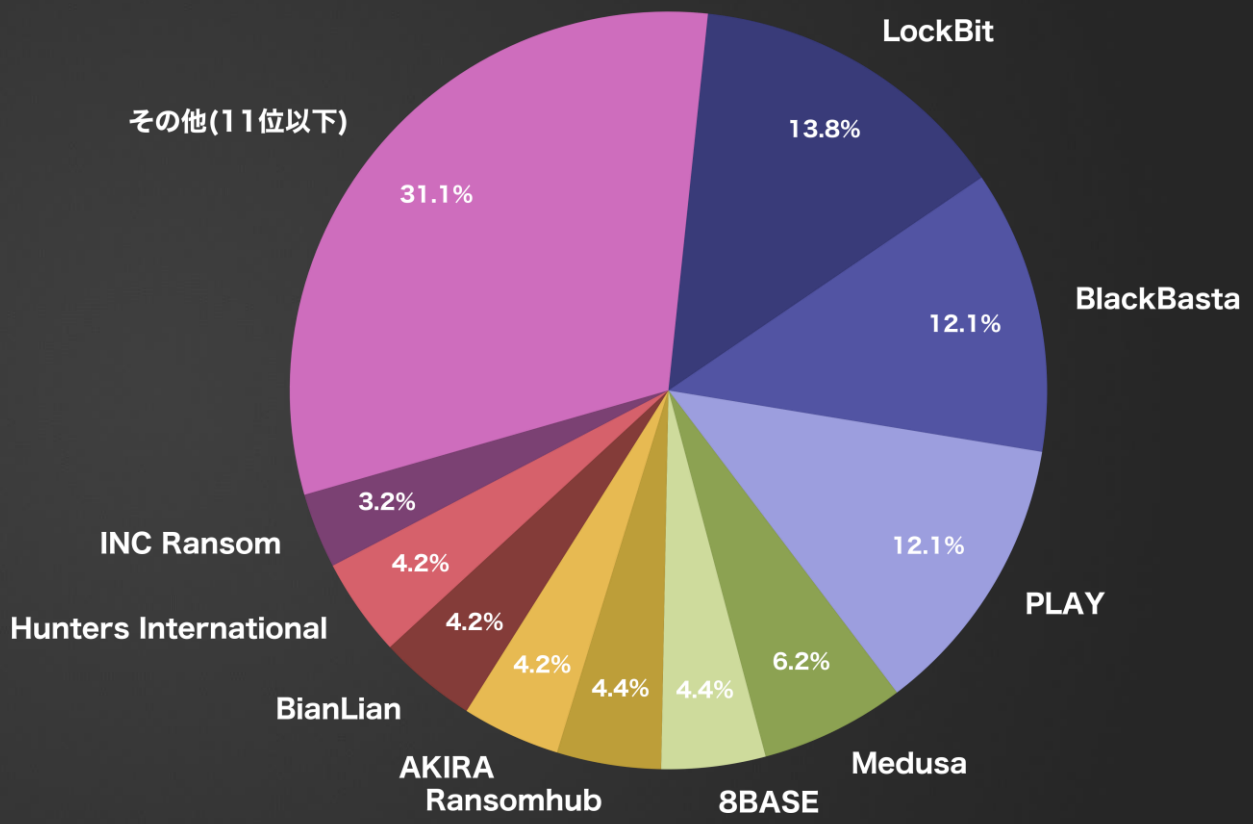
Know your enemy.
Defense leadership.

● 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	12.1	+ 25
PLAY	49	12.1	+ 24
Medusa	25	6.2	+ 11
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

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

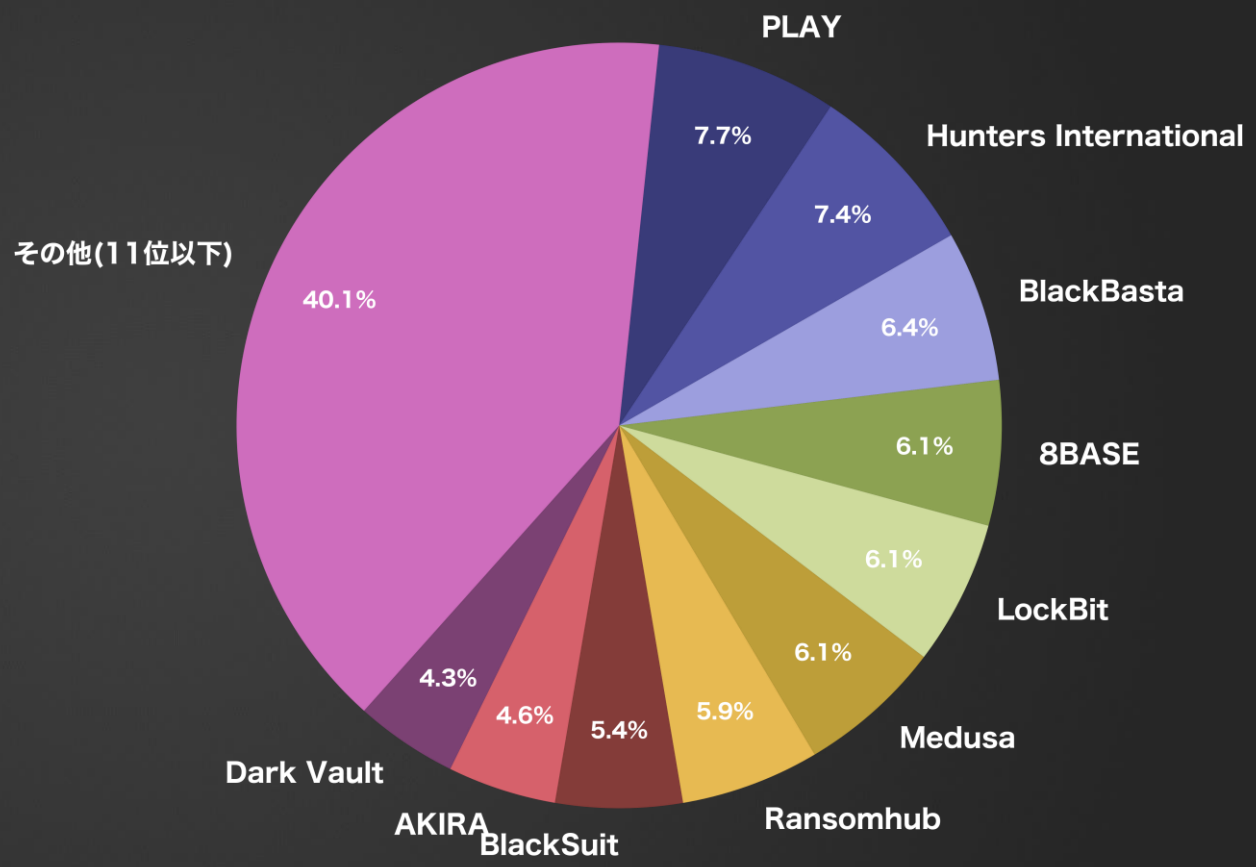
Know your enemy.
Defense leadership.®

● 月別内訳 攻撃グループ TOP10 （2024年 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	7.7	- 19
Hunters International	29	7.4	+ 12
BlackBasta	25	6.4	- 24
8BASE	24	6.1	+ 6
LockBit	24	6.1	- 32
Medusa	24	6.1	- 1
Ransomhub	23	5.9	+ 5
BlackSuit	21	5.4	+ 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

Know your enemy.
Defense leadership.®

2024

4

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

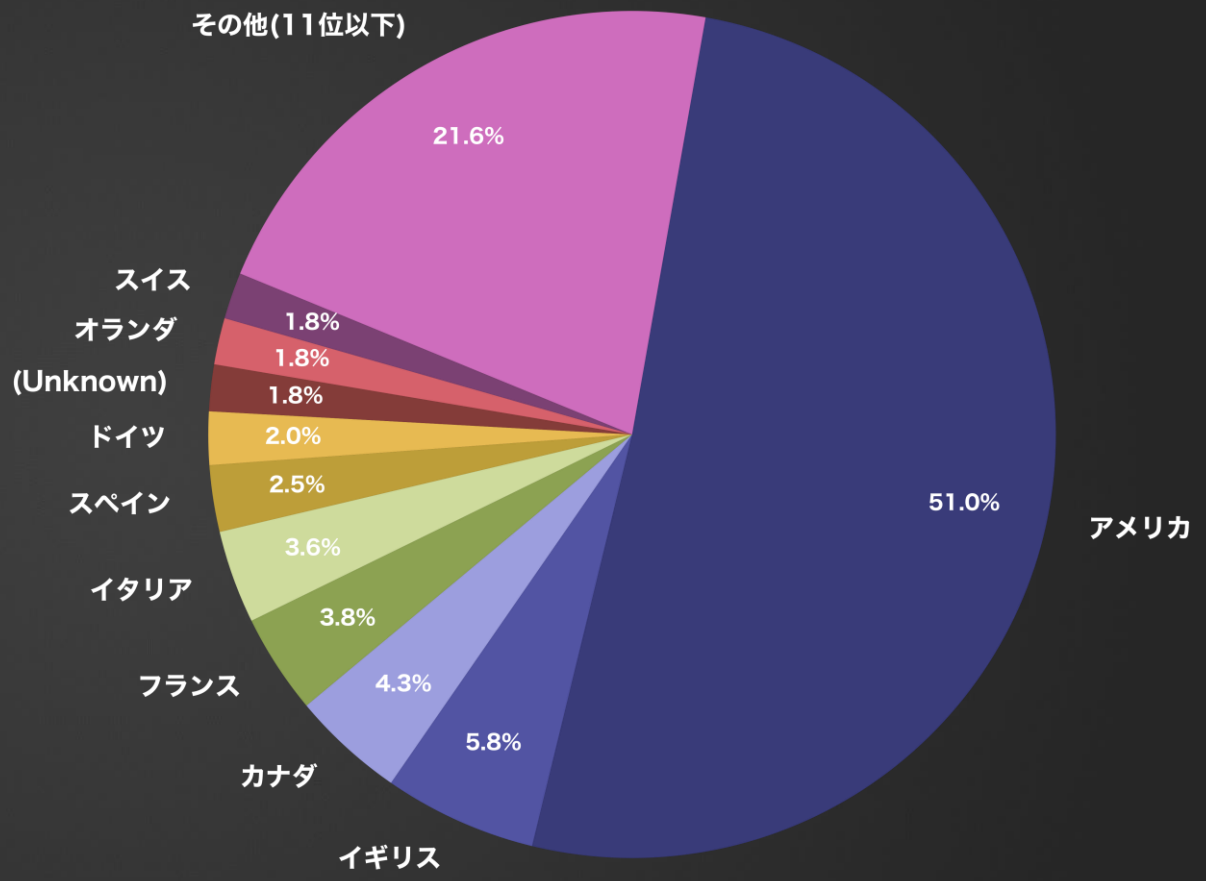
Know your enemy.
Defense leadership.®

● 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	201	51.0	+ 46
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
ドイツ	8	2.0	+ 2
(Unknown)	7	1.8	+ 6
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 － ⑥

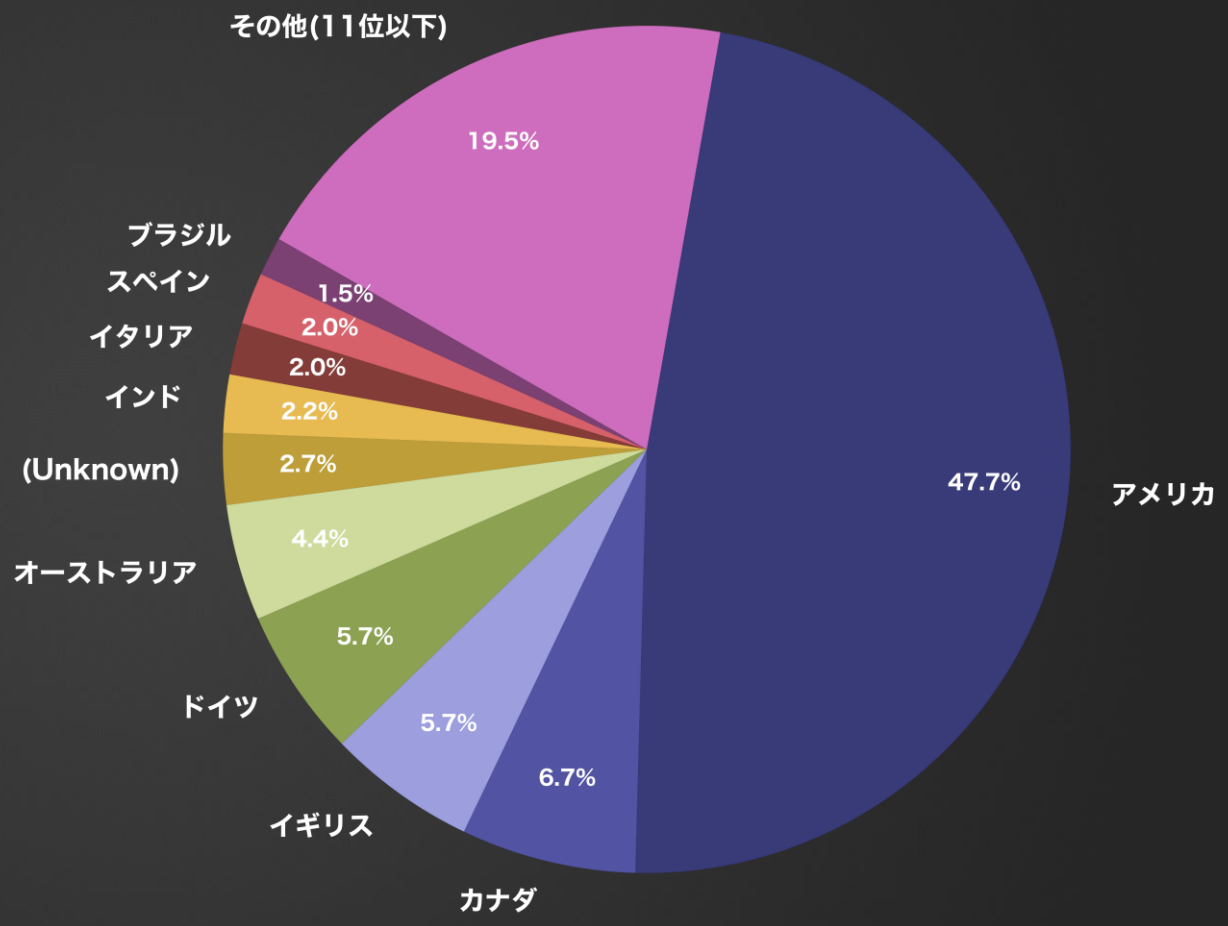
Know your enemy.
Defense leadership.®

● 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	47.7	- 8
カナダ	27	6.7	+ 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	+ 4
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 － ⑦

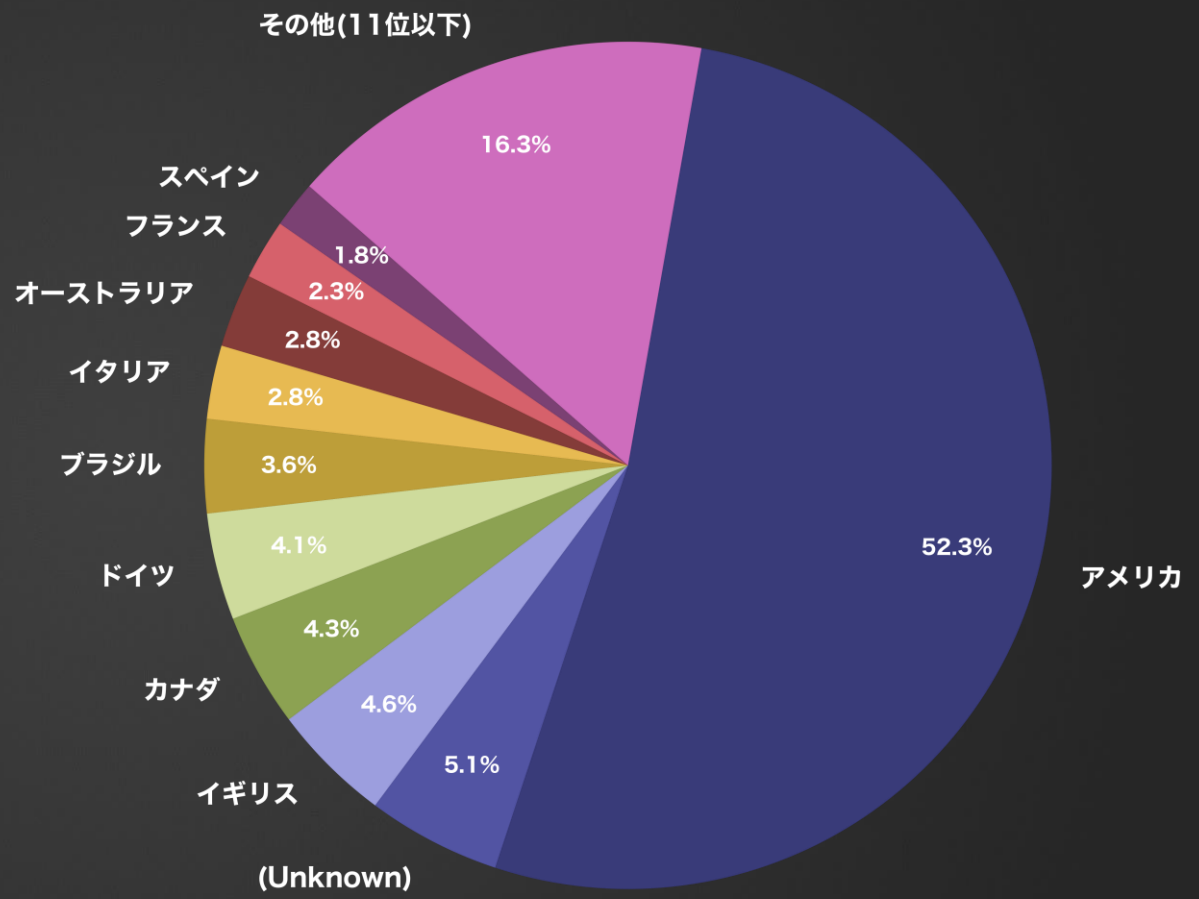
Know your enemy.
Defense leadership.®

● 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	205	52.3	+ 12
(Unknown)	20	5.1	+ 9
イギリス	18	4.6	- 5
カナダ	17	4.3	- 10
ドイツ	16	4.1	- 7
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

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

2024

4

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

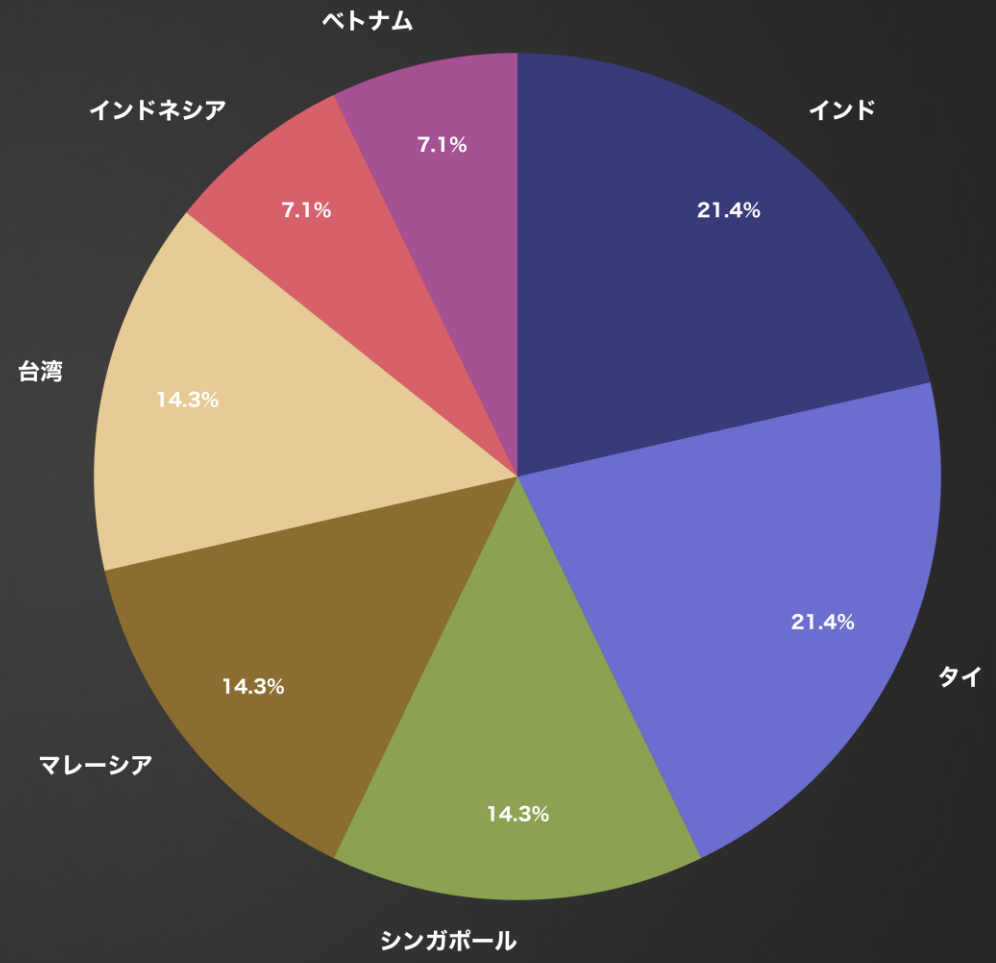
Know your enemy.
Defense leadership.

● 月別内訳 被害国TOP10 （ 2024年 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 － ⑨

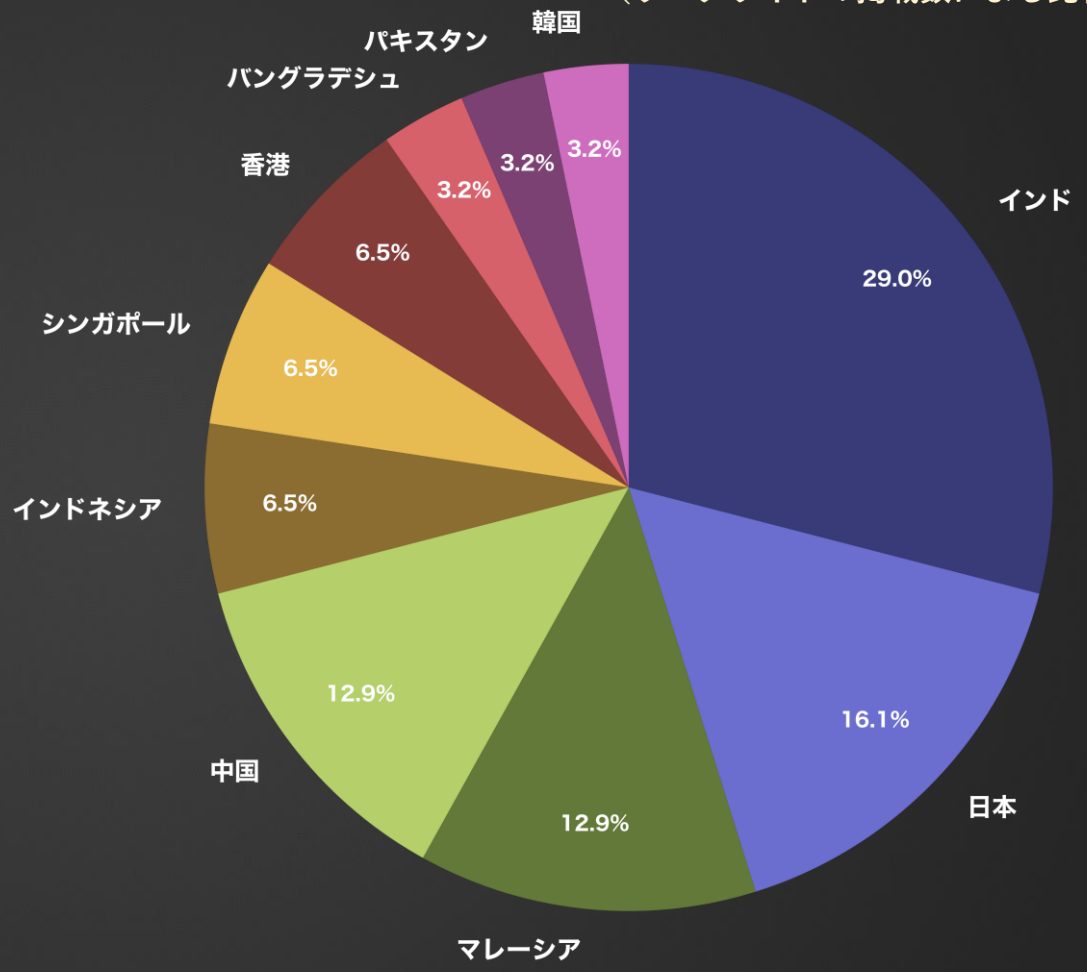
Know your enemy.
Defense leadership.

● 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	+ 5
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 － ⑩

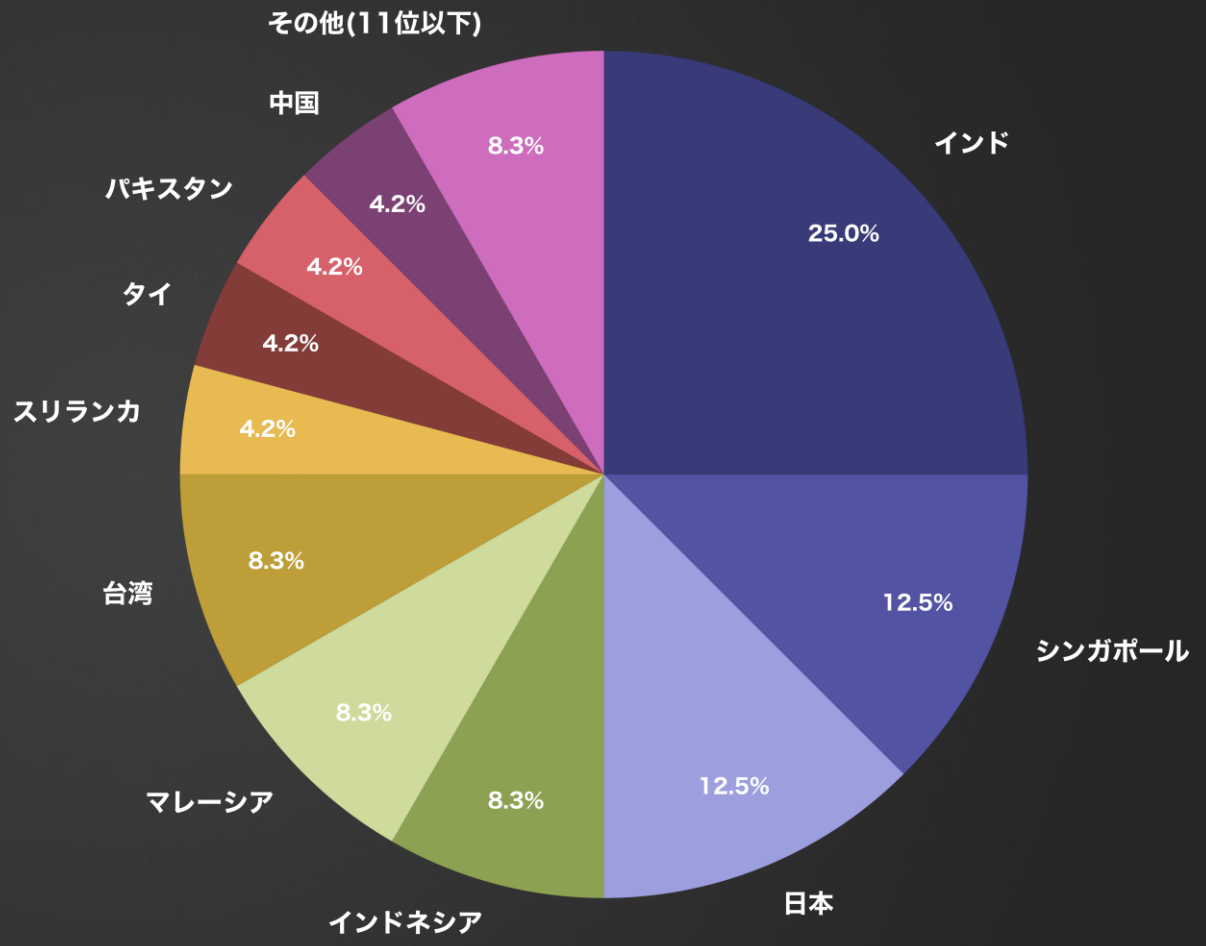
Know your enemy.
Defense leadership.

● 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

Know your enemy.
Defense leadership.®

2024

4

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

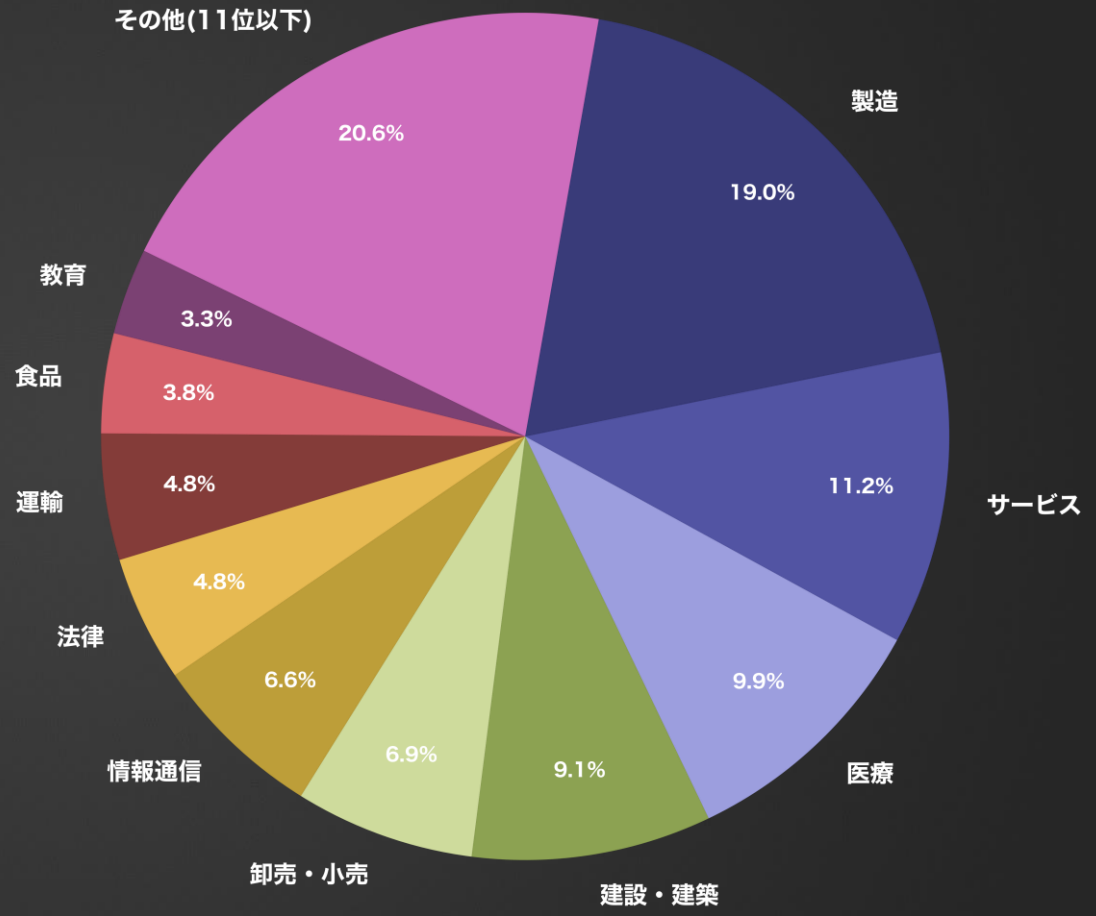
Know your enemy.
Defense leadership.

● 月別内訳 業種 TOP10 （2024年 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	75	19.0	+ 18
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	26	6.6	+ 6
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 － ⑫

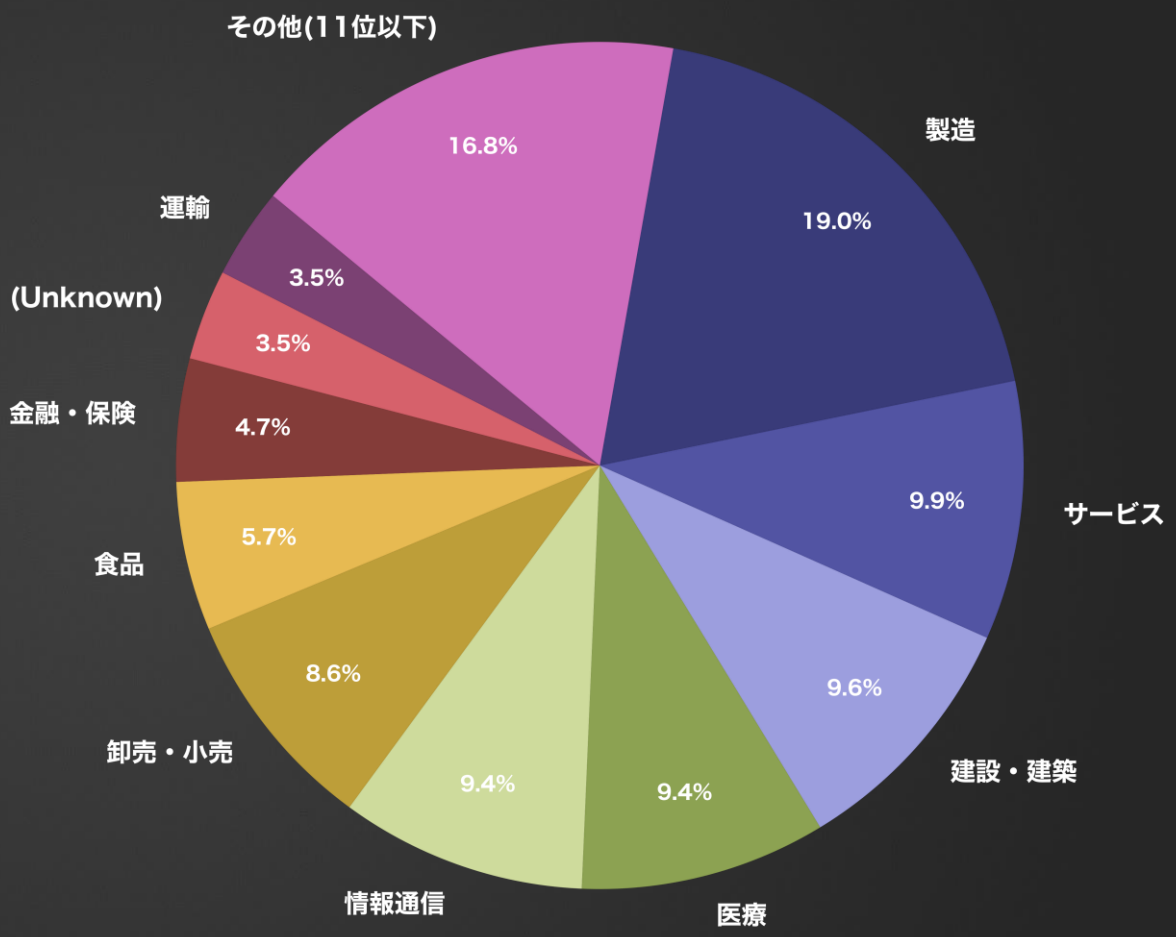
Know your enemy.
Defense leadership.®

● 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	19.0	+ 2
サービス	40	9.9	- 4
建設・建築	39	9.6	+ 3
医療	38	9.4	- 1
情報通信	38	9.4	+ 12
卸売・小売	35	8.6	+ 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 － ⑬

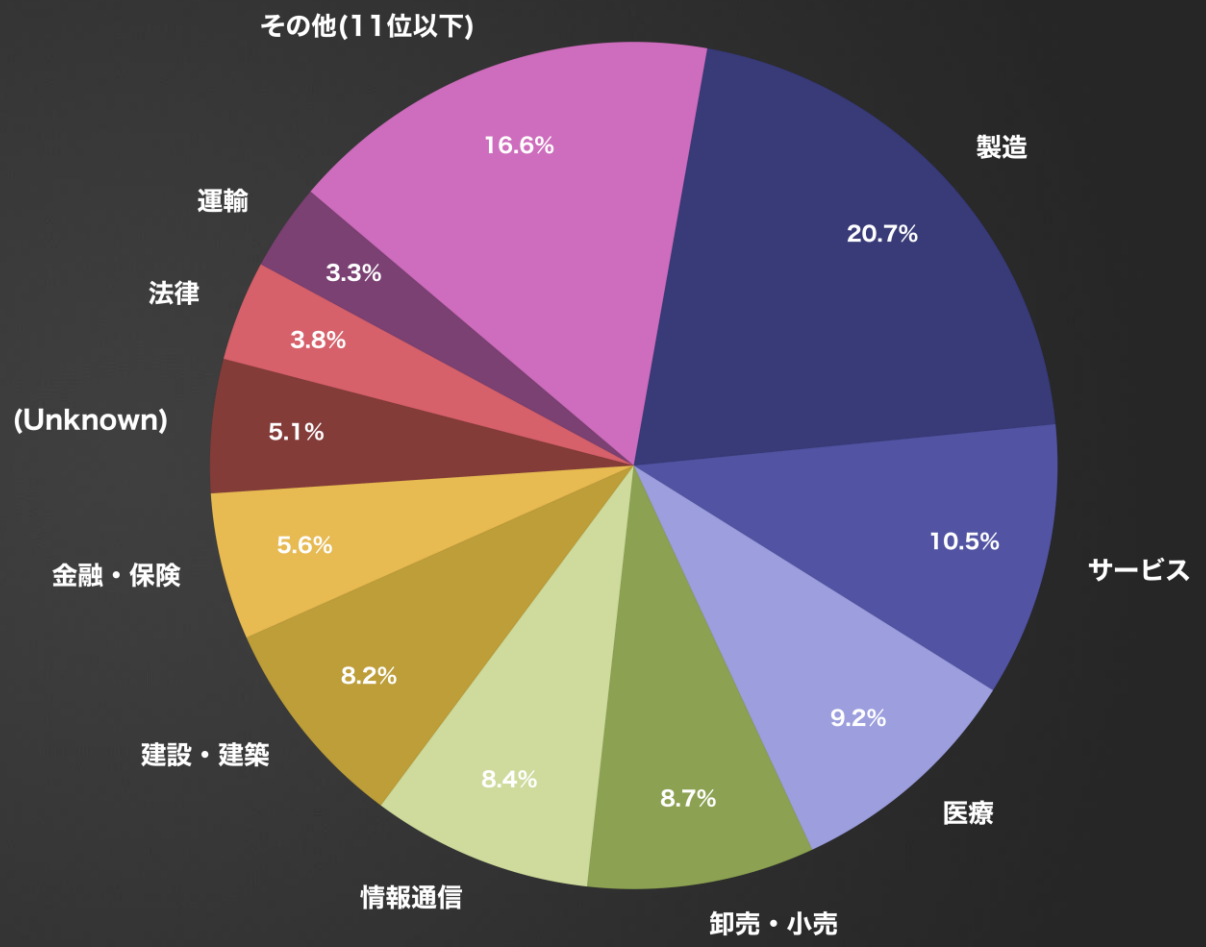
Know your enemy.
Defense leadership.

● 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	20.7	+ 4
サービス	41	10.5	+ 1
医療	36	9.2	- 1
卸売・小売	34	8.7	- 1
情報通信	33	8.4	- 5
建設・建築	32	8.2	- 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

Know your enemy.
Defense leadership.®

2024

4

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

MBSD Know your enemy. Defense leadership.®

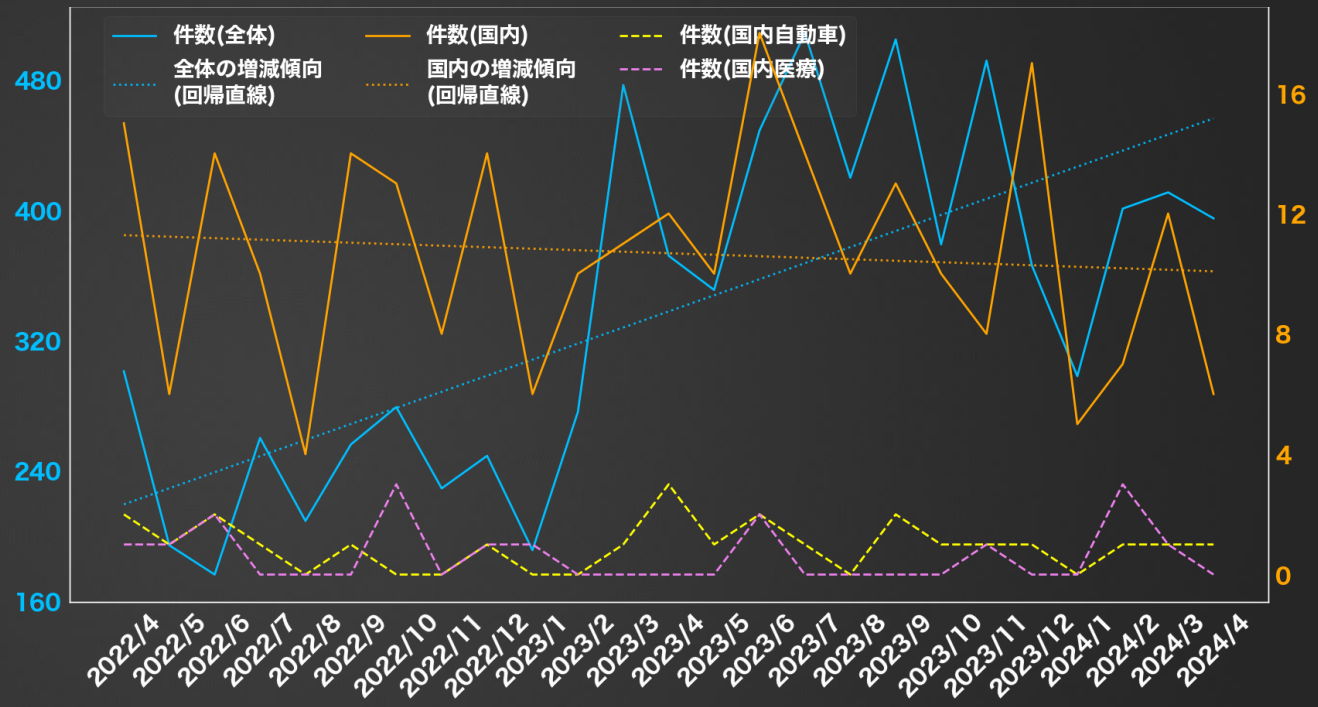
● 被害数の推移（2022年4月～2024年4月／全世界及び国内）(MBSD調べ)

※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)
2022/4	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	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	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	411	12	1	1
2024/4	395	6	1	0
合計	8445	267	24	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
4

※ 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

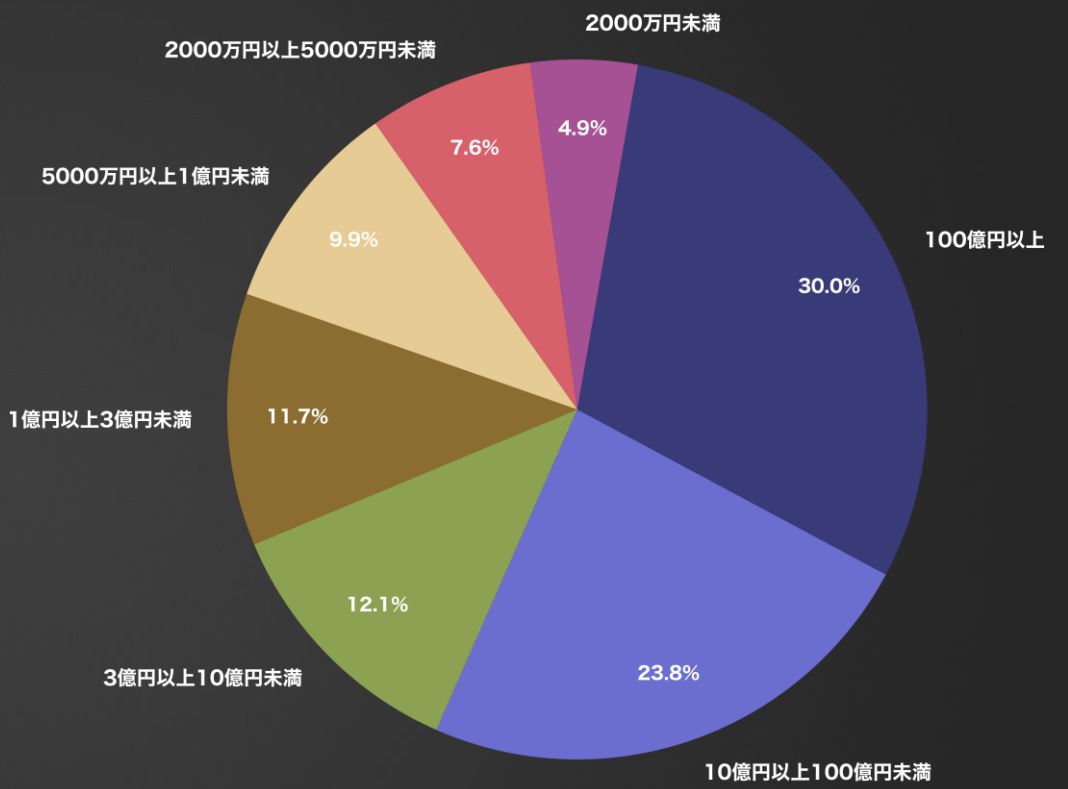
Know your enemy.
Defense leadership.

● 月別内訳 資本金別 （ 2022年4月～2024年4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	30.0
10億円以上100億円未満	53	23.8
3億円以上10億円未満	27	12.1
1億円以上3億円未満	26	11.7
5000万円以上1億円未満	22	9.9
2000万円以上5000万円未満	17	7.6
2000万円未満	11	4.9

▼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：34.1%
・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

4

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。

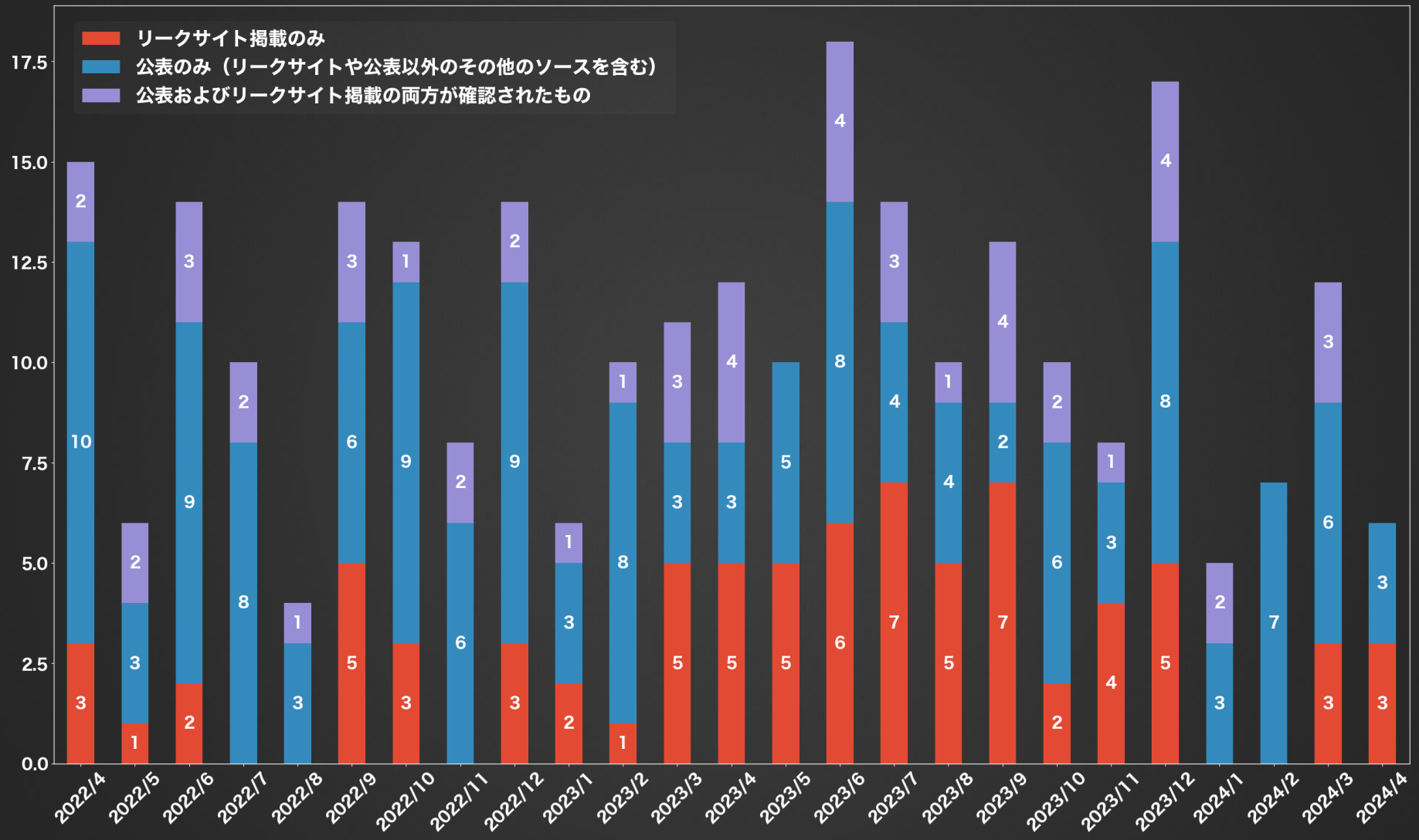
Created by Cyber Intelligence Group

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4月～2024年4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

4

※ 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4月～2024年4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
2023/4	(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
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

※ 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4月～2024年4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
2023/10	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
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

被害月	攻撃グループ	業種概要
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)	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	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

※ 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 － ⑱

Know your enemy.
Defense leadership.®

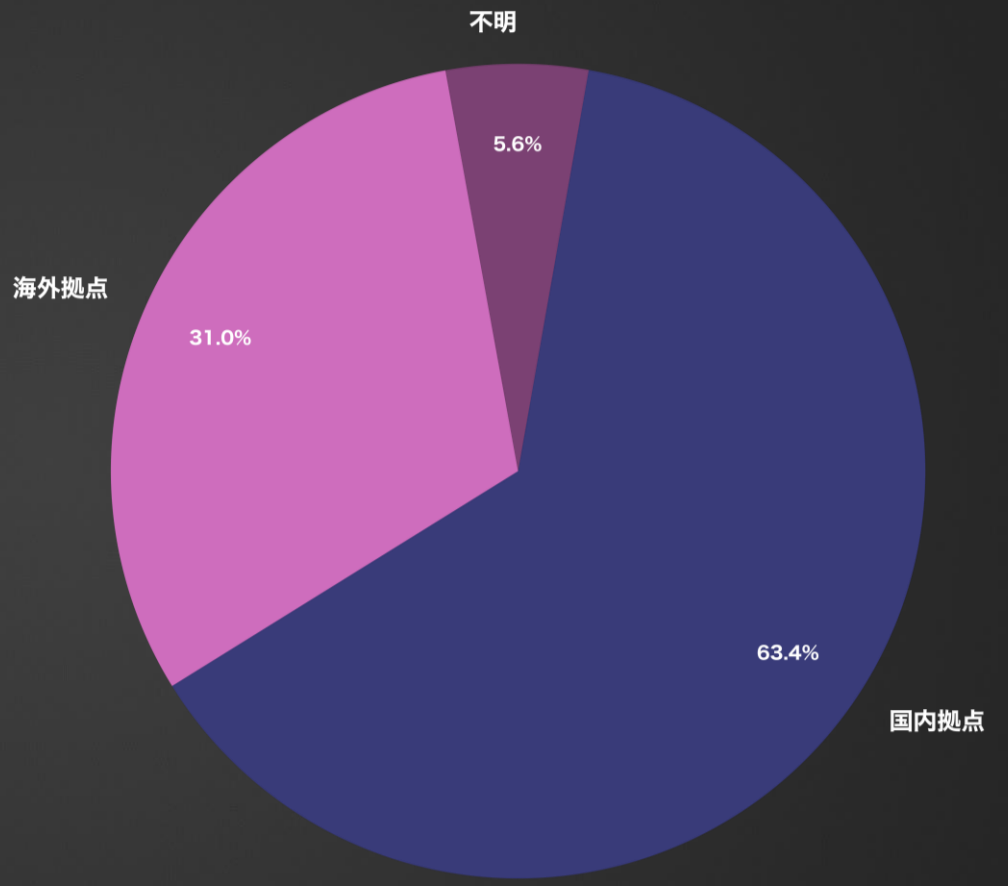
● 公となった国内被害組織における拠点割合（ 過去1年間／2023年4月～2024年4月）(MBSD調べ)

（※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	63.4
海外拠点	44	31.0
不明	8	5.6

▼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

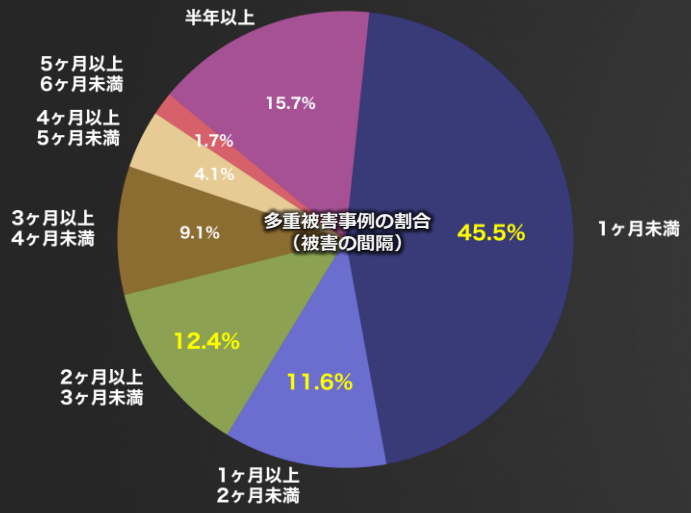
暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑲

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

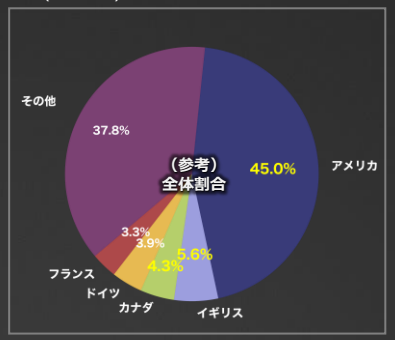
多重被害に遭った被害組織の傾向と分析 （MBSD調べ）
（過去2年間／2022年5月～2024年4月）

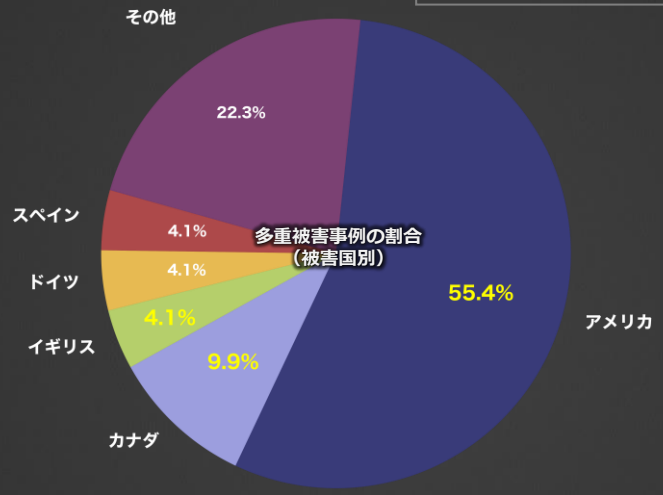
▼被害の間隔
（一度目の被害から二度目の被害までの間隔）



▼被害国別

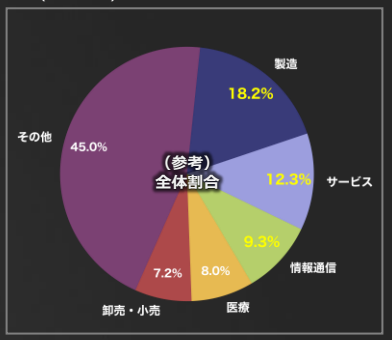
(参考比較) 同期間の全データにおける割合

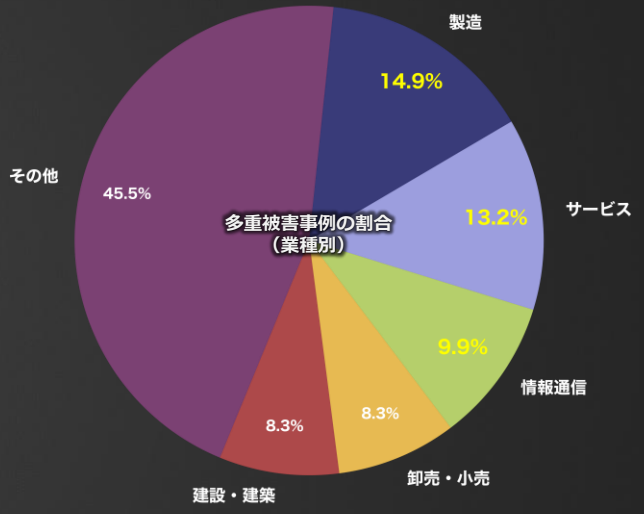




▼業種別

(参考比較) 同期間の全データにおける割合





▶多重被害に遭った組織数の累計：121件（全体8154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