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8月号 Rev 1.00
(2024年7月分)

2024
7

Created by Cyber Intelligence Group

目次

Know your enemy. Defense leadership.

総括と監視対象（レポート① ~ ③）

グローバル統計（レポート④ ~ ⑯）

日本関連組織を対象とした統計（レポート⑰ ~ ㉑）

多重被害に関する分析（レポート㉒ ~ ㉓）

その他

2024

7

総括と監視対象

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

今月のハイライト

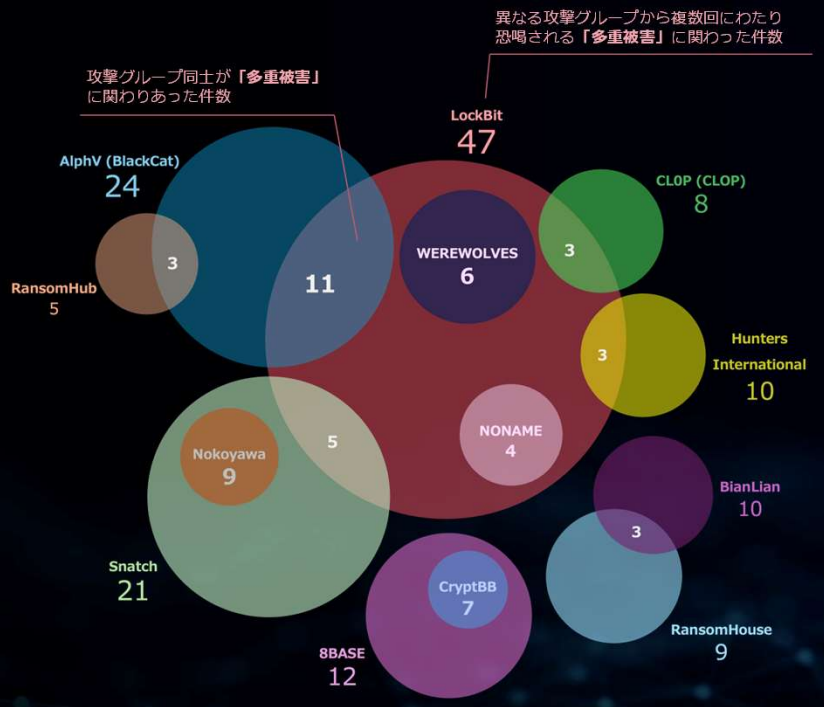
● 顕在化する攻撃グループ間の協力関係

2024年7月のリークサイト掲載は、RansomHubが同グループとして過去最多となった。この中にはAlphV (BlackCat)のリークサイトに掲載された日本関連組織も含まれていたが、今年前半には両グループが同じ海外の被害組織を掲載する事象が複数確認されており、これらの状況は両グループ間の繋がりを示唆している。

さらに、最近の攻撃グループ同士の関係性が疑われる事例として、LockBitがPLAYにツールとトレーニングを有償提供したとされる件(※1)も話題となった。
また別の事例として、2024年7月頃から活動が明るみとなった新興グループ「LYNX」の一部検体が、複数ベンダーの検知エンジンで「INC Ransom」として検出される状況を確認している。これは検体の一部が偶然類似した可能性などもある一方、2024年5月頃にINC Ransomのソースコードが販売された疑いもあり(※2)、LYNXの出現時期を鑑みると該当コードを流用した可能性も考えれなくはない。

我々の独自分析では、一度リークサイトに掲載されると、その後、異なる攻撃グループから繰り返し脅迫を受ける「多重被害」が複数発生している状況を確認（右図参照）。被害組織は単一の攻撃への対処だけでは根本的な解決に至らず、長期的な脅威に晒され続ける可能性がある。前述のランサムウェア攻撃グループ間の連携は、こうしたリスクを著しく高めることにも繋がるといえ、現状況を踏まえると、組織は継続的な被害も想定した事前対策を包括的に講じる必要があるだろう。

(※1) https://dailydarkweb.net/play-ransomware-and-lockbit-allegedly-created-an-alliance/
(※2) https://www.bleepingcomputer.com/news/security/inc-ransomware-source-code-selling-on-hacking-forums-for-300-000/



異なる攻撃グループによって発生した多重被害の状況
(2022年8月～2024年7月：多重被害に遭った被害組織合計131件のうち
「3件以上重なりがあるケース」を抜粋)

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

監視中のランサムウェア攻撃グループ情報（拠点数と一覧）

Know your enemy. Defense leadership.

● 当月監視対象の攻撃グループ数（※1）：191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：47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
- Brain Cipher
- BULLY
- CACTUS
- CHEERS
- ChileLocker (Arcrypter)
- Cicada3301
- CiphBit
- CipherLocker
- CL0P (CLOP)
- Cloak
- Conti
- Cooming Project
- CROSSLOCK
- CryptBB
- CRYPTNET
- CryptOn
- Cuba
- Cyclops
- DAGON
- DAIXIN
- dAn0n (danon)
- Dark Angels
- DARKBIT
- DARKPOWER
- DarkRace
- DarkRypt
- Darkside
- Dark Vault
- Dispossessor[Databroker]
- Donex
- Donut Leaks
- DoppelPaymer
- dotAdmin
- DragonForce
- DUNGHILL
- eCh0raix (eChoraix)
- El_Cometa
- EL DORADO
- EMBARGO
- Endurance
- Entropy
- Everest
- ● FOG
- FSOCIETY / FLOCKER
- FSTeam
- Grief
- Groove
- HANDARA [Hacktivist]
- Haron
- HelloGookie
- Hitler (AGL0BGVYCG)
- Hive
- HolyGhost
- Hotarus
- Hunters International
- ICEFIRE
- INC Ransom
- Insane
- Karakurt
- Karma
- KILLSEC
- Knight
- LAMBDA
- La Piovra
- LAPSUS$
- LILITH
- LockBit
- Lorenz
- LostTrust
- LV
- ● LYNX
- MADCAT
- ● MAD LIBERATOR
- 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 (VFOKX)
- NONAME [2023年確認]
- ● NULLBULGE
- Onyx
- Pandora
- Pay2Key
- Payload.bin
- PLAY
- Prometheus
- ● PRYX
- PUTIN TEAM
- Pysa / Mespinoza
- Qilin (Agenda)
- QIULONG
- Quantum
- RABBIT HOLE
- Ragnar Locker
- Ragnarok
- RA GROUP
- Rancoz
- Ransom Cartel
- Ransom Corp
- ● RANSOMCORTEX
- Ransomed.vc
- Ransom EXX
- RansomHouse
- RansomHub
- Ransomware Blog
- Ranzy
- RA WORLD
- Raznatovic
- RedAlert (N13V)
- Red Ransomware Group (Red CryptoApp)
- Relic
- Revil (Sodinokibi)
- Rhysida
- Risen
- ROOK
- Royal
- Rransom
- Sabbath (54bb47h)
- SenSayQ
- shaoleaks
- SIEGEDSEC
- SLUG
- Snatch
- Solidbit
- Space Bears
- Sparta
- Spook
- STORMOUS
- Sugar
- Suncrypt
- SynACK
- ThreeAM (3AM)
- TRIGONA
- TRINITY
- TRISEC
- Underground
- UnSafe
- ● VanirGroup
- Vice Society
- V IS VENDETTA
- VSOP
- WEREWOLVES
- x001xs
- XING Team
- Yanluowang
- Zeon
- Zero Tolerance

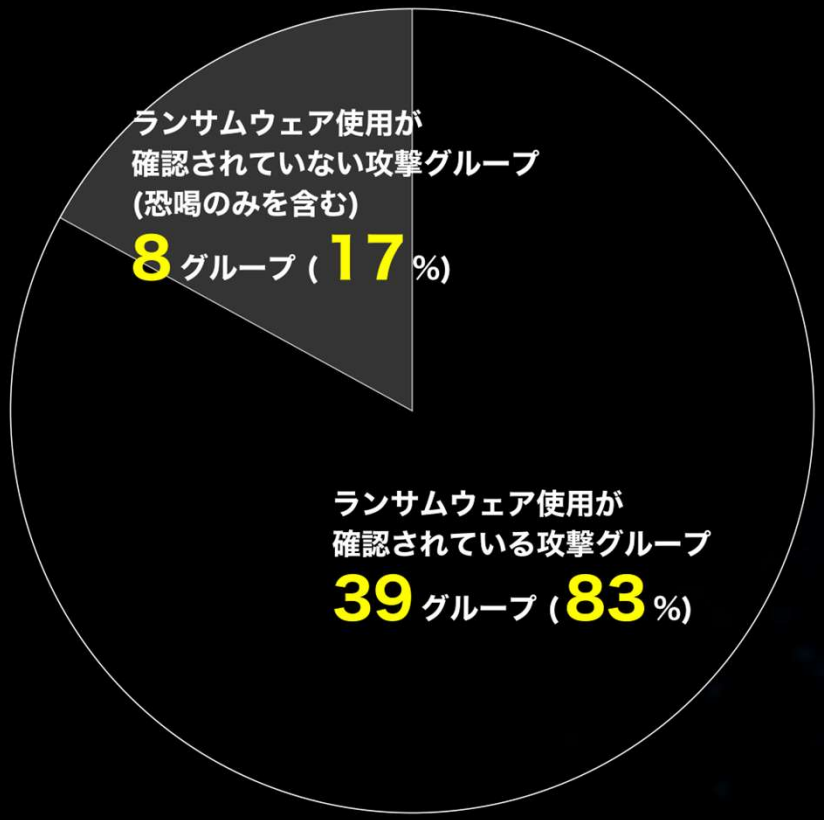
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

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7月）

（※2024年7月にリークサイト掲載を確認した攻撃グループ全47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や、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7月に活動中である事が確認された全47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。

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

2024

7

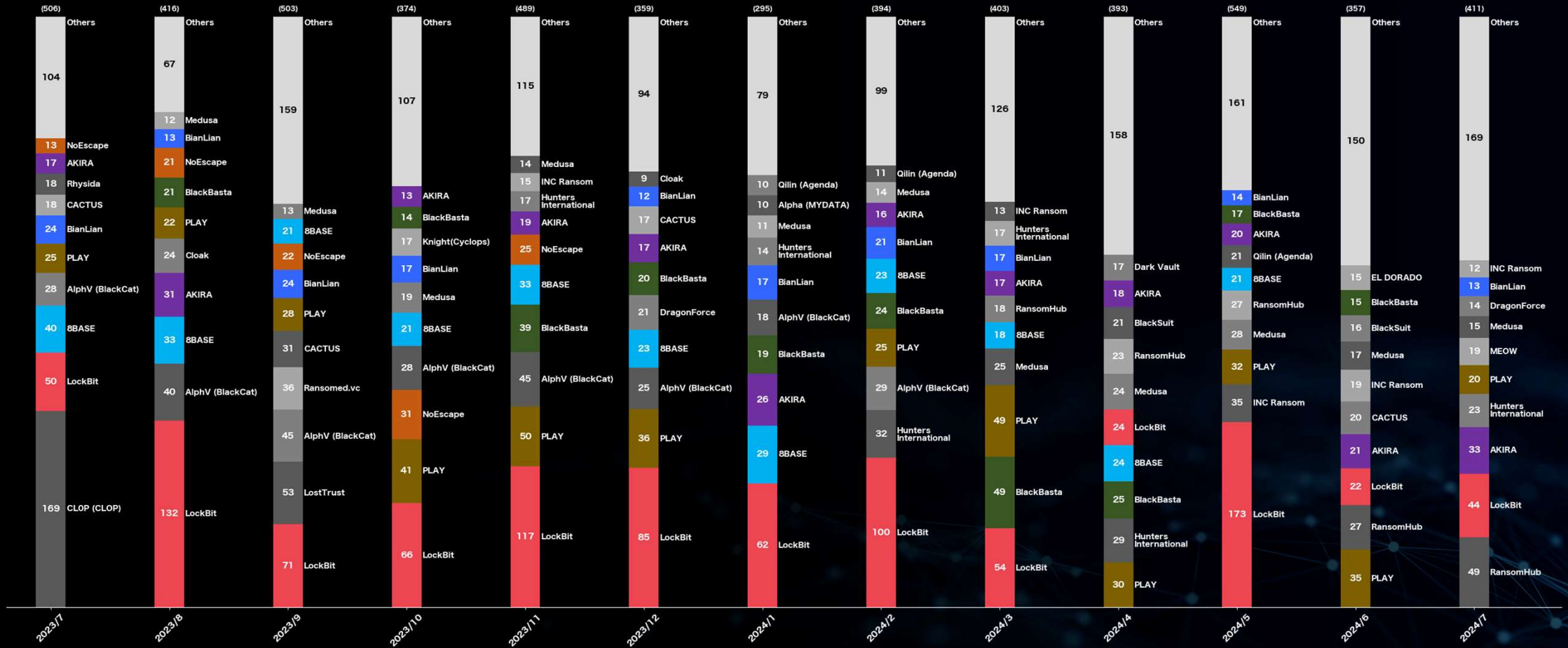
年間 統計

（全世界）

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

攻撃グループ割合で見る被害数の年間統計

(2023年7月～2024年7月／全世界) (MBSD調べ)



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

攻撃グループ 月別統計

（全世界）

（過去3ヶ月分）

2024

7

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

月別内訳 攻撃グループ TOP10

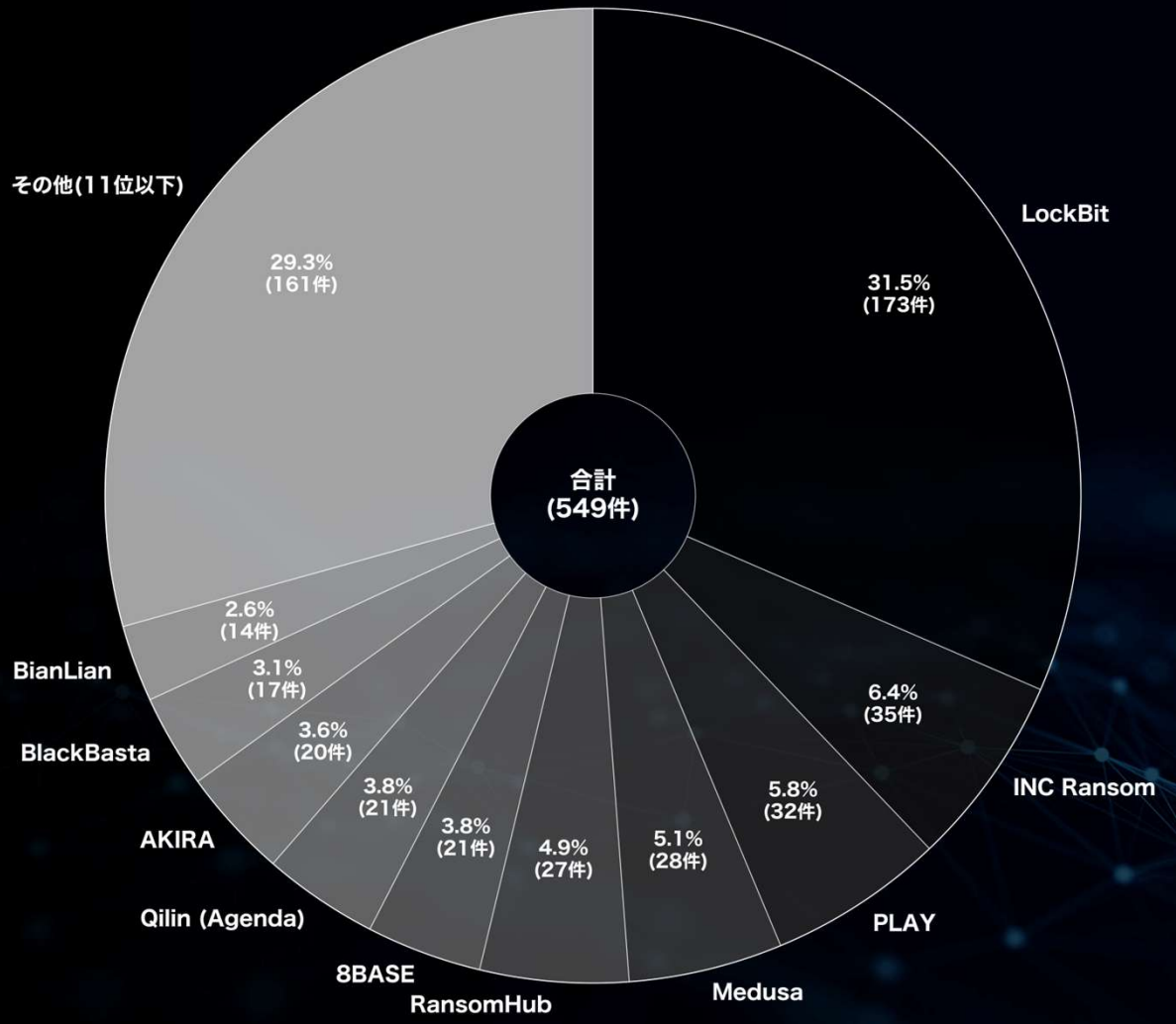
(2024年 5 月／全世界) (MBSD調べ)

Know your enemy. Defense leadership.

※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）



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

月別内訳 攻撃グループ TOP10

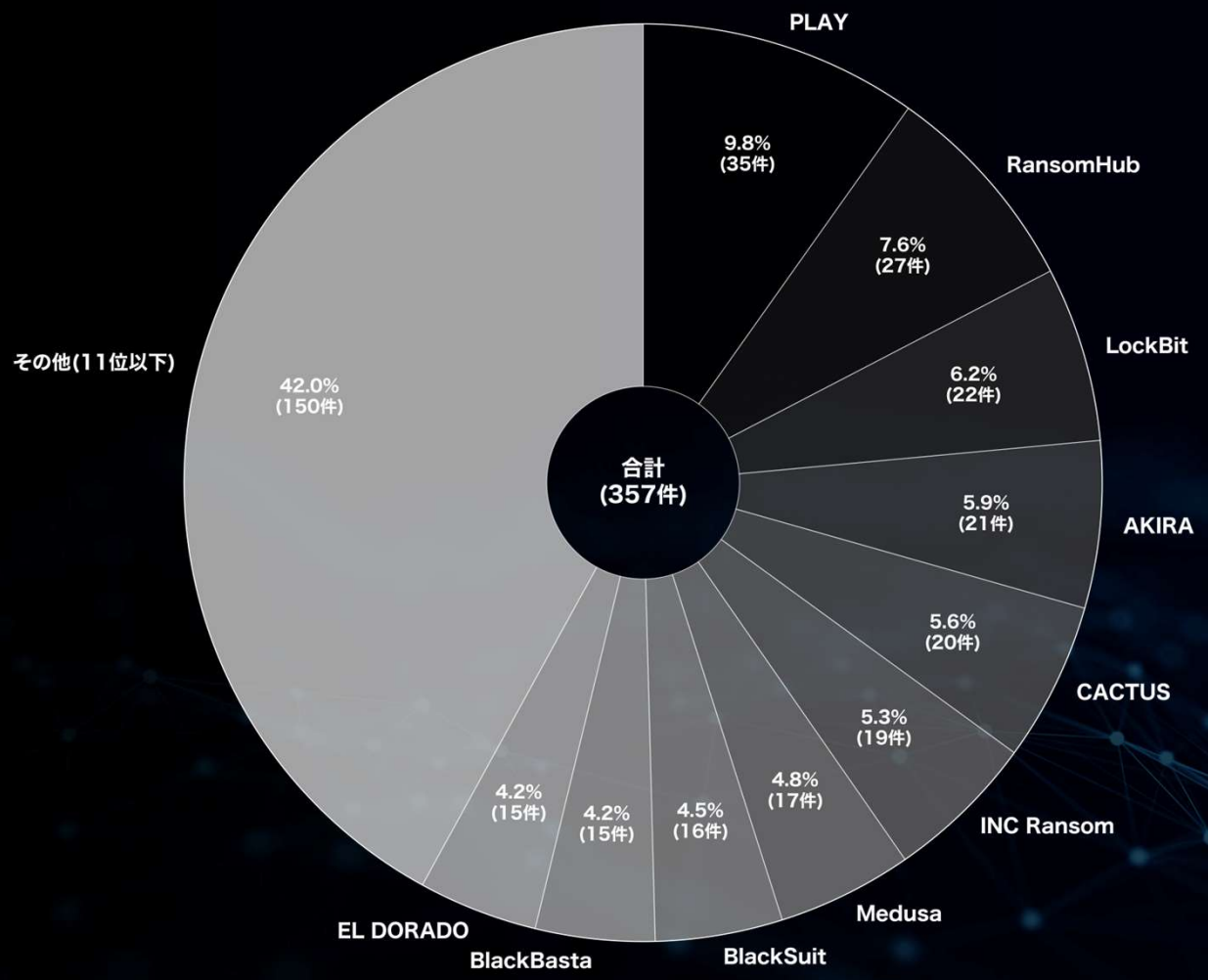
(2024年 6 月／全世界) (MBSD調べ)

Know your enemy. Defense leadership.

※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	35	9.8	+ 3
RansomHub	27	7.6	± 0
LockBit	22	6.2	- 151
AKIRA	21	5.9	+ 1
CACTUS	20	5.6	+ 15
INC Ransom	19	5.3	- 16
Medusa	17	4.8	- 11
BlackSuit	16	4.5	+ 2
BlackBasta	15	4.2	- 2
EL DORADO	15	4.2	+ 15

▼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）



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

月別内訳 攻撃グループ TOP10

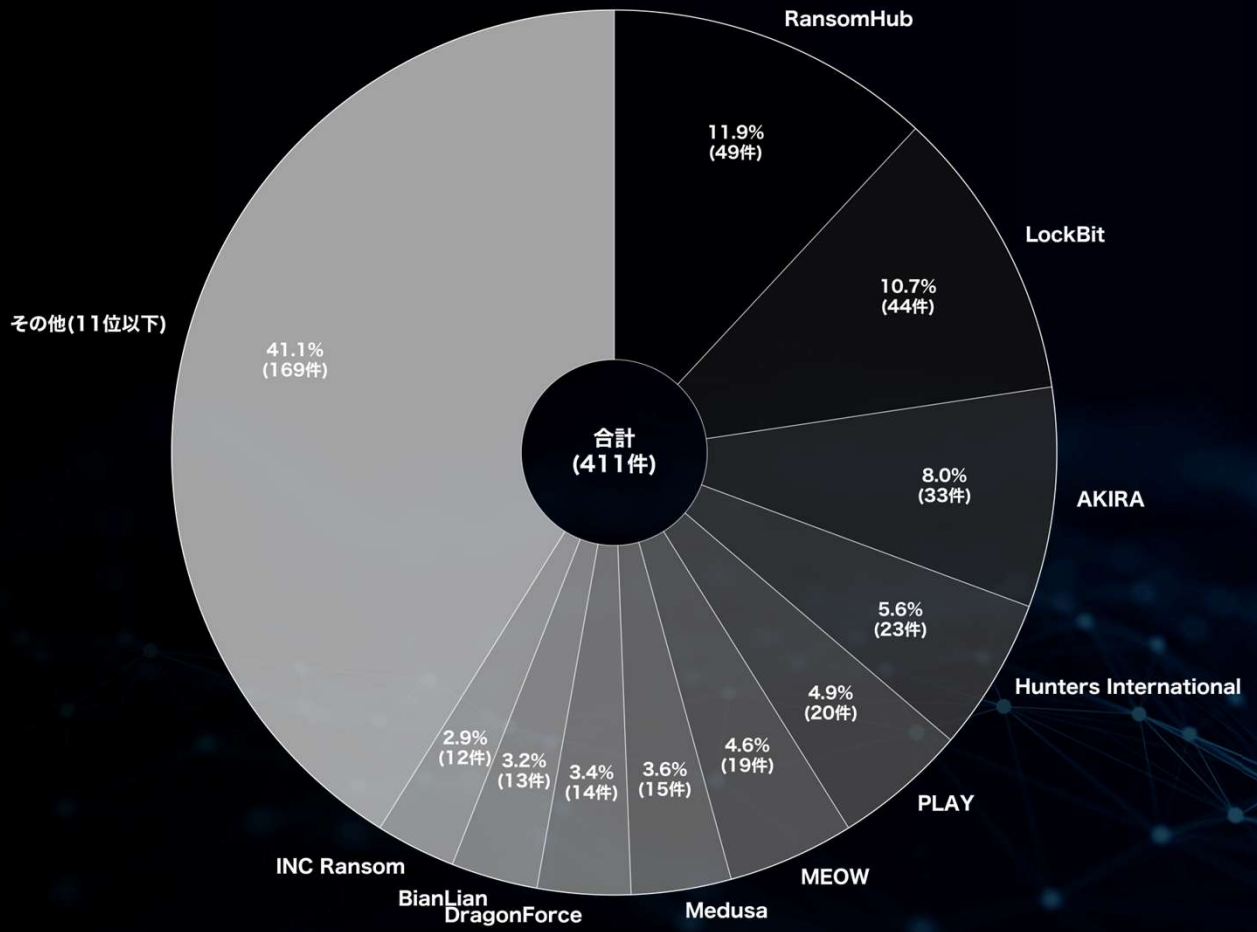
(2024年 7 月／全世界) (MBSD調べ)

Know your enemy. Defense leadership.

※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)
RansomHub	49	11.9	+ 22
LockBit	44	10.7	+ 22
AKIRA	33	8.0	+ 12
Hunters International	23	5.6	+ 15
PLAY	20	4.9	- 15
MEOW	19	4.6	+ 17
Medusa	15	3.6	- 2
DragonForce	14	3.4	+ 6
BianLian	13	3.2	+ 4
INC Ransom	12	2.9	- 7

▼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）



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

被害国 月別統計
（全世界） （過去3ヶ月分）

2024
7

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

月別内訳 被害国TOP10

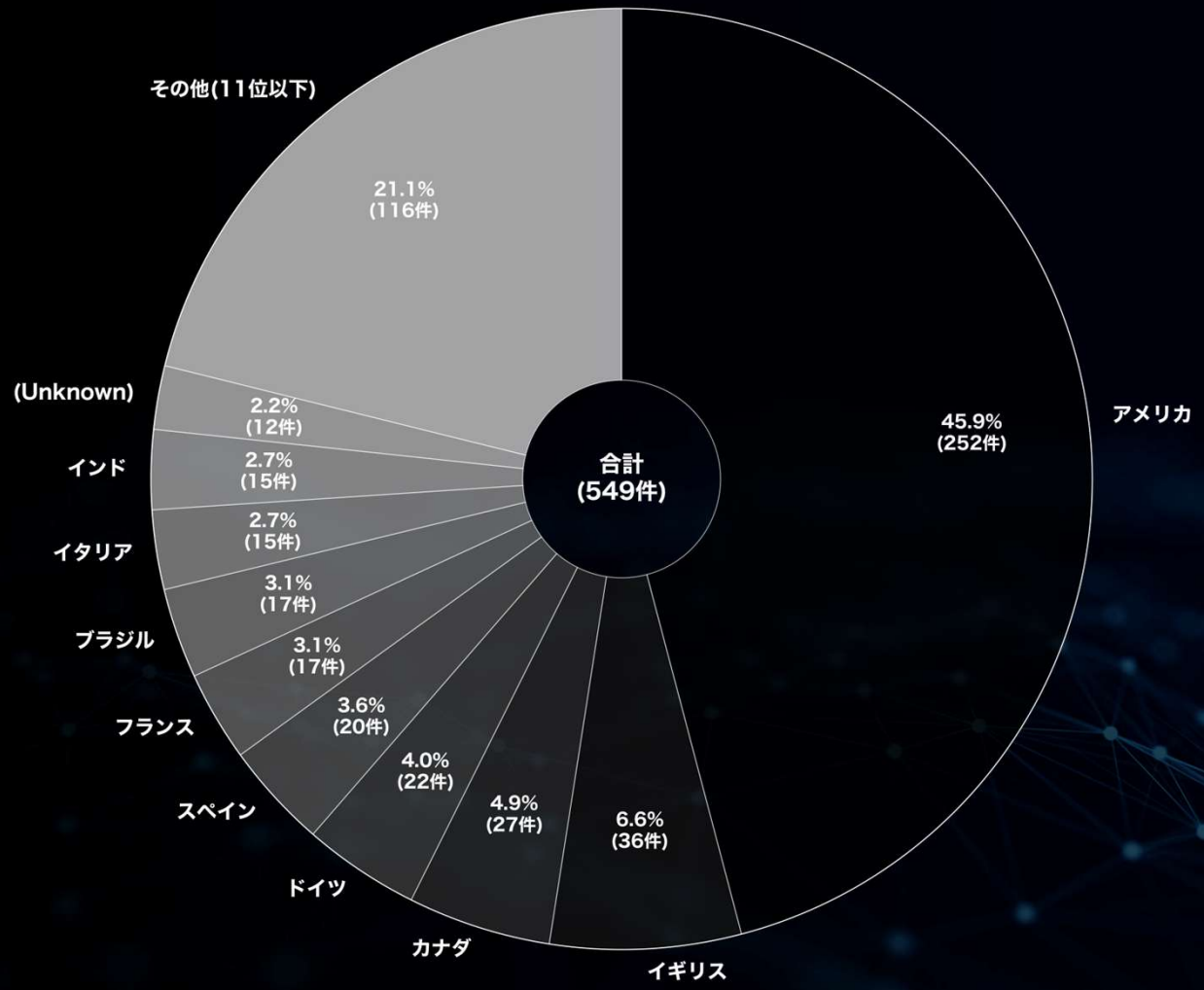
(2024年 5 月／全世界) (MBSD調べ)

Know your enemy. Defense leadership.

※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）



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

月別内訳 被害国TOP10

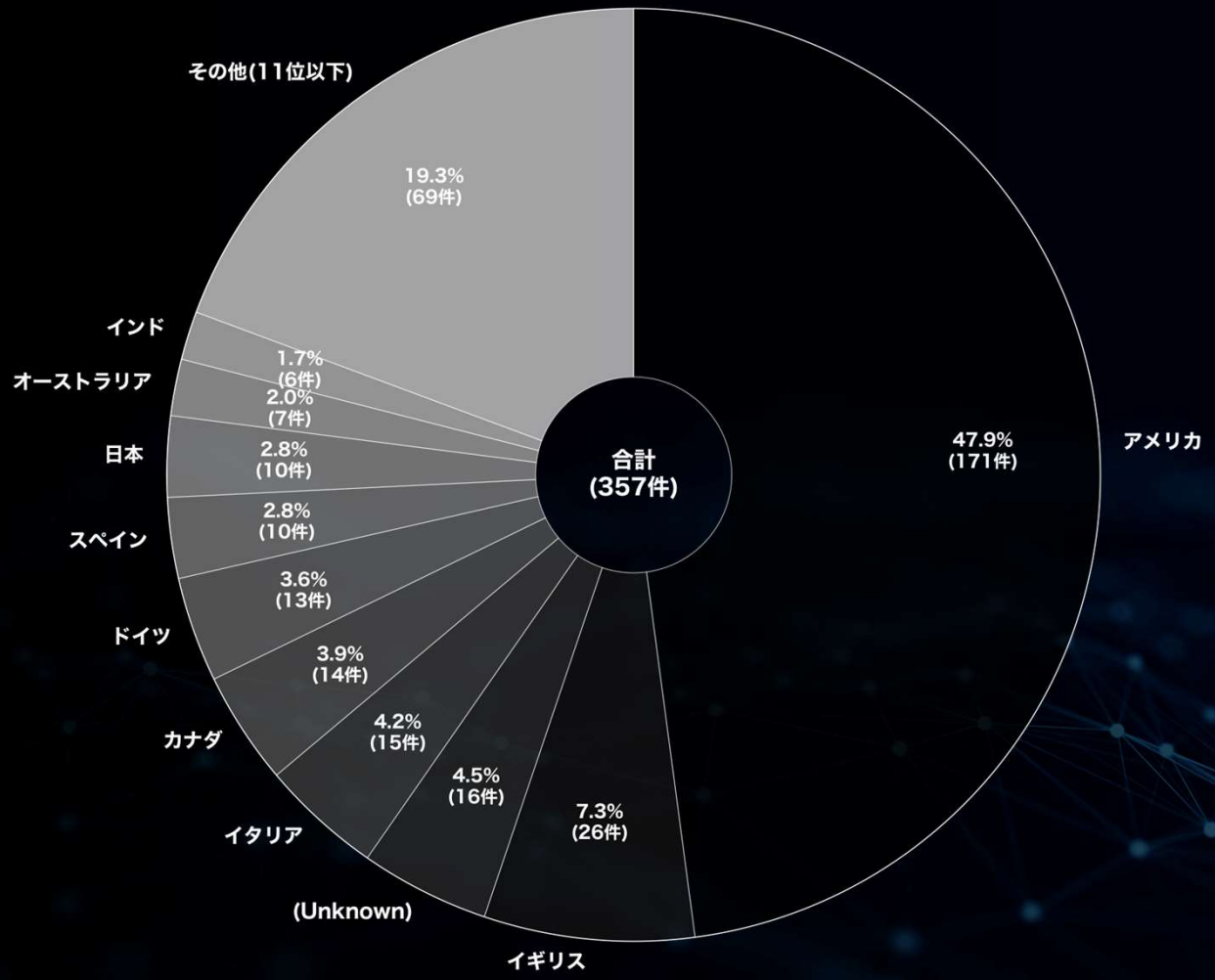
(2024年 6 月／全世界) (MBSD調べ)

Know your enemy. Defense leadership.

※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	171	47.9	- 81
イギリス	26	7.3	- 10
(Unknown)	16	4.5	+ 4
イタリア	15	4.2	± 0
カナダ	14	3.9	- 13
ドイツ	13	3.6	- 9
スペイン	10	2.8	- 10
日本	10	2.8	± 0
オーストラリア	7	2.0	+ 5
インド	6	1.7	- 9

▼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）



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

月別内訳 被害国TOP10

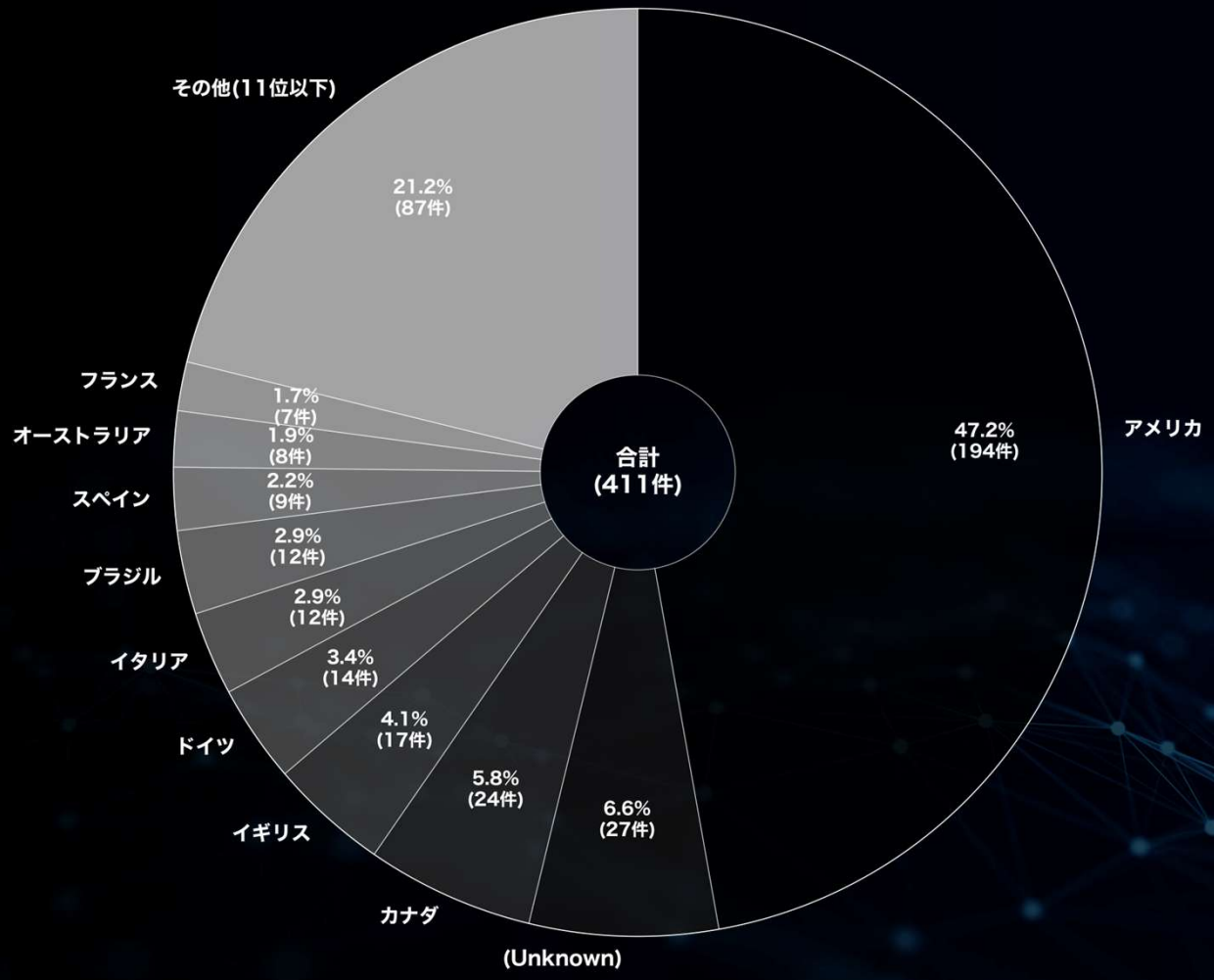
(2024年 7 月／全世界) (MBSD調べ)

Know your enemy. Defense leadership.

※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	47.2	+ 23
(Unknown)	27	6.6	+ 11
カナダ	24	5.8	+ 10
イギリス	17	4.1	- 9
ドイツ	14	3.4	+ 1
イタリア	12	2.9	- 3
ブラジル	12	2.9	+ 6
スペイン	9	2.2	- 1
オーストラリア	8	1.9	+ 1
フランス	7	1.7	+ 3

▼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）



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

2024

7

被害国 月別統計

（アジア） （過去3ヶ月分）

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

月別内訳 被害国TOP10

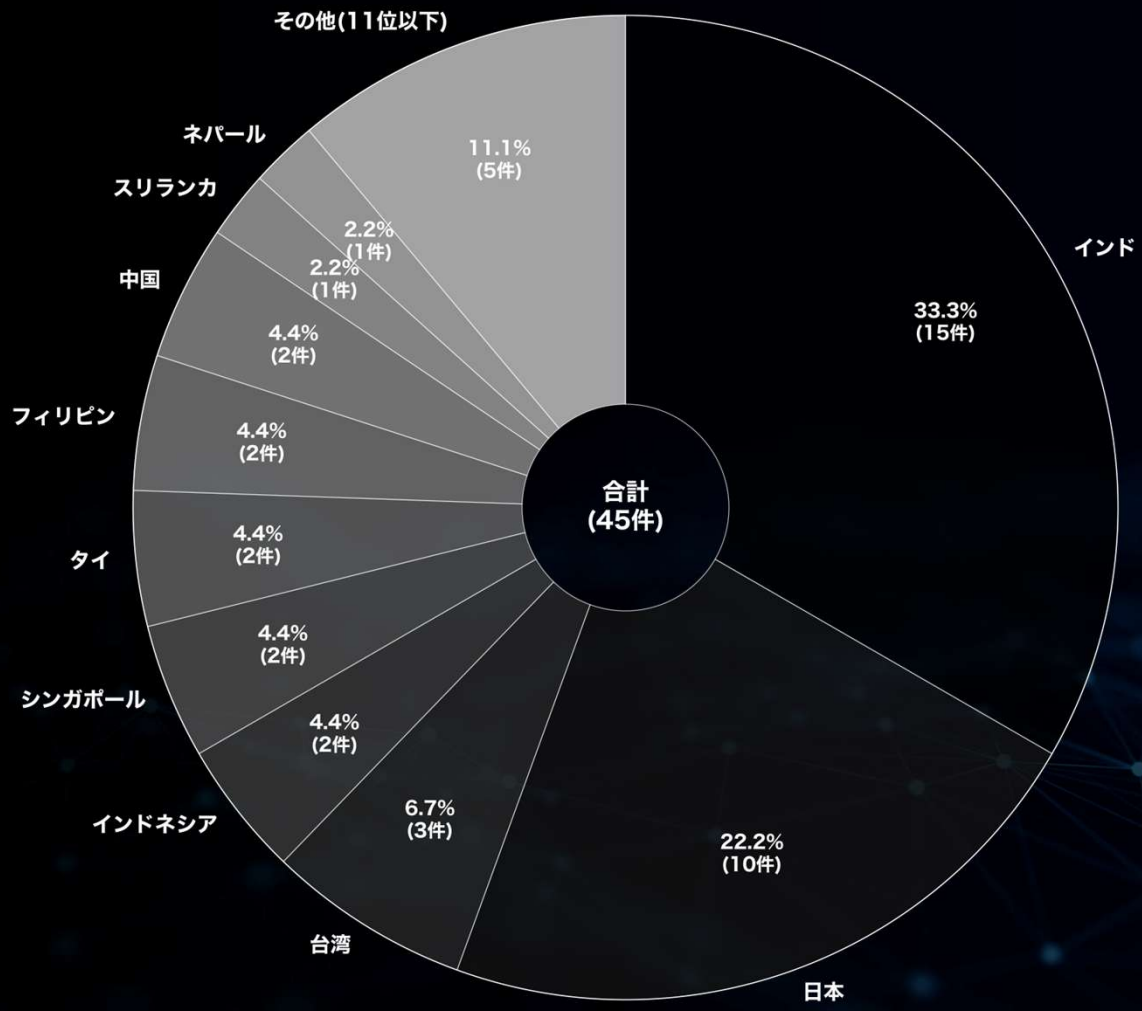
(2024年 5 月／アジア) (MBSD調べ)

Know your enemy. Defense leadership.

※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）



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

月別内訳 被害国TOP10

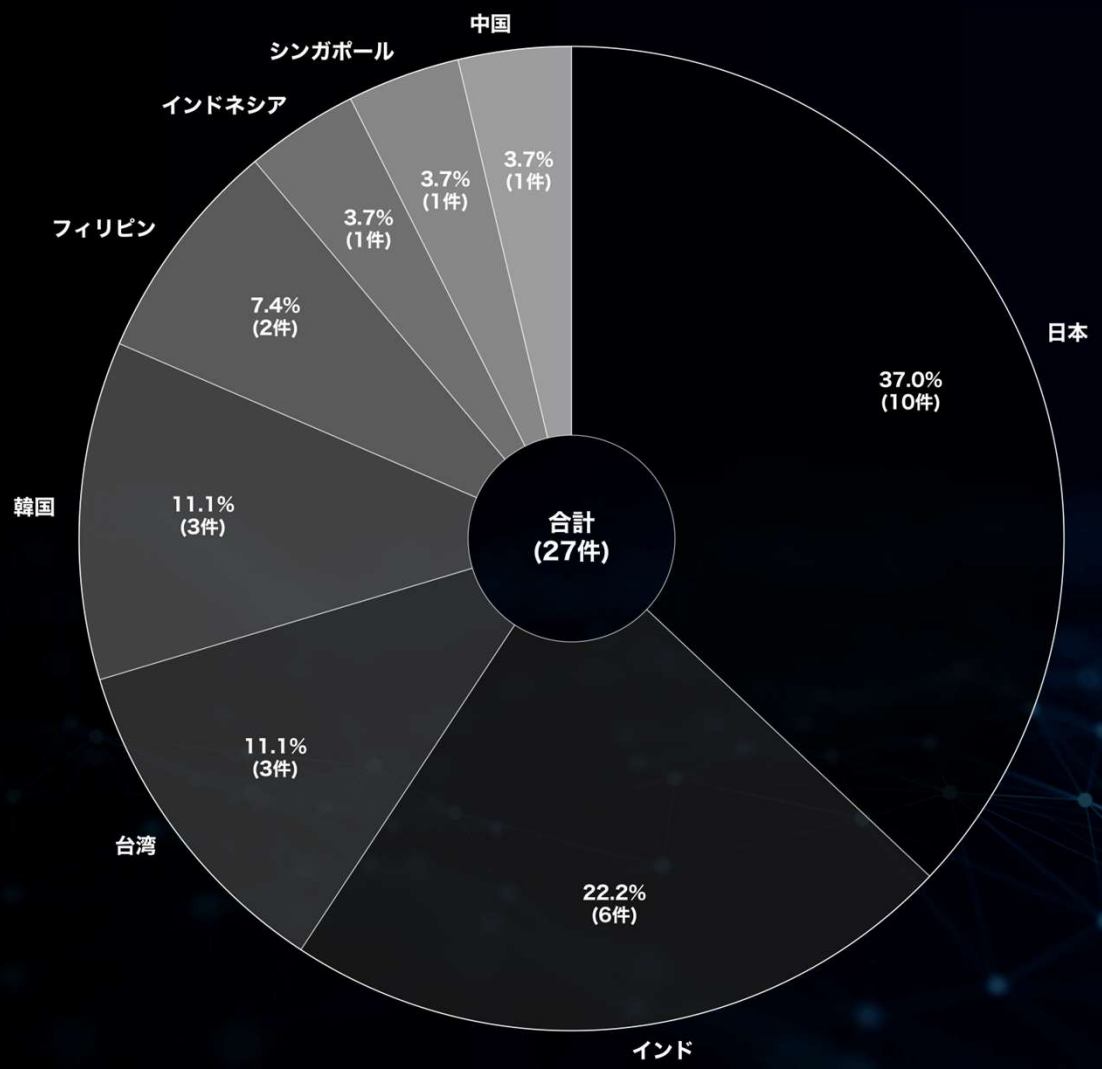
(2024年 6 月／アジア) (MBSD調べ)

Know your enemy. Defense leadership.

※件数順に降順／同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
日本	10	37.0	± 0
インド	6	22.2	- 9
台湾	3	11.1	± 0
韓国	3	11.1	+ 2
フィリピン	2	7.4	± 0
インドネシア	1	3.7	- 1
シンガポール	1	3.7	- 1
中国	1	3.7	- 1

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



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

月別内訳 被害国TOP10

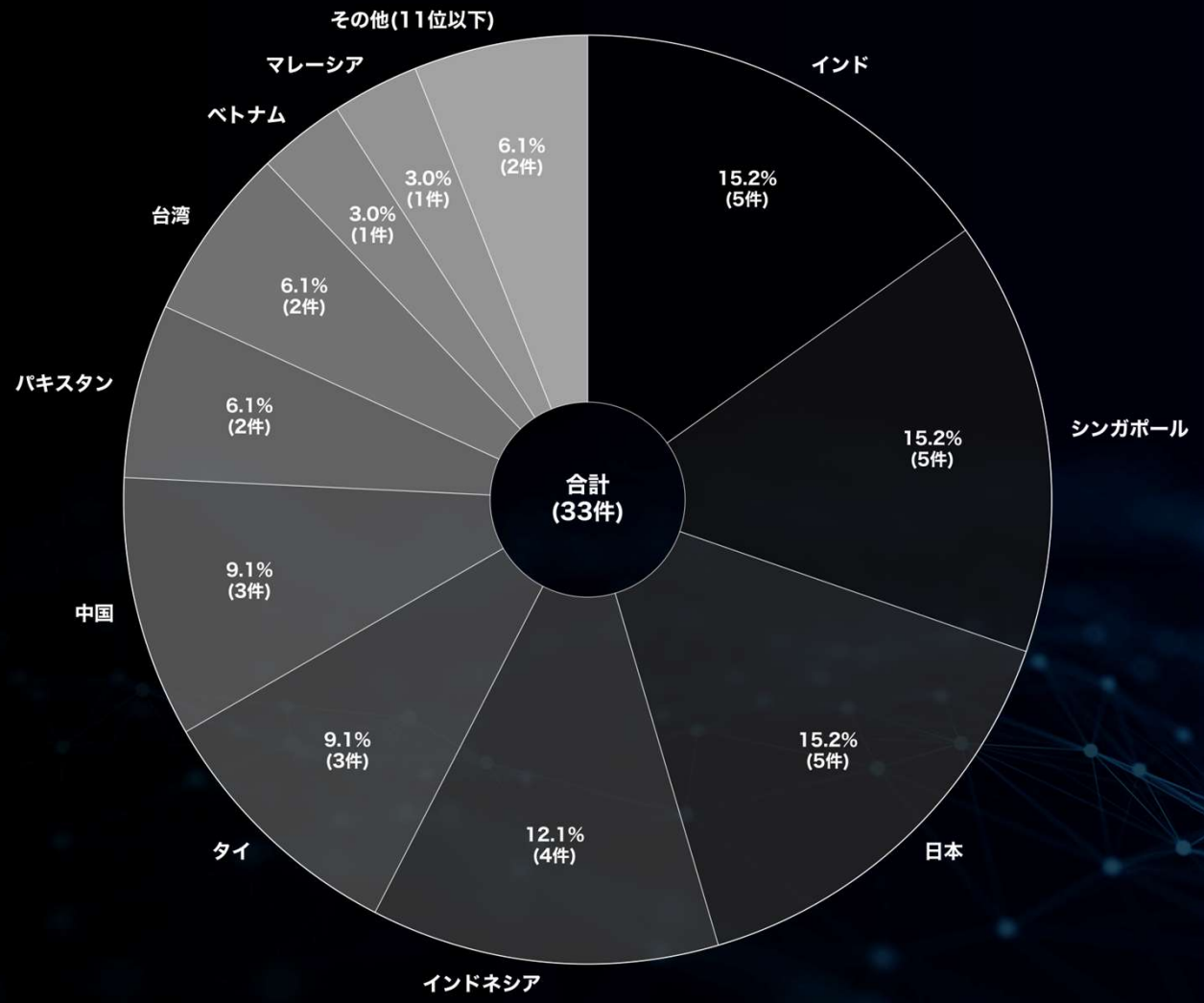
(2024年 7 月／アジア) (MBSD調べ)

Know your enemy. Defense leadership.

※件数順に降順／同件数のものが含まれる場合は名前順でTOP10までを記載

国名	件数	割合(%)	前月比(件数)
インド	5	15.2	- 1
シンガポール	5	15.2	+ 4
日本	5	15.2	- 5
インドネシア	4	12.1	+ 3
タイ	3	9.1	+ 3
中国	3	9.1	+ 2
パキスタン	2	6.1	+ 2
台湾	2	6.1	- 1
ベトナム	1	3.0	+ 1
マレーシア	1	3.0	+ 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）



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

2024

7

業種 月別統計

（全世界） （過去3ヶ月分）

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

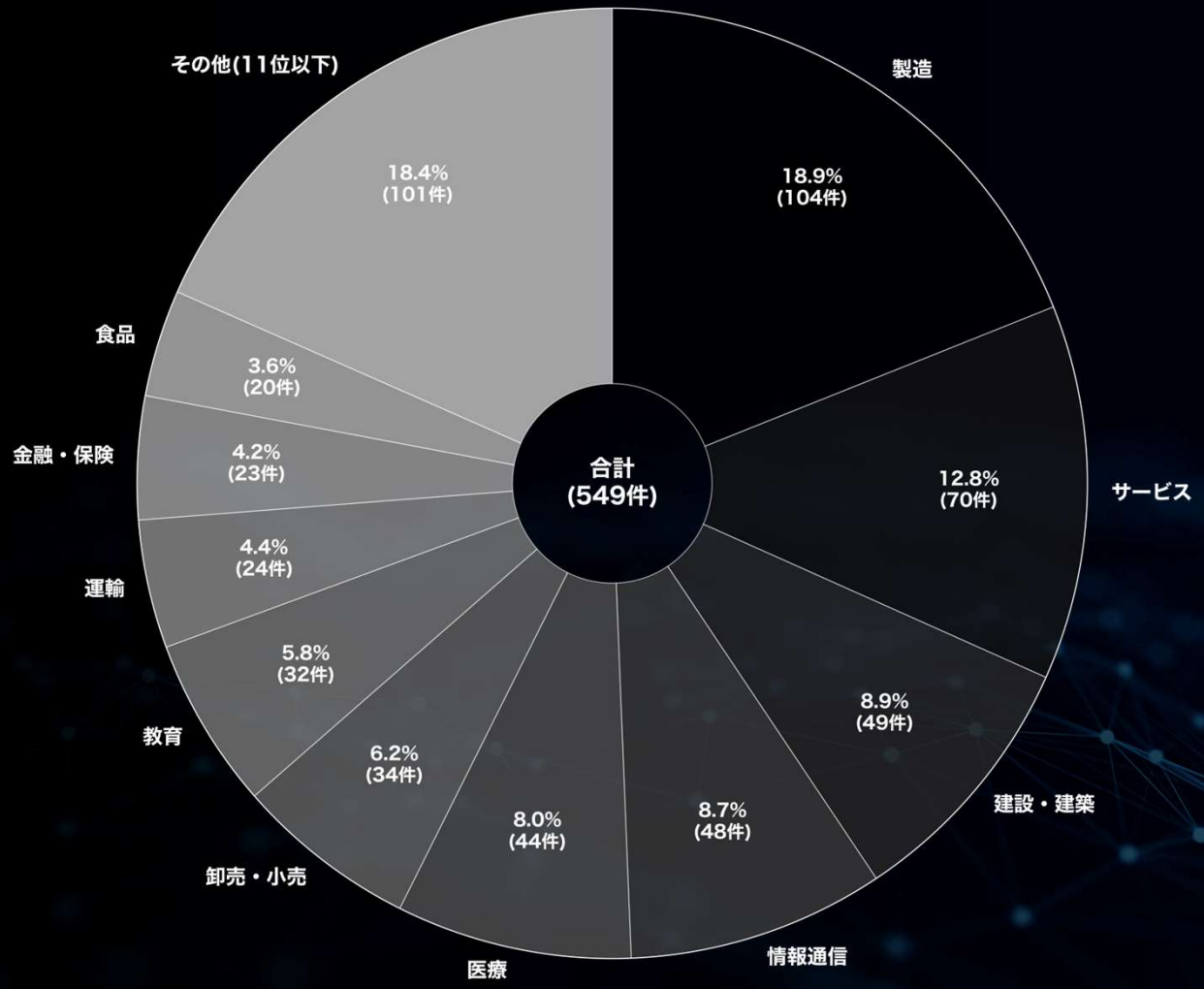
月別内訳 業種 TOP10

(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）



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

月別内訳 業種 TOP10

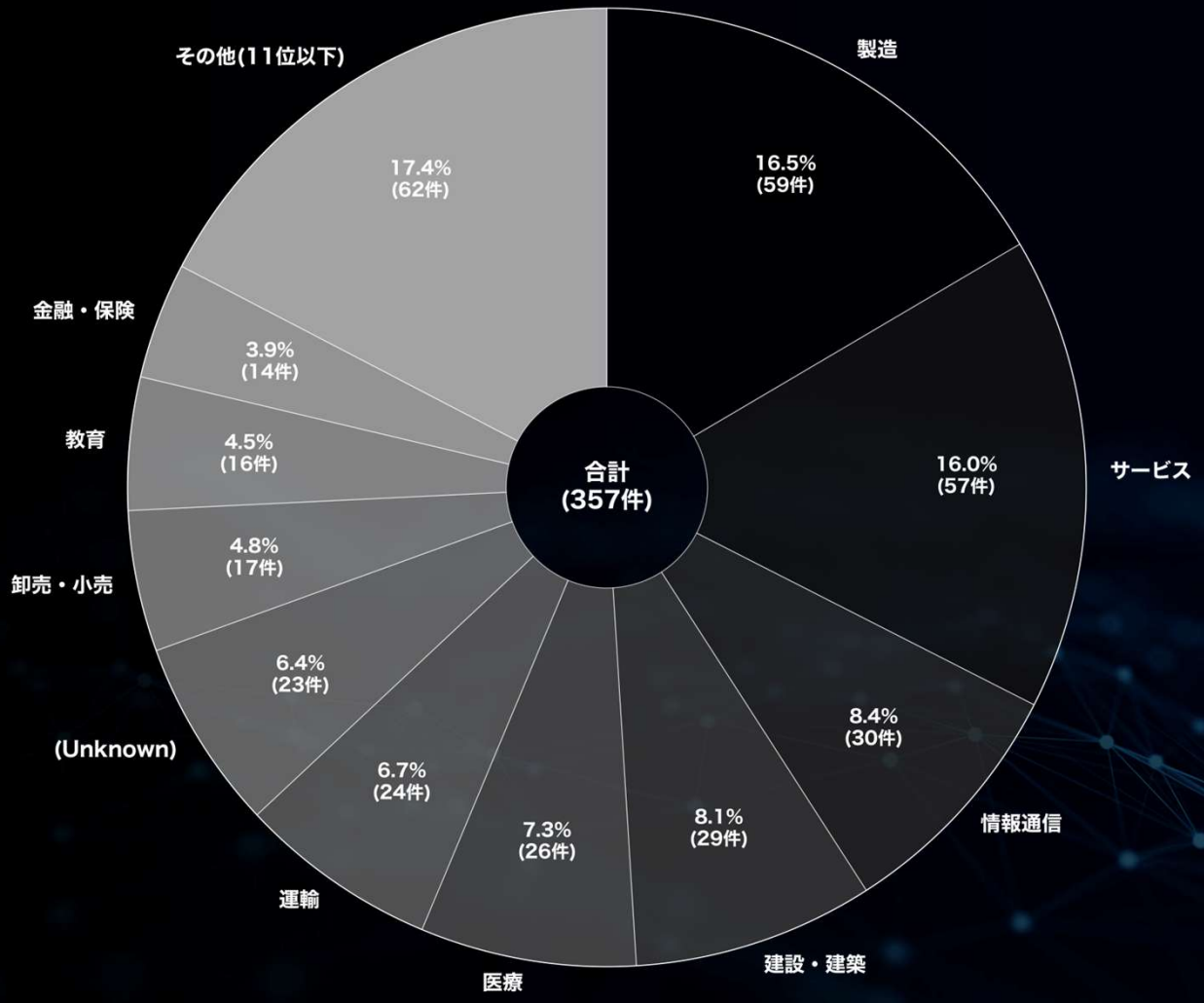
(2024年 6 月／全世界) (MBSD調べ)

Know your enemy. Defense leadership.®

※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	59	16.5	- 45
サービス	57	16.0	- 13
情報通信	30	8.4	- 18
建設・建築	29	8.1	- 20
医療	26	7.3	- 18
運輸	24	6.7	± 0
(Unknown)	23	6.4	+ 12
卸売・小売	17	4.8	- 17
教育	16	4.5	- 16
金融・保険	14	3.9	- 9

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



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

月別内訳 業種 TOP10

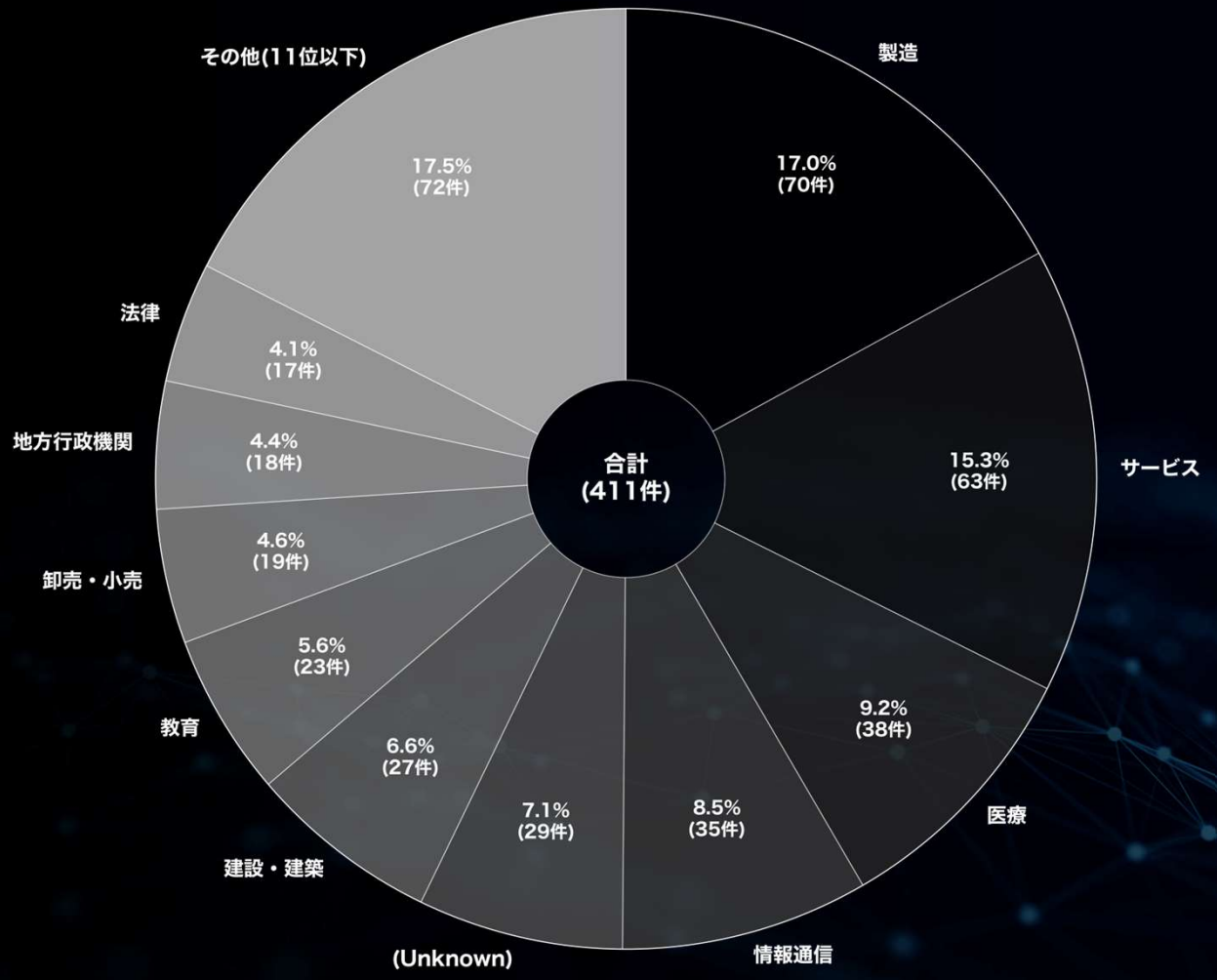
(2024年 7 月／全世界) (MBSD調べ)

Know your enemy. Defense leadership.

※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	70	17.0	+ 11
サービス	63	15.3	+ 6
医療	38	9.2	+ 12
情報通信	35	8.5	+ 5
(Unknown)	29	7.1	+ 6
建設・建築	27	6.6	- 2
教育	23	5.6	+ 7
卸売・小売	19	4.6	+ 2
地方行政機関	18	4.4	+ 9
法律	17	4.1	+ 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）



※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

被害数の推移に関する統計
（全世界及び国内）

2024
7

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

被害数の推移

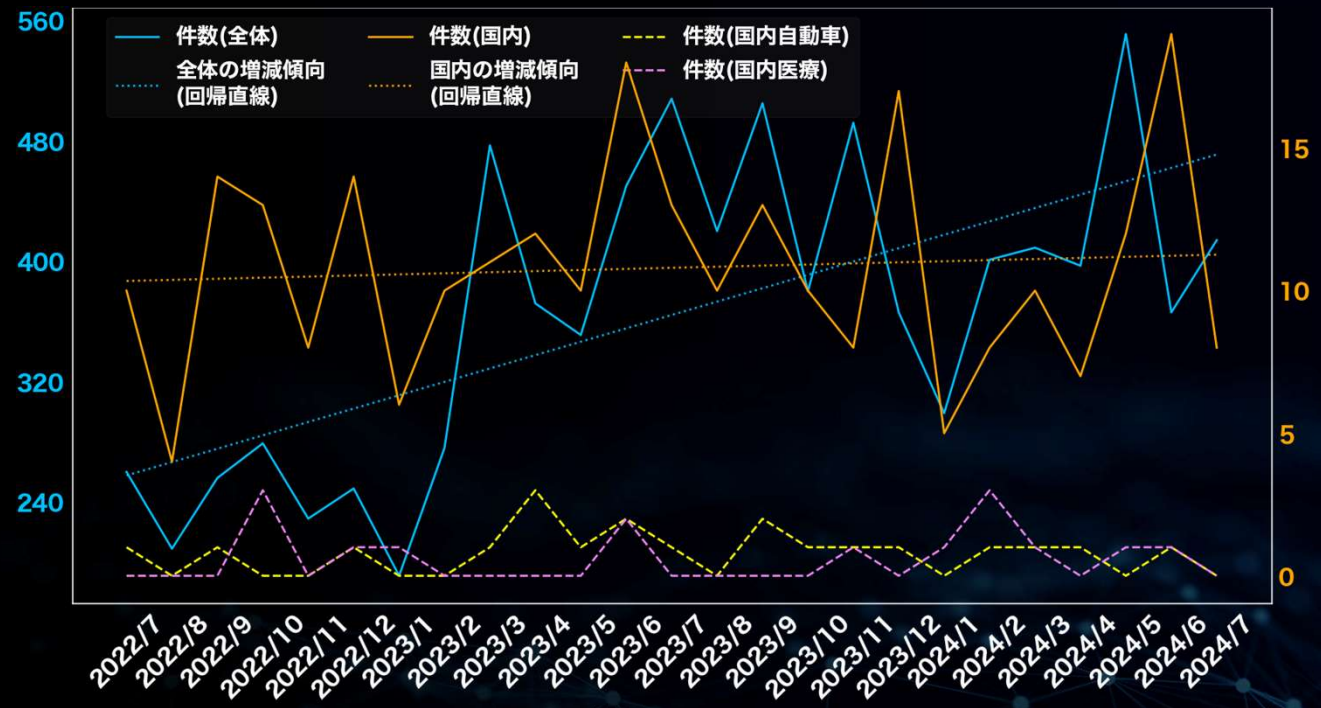
（2022年7月～2024年7月／全世界及び国内）(MBSD調べ)

※件数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)
2022/7	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	450	18	2	2
2023/7	508	13	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	299	5	0	1
2024/2	401	8	1	3
2024/3	409	10	1	1
2024/4	397	7	1	0
2024/5	551	12	0	1
2024/6	366	19	1	1
2024/7	414	8	0	0
合計	9107	270	20	15

▼過去2年間におけるランサムウェア全体の活動推移（全リークサイトの掲載総数の推移）

※全体統計に併せ、よく注目されがちな国内の２業種をピックアップして掲載している。



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

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

資本金別 月別統計
（国内）

2024
7

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

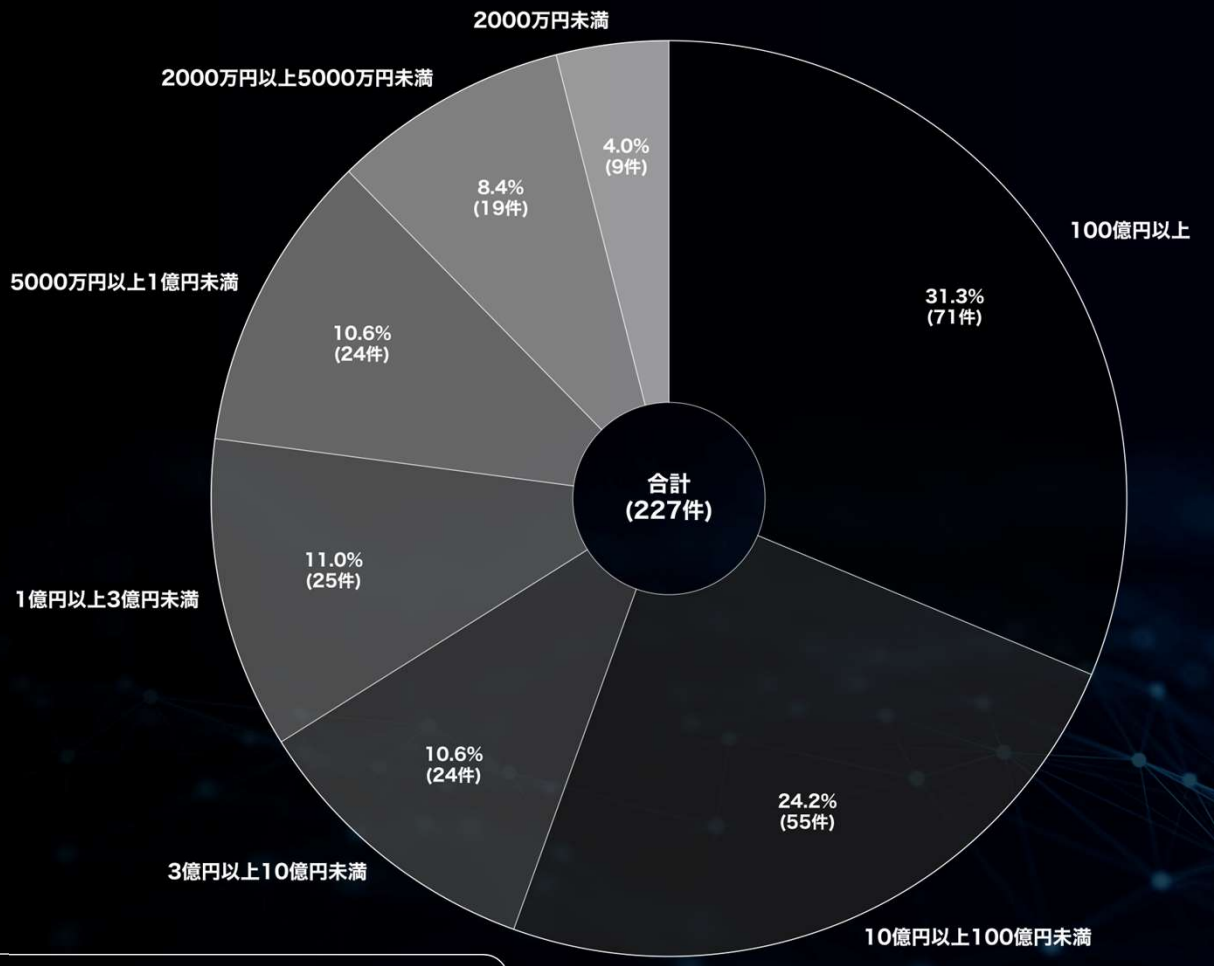
月別内訳 資本金別

(2022年7月～2024年7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	71	31.3
10億円以上100億円未満	55	24.2
3億円以上10億円未満	24	10.6
1億円以上3億円未満	25	11.0
5000万円以上1億円未満	24	10.6
2000万円以上5000万円未満	19	8.4
2000万円未満	9	4.0

▼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：34.0%
・10億円未満が該当するとした場合：44.6%

（※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）

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

公表と暴露に関する統計
（国内）

2024
7

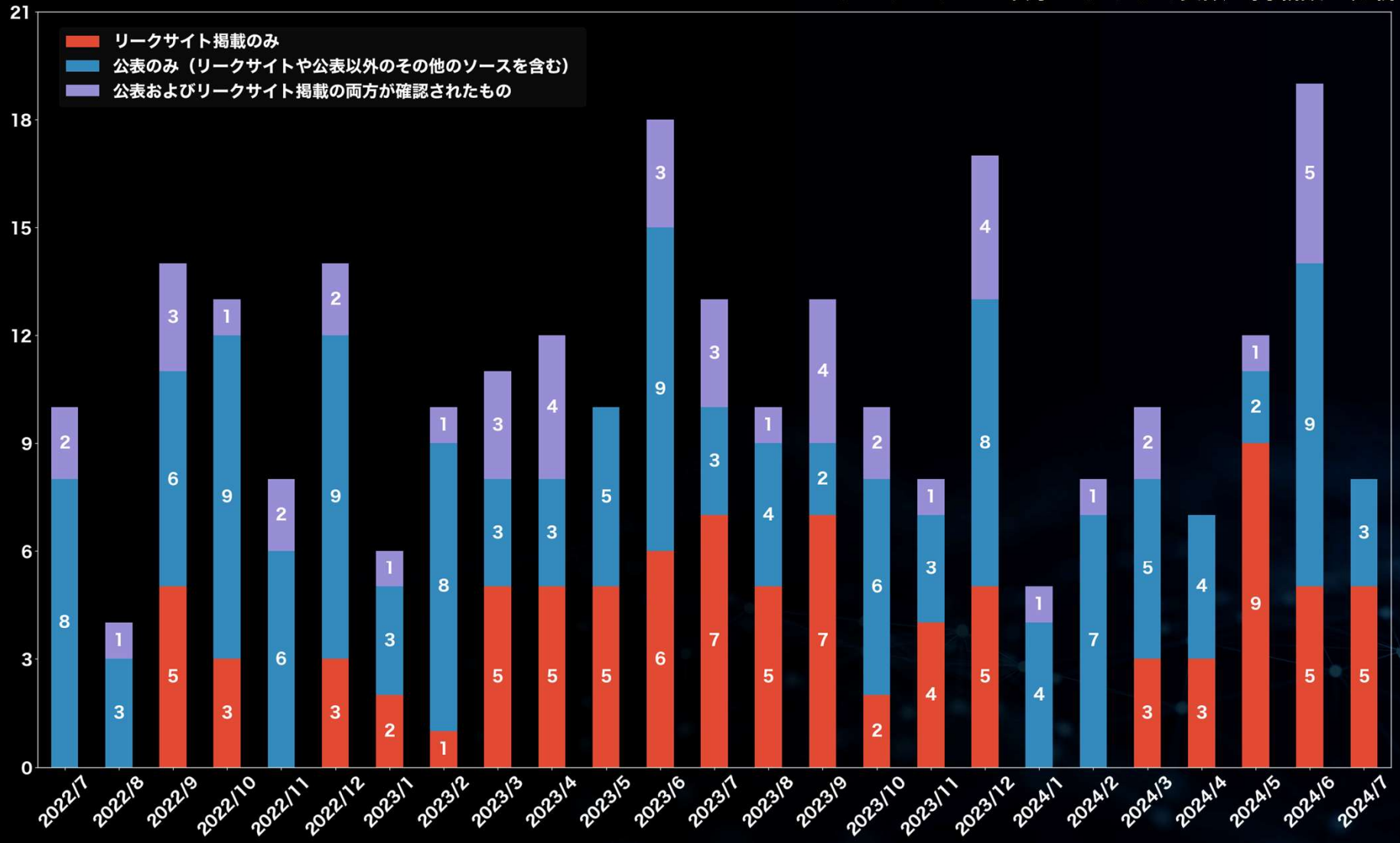
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

公表割合 月別内訳

（2022年7月～2024年7月／国内）(MBSD調べ)

Know your enemy. Defense leadership.

▼ランサムウェア攻撃における公表数と掲載数の分析



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

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

公となった国内被害組織 概要一覧

2024

7

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

公となった国内被害組織概要一覧

（過去1年間／2023年7月～2024年7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
2023/7	LockBit	船舶ターミナルシステム
2023/7	PLAY	大手生活用品メーカー(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	AlphV (BlackCat)	大手食品メーカー(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	(Unknown)	化粧品メーカー
2023/7	AKIRA	大手音楽関連商品メーカー(海外拠点)
2023/7	CL0P (CLOP)	大手電気機器メーカー(海外拠点)
2023/7	(Unknown)	大手信販会社
2023/7	CL0P (CLOP)	自動車部品メーカー(海外拠点)
2023/7	NoEscape	土木建設会社
2023/8	Mallox	和菓子メーカー
2023/8	(Unknown)	電気設備工事会社
2023/8	NoEscape	電気設備工事会社
2023/8	CL0P (CLOP)	大手印刷機械メーカー
2023/8	LockBit	大手物流会社(海外拠点)
2023/8	(Unknown)	大手教育関連事業会社
2023/8	(Unknown)	教育関連事業会社
2023/8	AlphV (BlackCat)	大手精密機器メーカー
2023/8	(Unknown)	容器メーカー
2023/8	LockBit	総合機器装置メーカー
2023/9	LockBit	大手塗料メーカー(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	Qilin (Agenda)	大手繊維製品メーカー(海外拠点)
2023/9	BlackByte	自動車部品メーカー
2023/9	AKIRA	パッケージ製品メーカー(海外拠点)
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	AlphV (BlackCat)	大手運輸サービス会社(海外拠点)
2023/9	STORMOUS	大手電子機器メーカー
2023/9	AlphV (BlackCat)	自動車部品メーカー(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	NoEscape	自動車部品メーカー
2023/10	PLAY	眼鏡メーカー
2023/10	AlphV (BlackCat)	大手専門商社
2023/10	Ransomed.vc	インターネットプロバイダー
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
2023/11	LockBit	自転車部品メーカー
2023/11	(Unknown)	耐火製品メーカー
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	(Unknown)	公立病院
2023/11	Hunters International	大手機械部品メーカー
2023/11	Medusa	金融サービス会社(海外拠点)
2023/11	INC Ransom	大手輸送用機器メーカー(海外拠点)
2023/12	LockBit	エネルギーサービス運営管理会社
2023/12	AKIRA	大手自動車メーカー(海外拠点)
2023/12	(Unknown)	大手出版社
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	(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	LockBit	社会福祉法人
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	BlackBasta	大手ガラス製品メーカー(海外拠点)
2023/12	(Unknown)	地方新聞社
2023/12	DragonForce	大手食品メーカー(海外拠点)
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)
2024/1	(Unknown)	国立研究開発法人
2024/1	LockBit	包装用品メーカー
2024/1	(Unknown)	漁網総合メーカー
2024/1	LockBit	公益財団法人
2024/1	(Unknown)	建設機材サービス
2024/2	(Unknown)	医療関連製品卸売業
2024/2	(Unknown)	ITサービス会社
2024/2	(Unknown)	医療検査機関
2024/2	LockBit	自動車部品メーカー
2024/2	LockBit	化学メーカー
2024/2	(Unknown)	総合商店運営
2024/2	(Unknown)	物流サービス会社
2024/2	(Unknown)	医療機関

（※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）

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

公となった国内被害組織概要一覧

（過去1年間／2023年7月～2024年7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
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	(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	LockBit	合成繊維製造会社
2024/3	LockBit	合成繊維製造会社
2024/3	8BASE	自動車部品メーカー(海外拠点)
2024/3	(Unknown)	建設関連事業会社
2024/3	Hunters International	医療機器メーカー
2024/4	8BASE	電子部品メーカー
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	(Unknown)	繊維製品サプライヤー
2024/4	(Unknown)	ボルトメーカー
2024/4	LockBit	アクセサリーパーツメーカー
2024/4	(Unknown)	電子機器サプライヤー
2024/5	LockBit	製紙会社(海外拠点)
2024/5	Hunters International	音響関連機器メーカー(海外拠点)
2024/5	CL0P (CLOP)	大手文房具メーカー(海外拠点)
2024/5	(Unknown)	化学製品メーカー
2024/5	Ransomhub	ソフトウェア企業
2024/5	RansomHouse	建築部品メーカー
2024/5	(Unknown)	地方独立行政法人
2024/5	LockBit	ITサービス会社(海外拠点)
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

被害月	攻撃グループ	業種概要
2024/5	8BASE	税理士法人
2024/6	(Unknown)	電子機器メーカー
2024/6	8BASE	電動機メーカー(海外拠点)
2024/6	8BASE	ITサービス会社
2024/6	(Unknown)	製薬会社
2024/6	AKIRA	大手電機メーカー(海外拠点)
2024/6	(Unknown)	機械部品メーカー
2024/6	(Unknown)	化学メーカー(海外拠点)
2024/6	(Unknown)	総合会計・コンサルティンググループ
2024/6	BlackSuit	大手出版社
2024/6	CACTUS	アパレルメーカー
2024/6	INC Ransom	工業機械メーカー(海外拠点)
2024/6	(Unknown)	仏具メーカー
2024/6	(Unknown)	建設コンサルタント会社
2024/6	CACTUS	内装材メーカー(海外拠点)
2024/6	8BASE	総合インフラ施工会社
2024/6	8BASE	総合建設メーカー
2024/6	LockBit	通信機器メーカー
2024/6	(Unknown)	総合エンジニアリング会社
2024/6	(Unknown)	食品メーカー
2024/7	Ransomhub	大手システムインテグレーター(海外拠点)
2024/7	(Unknown)	電子機器メーカー(海外拠点)
2024/7	(Unknown)	印刷サービス会社
2024/7	(Unknown)	大手総合ディスプレイ企業
2024/7	Hunters International	光学レンズメーカー
2024/7	Ransomhub	大手建設会社
2024/7	MEOW	空調機器メーカー
2024/7	CACTUS	電子部品メーカー(海外拠点)

（※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）

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

公となった国内被害組織における拠点割合

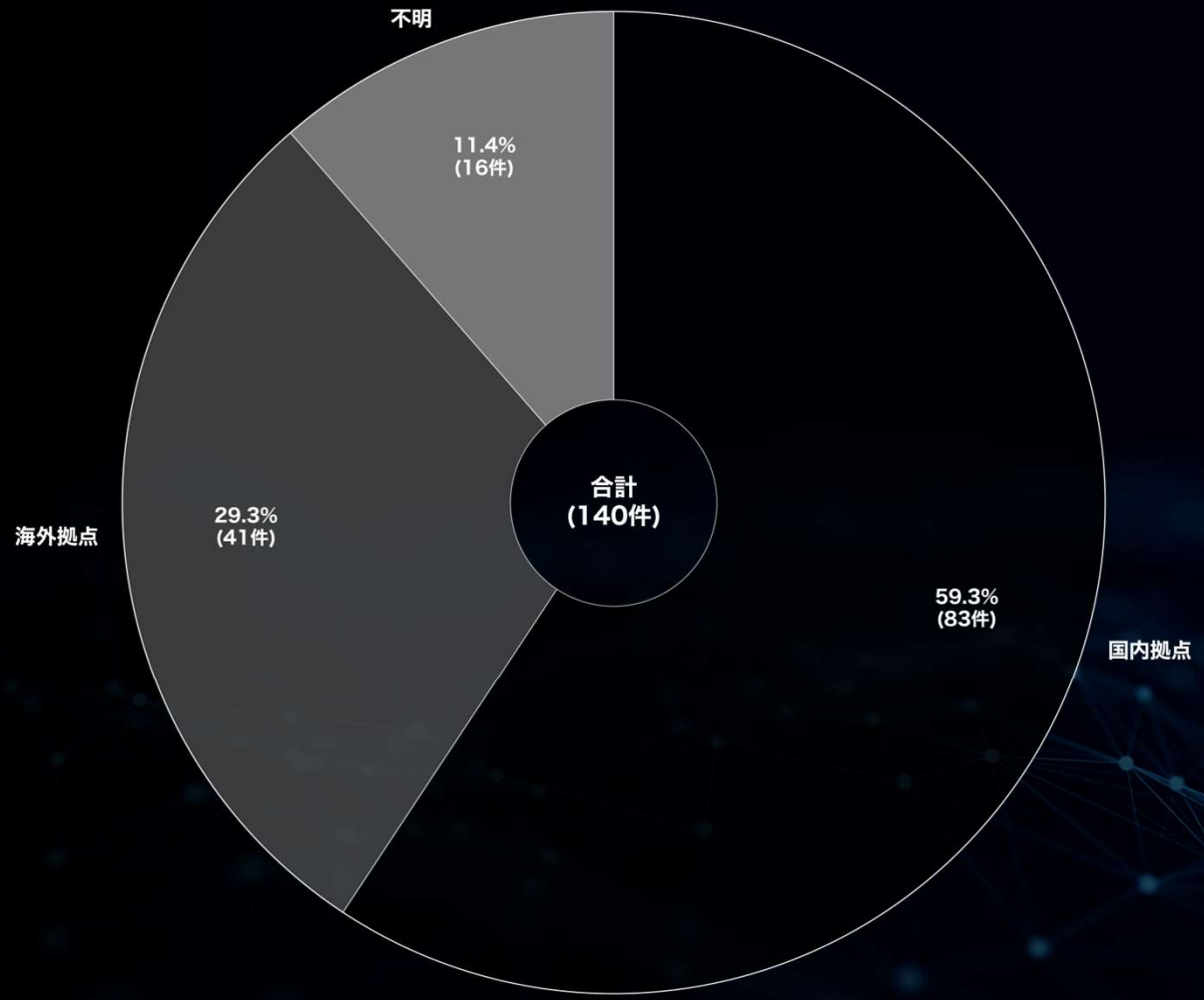
（過去1年間／2023年7月～2024年7月）(MBSD調べ)

（※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	83	59.3
海外拠点	41	29.3
不明	16	11.4

▼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）

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

2024

7

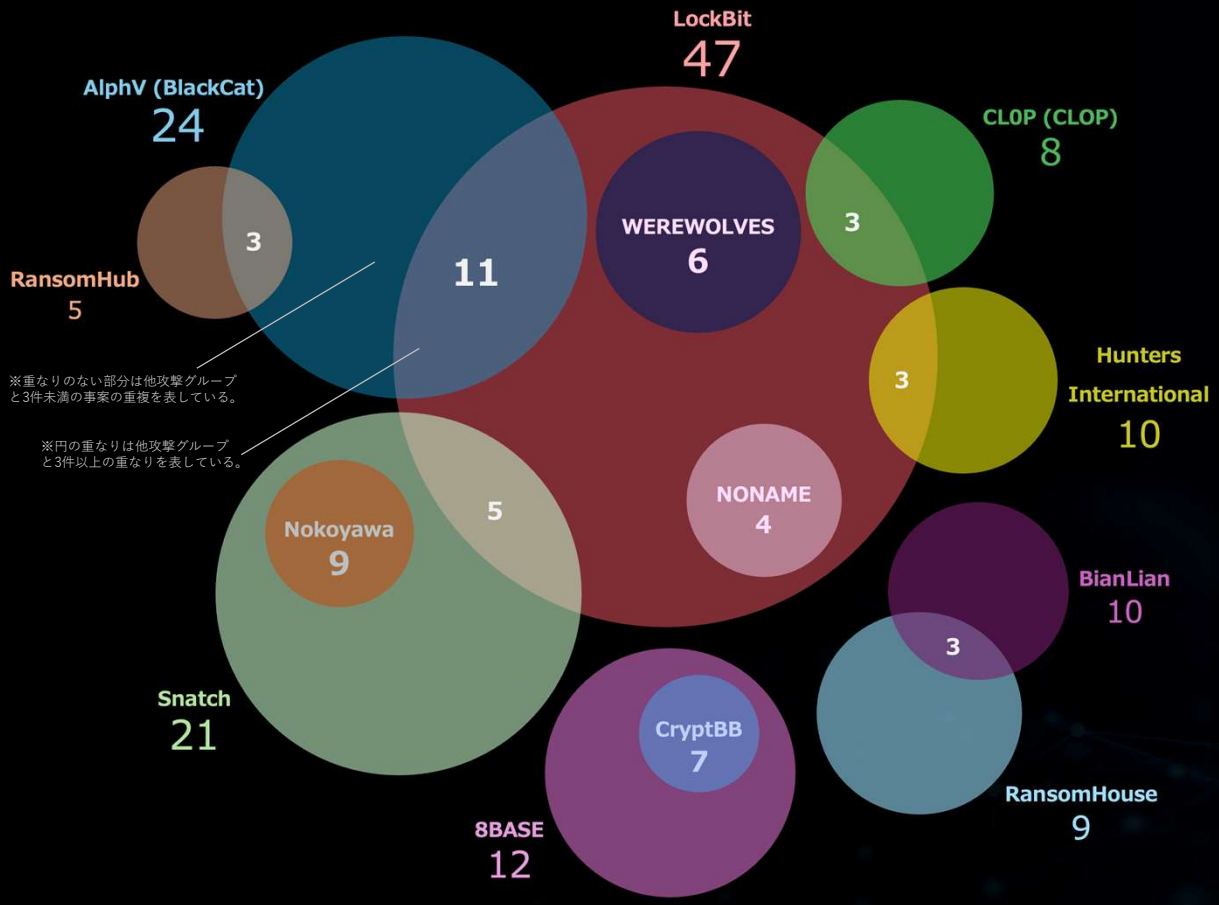
多重被害に関する分析

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

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

（過去2年間／2022年8月～2024年7月／累計131件）(MBSD調べ)

※多重被害に遭った組織数の累計



※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)のアフィリエイトが被害組織のデータを他の攻撃グループに持ち込んだことで、その被害組織が異なる攻撃グループから連続して脅迫されてしまったというケースが挙げられる。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。

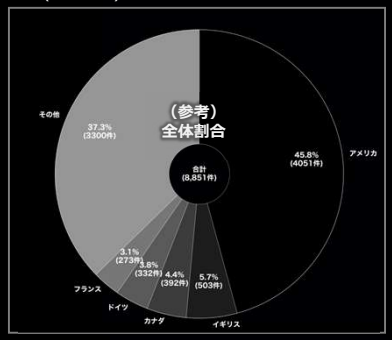
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

多重被害に遭った被害組織の傾向と分析

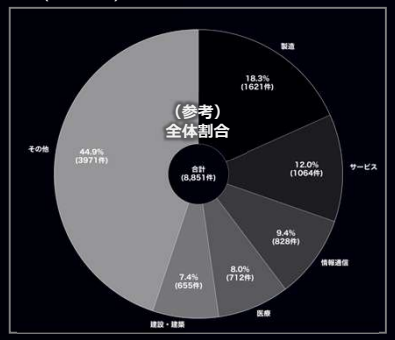
（過去2年間／2022年8月～2024年7月）(MBSD調べ)

※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

(参考比較) 同期間の全データにおける割合

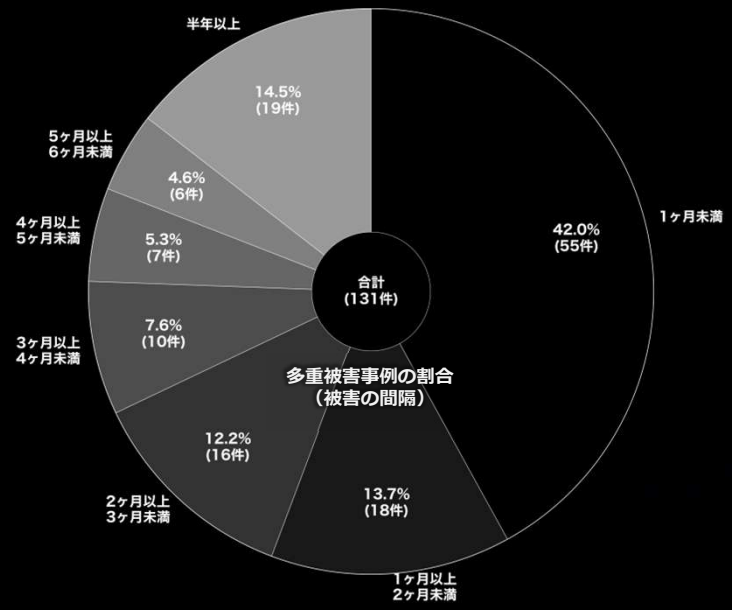


(参考比較) 同期間の全データにおける割合

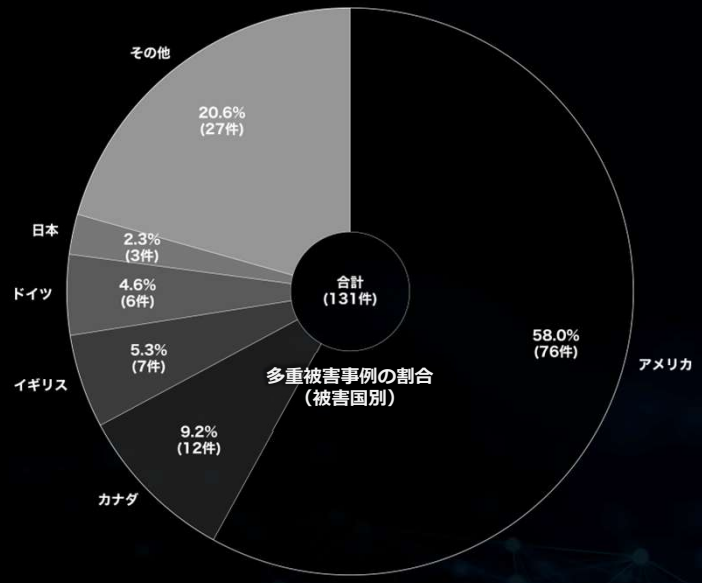


▼被害の間隔

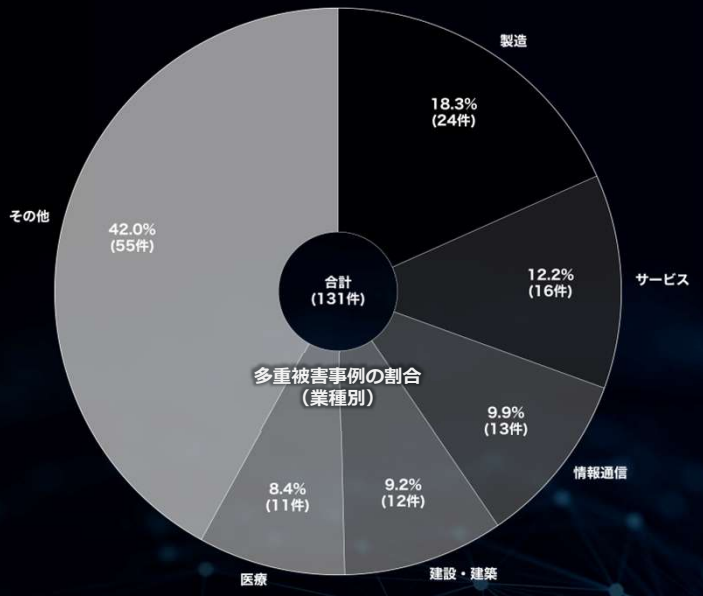
（一度目の被害から二度目の被害までの間隔）



▼被害国別



▼業種別



▶多重被害に遭った組織数の累計：131件（全体8851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。

※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

CIGのコンテンツ紹介

Know your enemy. Defense leadership.

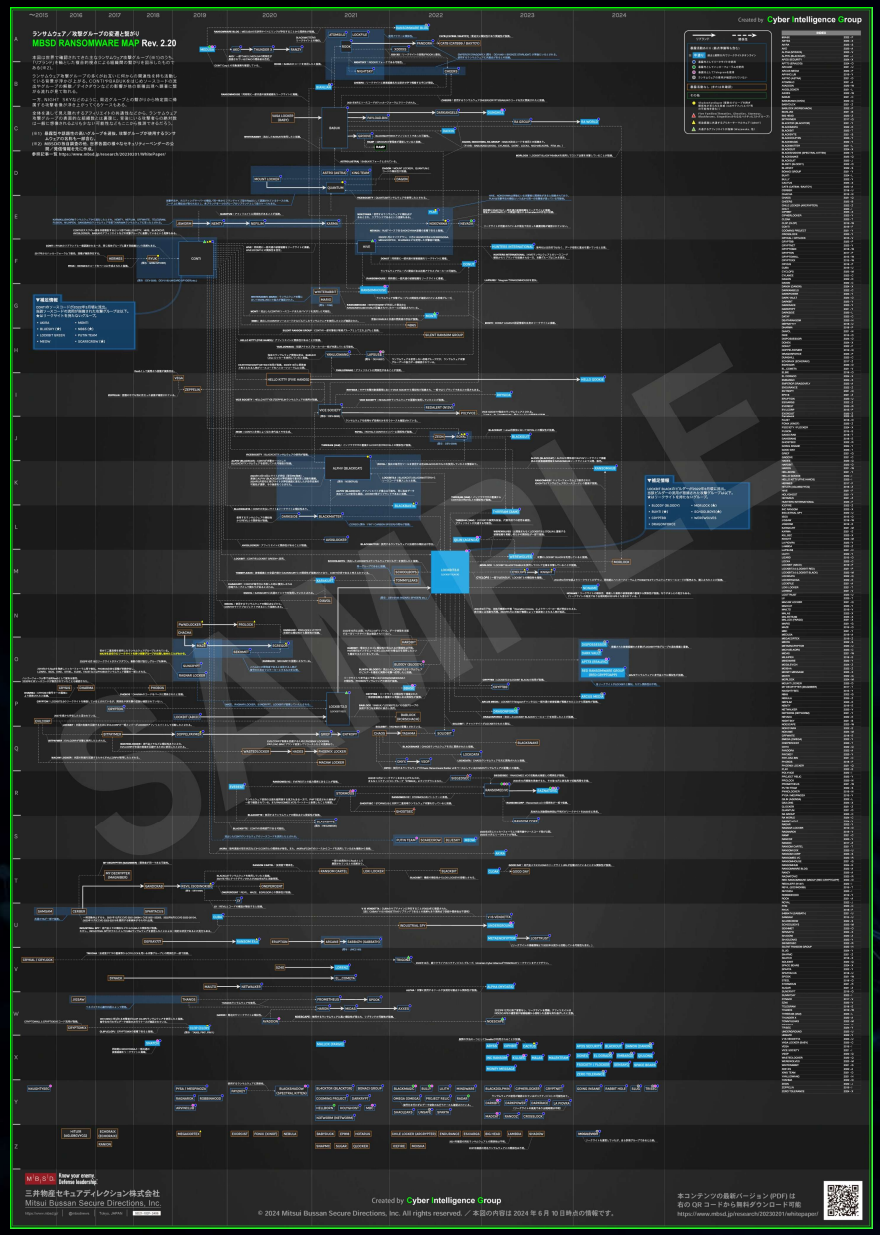
Cyber Intelligence Group（CIG）では、ランサムウェアに関する様々な観点からの分析結果を情報発信しています。ぜひとも皆様の脅威情報の把握にご活用ください。

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

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

● 技術ブログ：
https://www.mbsd.jp/research/cig/
https://www.mbsd.jp/research/t.yoshikawa/

MBSD RANSOMWARE MAP (Rev.2)



本資料に関する留意事項及び二次利用について

Know your enemy.
Defense leadership.

留意事項

・ 攻撃グループや被害組織などについて、正確な情報が公開されていない項目は「(Unknown)」として集計しています。

・各分析における掲載数は、特に注釈がない限り、公表や報道を含めず、リークサイトに掲載された数のみを基にしています。
（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）を含みます。

・ 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 Cyber Intelligence Group (CIG) 独自の観測および集計結果となります。

・ 件数については、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基に集計しています。

・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まれています。

・ 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ます。

・ 集計方法の変更や、時間が長期経過し公開／公表されるケースを再集計する場合もあるため、常に最新月のレポートを参照してください。

二次利用等に関して

本レポート記載内容の二次利用は基本的に自由&無料となります。
ただし、ご利用、転載、引用などされる際は出典元を「MBSD Cyber Intelligence Group (CIG)」と明記いただきますようお願いいたします。
(※セミナー、出版物、メディア等での本情報の引用・転載は、原則として許可いたします。ただし、ご利用の際は必ず事前に以下のお問い合わせ窓口から詳細をお知らせください。)

お問い合わせ窓口：https://www.mbsd.jp/contact/

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