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

2025年3月号 Rev 1.00
(2025年2月分)

2025

2

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 ~ ㉒）

中小企業における被害分析（レポート㉓ ~㉖）

多重被害に関する分析（レポート㉗ ~ ㉘）

業種に関する分析（レポート㉙）

その他

2025

2

総括と監視対象

今月のハイライト

● CL0P（CLOP）によるゼロデイ脆弱性を悪用した大規模攻撃と被害組織

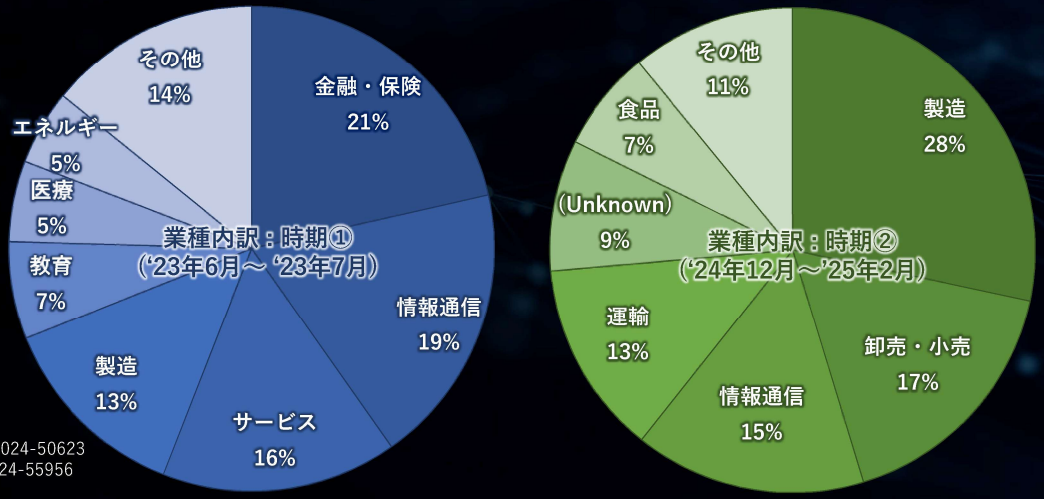
2024年末、サイバー犯罪グループCL0Pが自身のリークサイト上に、ゼロデイ脆弱性※1を悪用した大規模攻撃に関する声明を掲載した。
※1）CLEO社のファイル転送管理プラットフォームに存在するゼロデイ脆弱性(CVE-2024-50623およびCVE-2024-55956)

CL0Pは過去にも複数回、ゼロデイ脆弱性を悪用した大規模攻撃を展開している。下図は過去2年間のCL0Pのリークサイト掲載数の推移を示したものである。
近年のCL0Pの活動は長期間の停滞期ののち、突発的にリークサイトに攻撃声明や被害組織情報を掲載するケースが特徴的である。2023年中頃のProgress Software社のファイル転送ソフトを標的とした攻撃※2と、今回の攻撃の間も約1年半もの期間が空いている。このような特徴から表面上は活動が停滞しているように見えても、この期間に次の大規模攻撃への準備や実際の攻撃をすでに開始している可能性が考えられる。

2023年6月から7月（上図の**時期①**）、2024年12月から2025年2月（上図の**時期②**）に掲載された組織の業種を分析すると、内訳は大きく異なることがわかる（右図）。

ゼロデイ攻撃による被害はどの業界でも起こりうる脅威であり、各組織はベンダーから提供されるセキュリティアップデートを迅速に適用することが重要である。
特に今回のゼロデイ攻撃では、初回のパッチ適用後も新たな攻撃手法が発見され、2度目の修正パッチがリリースされている。
このことは、脆弱性情報を継続的に把握し適切に対応することの重要性を改めて示している。

各ゼロデイ攻撃ごとに異なる業種分布



※1 : https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623
https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956
※2 : https://www.progress.com/trust-center/moveit-transfer-and-moveit-cloud-vulnerability

※ 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）：216（※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：49

※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)
● Anubis
Apos Security
APT73 (Eraleig)
ARCUS MEDIA
Argonauts
ArvinClub
Astro (Astra)
AtomSilo
Avaddon
AvosLocker
Axxes
Babuk
Babuk (2025)
BASHE
BianLian
BL0ODY (BLOODY)
Bl4ckt0r (BlackTor)
BlackBasta
BlackByte
BlackDolphin
BlackLock
BlackMatter
Blackout
BlackSuit
BLUEBOX
BLUESKY
Brain Cipher
BULLY
CACTUS
CHEERS
ChileLocker (Arcrypter)
CHORT
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
DragonRansomware
DUNGHILL
eCh0raix (eChoraix)
El_Cometa
EL DORADO
EMBARGO
Endurance
Entropy
Everest
FOG
FSOCIETY / FLOCKER
FSTeam
Funksec
GD LockerSec
Grief
Groove
HANDARA [Hacktivist]
Haron
HELLCAT
Helldown
HelloGookie
Hitler (AGL0BGVYCG)
Hive
HolyGhost
Hotarus
Hunters International
ICEFIRE
INC Ransom
Insane
INTERLOCK
KAIROS
Karakurt
Karma
KILLSEC
Knight
● Kraken (HelloKitty)
LAMBDA
La Piovra
LAPSUS$
LILITH
● Linkc
LockBit
Lorenz
LostTrust
LV
LYNX
MADCAT
MAD LIBERATOR
MALAS
MalekTeam
Mallox
MBC
Medusa
MEOW
Metaencryptor
Midas
Mindware
Mogilevich [fraud]
MOISHA
Money Message
Monti
Morpheus
Mount Locker
N3tw0rm (NetWorm)
N4UGHTYSEC (NAUGHTYSEC)
Nefilim
Nevada
NightSky
NITROGEN
NoEscape
Nokoyawa
NONAME (VFOKX)
NONAME [2023年確認]
NULLBULGE
Onyx
Orca
Pandora
Pay2Key
Payload.bin
PLAY
PLAYBOY
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
● RunSomeWares
Sabbath (54bb47h)
SAFEPAY
SARCOMA
SenSayQ
shaoleaks
SIEGEDSEC
SLUG
Snatch
Solidbit
Space Bears
Sparta
Spook
STORMOUS
Sugar
Suncrypt
SynACK
Termite
ThreeAM (3AM)
TRIGONA
TRINITY
TRISEC
Underground
UnSafe
Valencia
VanirGroup
Vice Society
V IS VENDETTA
VSOP
WEREWOLVES
x001xs
XING Team
Yanluowang
Zeon
Zero Tolerance

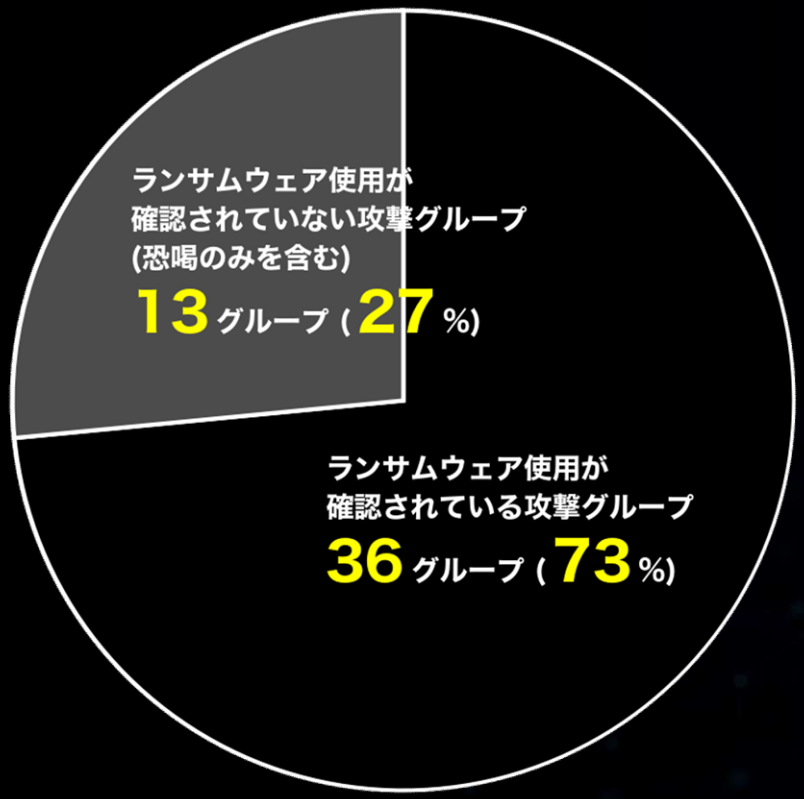
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

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（2025年 2月）

（※当月にリークサイト掲載を確認した攻撃グループ全 49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、2025年2月に活動中である事が確認された全49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。

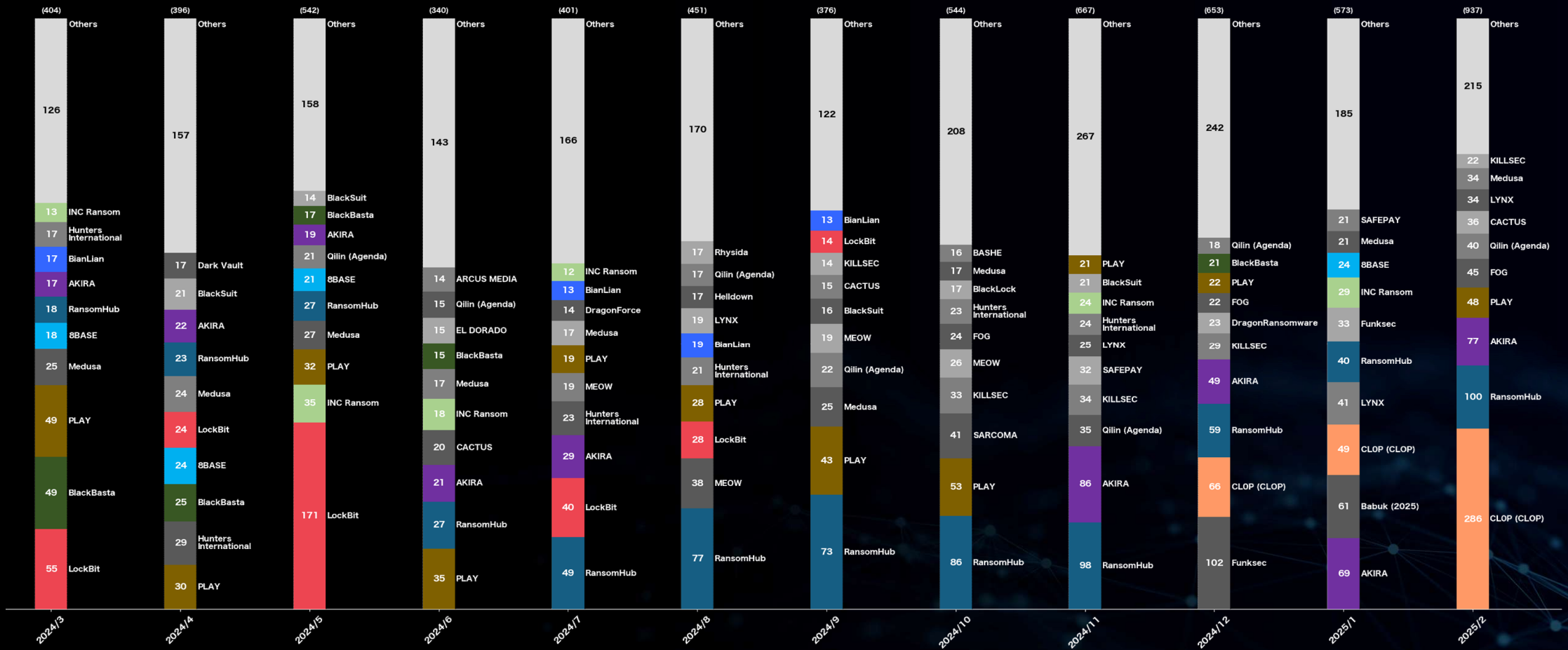
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

年間 統計
（全世界）

2025

2

攻撃グループ割合で見る被害数の年間統計（全世界）
（過去1年間／2024年3月～2025年2月）



※ 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）

2025

2

月別内訳 攻撃グループ TOP10（全世界）

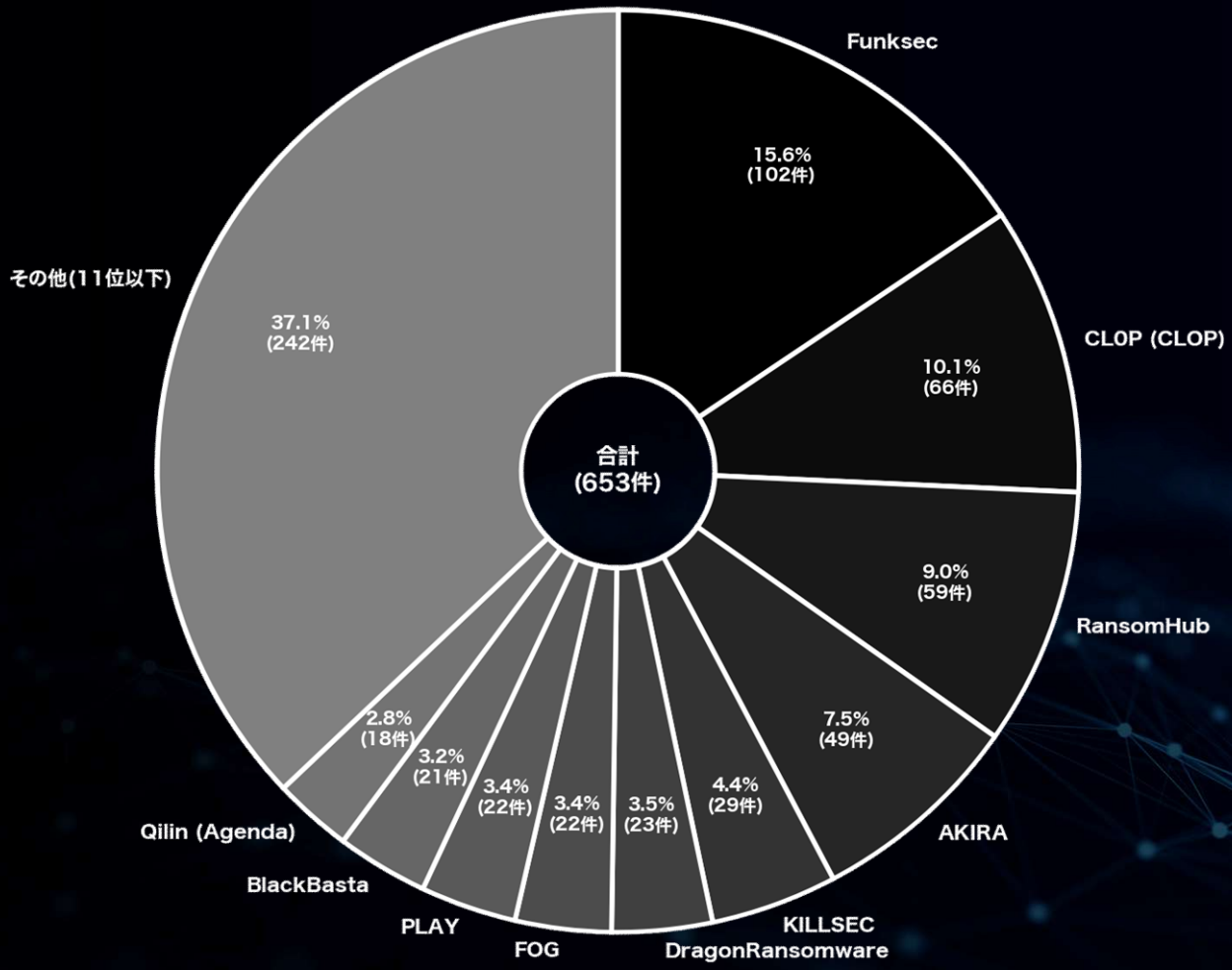
（2024年 12 月）

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)
Funksec	102	15.6	+ 102
CL0P (CLOP)	66	10.1	+ 66
RansomHub	59	9.0	- 39
AKIRA	49	7.5	- 37
KILLSEC	29	4.4	- 5
DragonRansomware	23	3.5	+ 15
FOG	22	3.4	+ 2
PLAY	22	3.4	+ 1
BlackBasta	21	3.2	+ 6
Qilin (Agenda)	18	2.8	- 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）



※ 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（全世界）

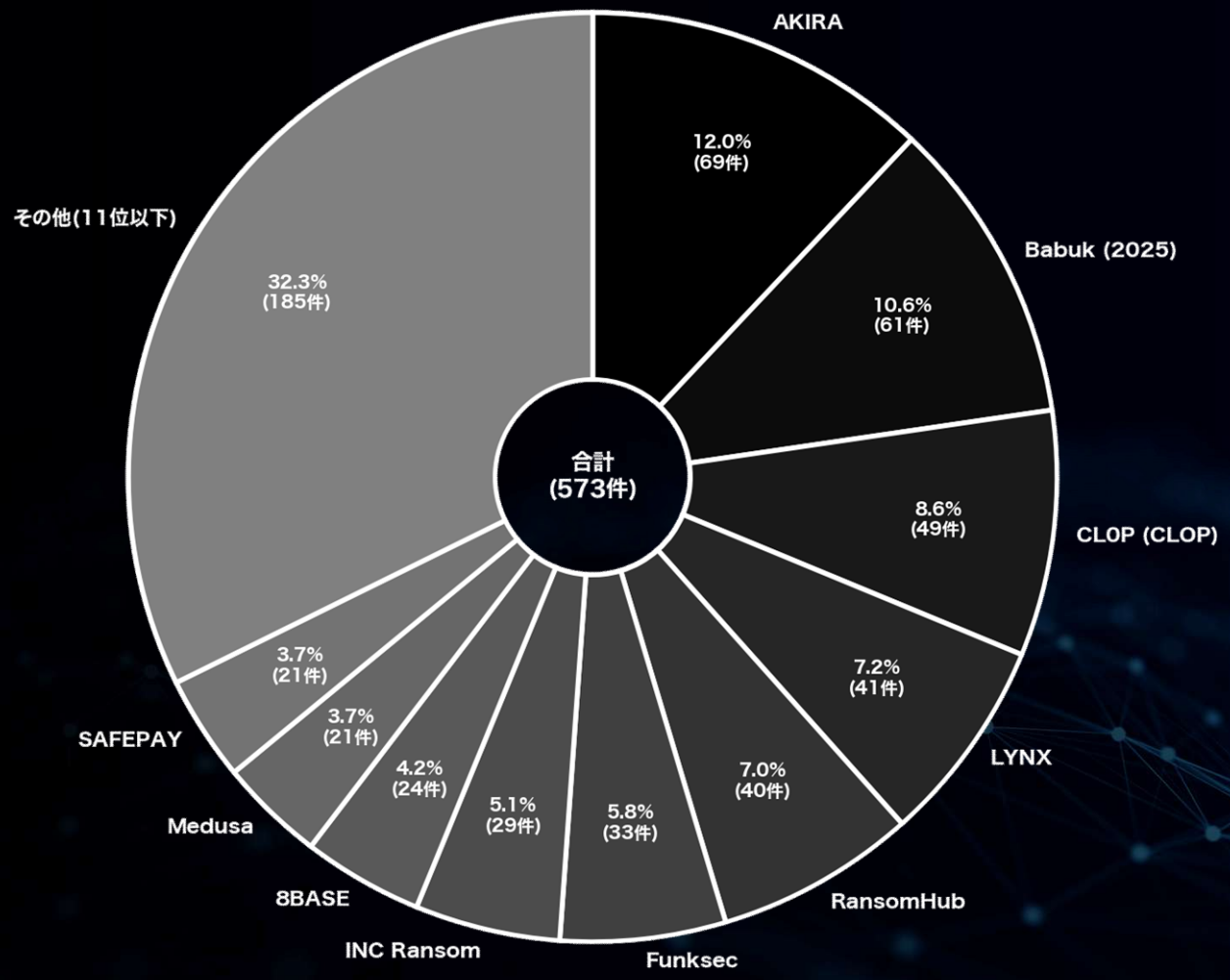
（2025年 1 月）

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)
AKIRA	69	12.0	+ 20
Babuk (2025)	61	10.6	+ 61
CL0P (CLOP)	49	8.6	- 17
LYNX	41	7.2	+ 28
RansomHub	40	7.0	- 19
Funksec	33	5.8	- 69
INC Ransom	29	5.1	+ 19
8BASE	24	4.2	+ 13
Medusa	21	3.7	+ 8
SAFEPAY	21	3.7	+ 6

▼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（全世界）

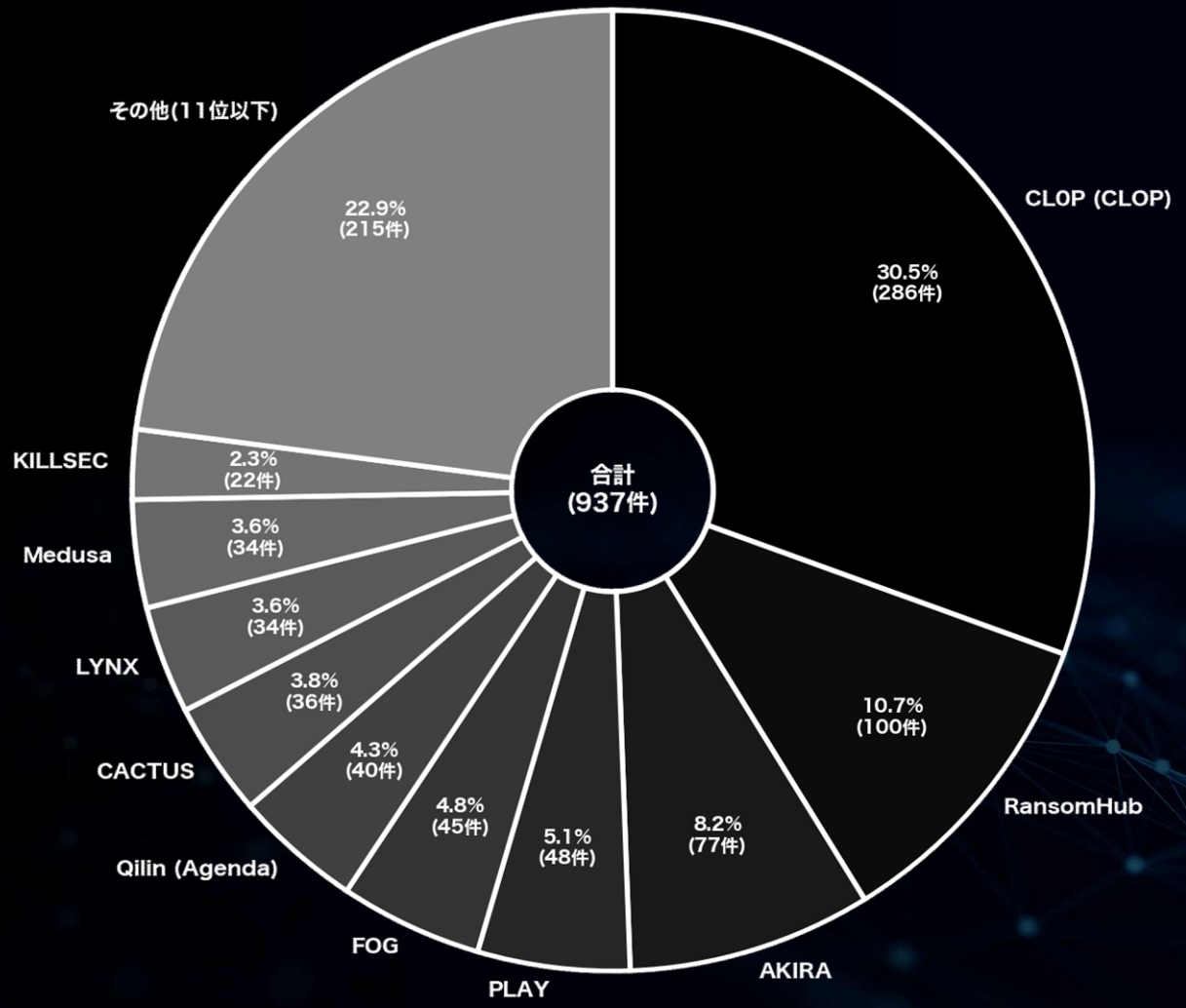
（2025年 2 月）

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)
CL0P (CLOP)	286	30.5	+ 237
RansomHub	100	10.7	+ 60
AKIRA	77	8.2	+ 8
PLAY	48	5.1	+ 37
FOG	45	4.8	+ 30
Qilin (Agenda)	40	4.3	+ 21
CACTUS	36	3.8	+ 27
LYNX	34	3.6	- 7
Medusa	34	3.6	+ 13
KILLSEC	22	2.3	+ 13

▼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

2025

2

被害国 月別統計

（全世界） （過去3ヶ月分）

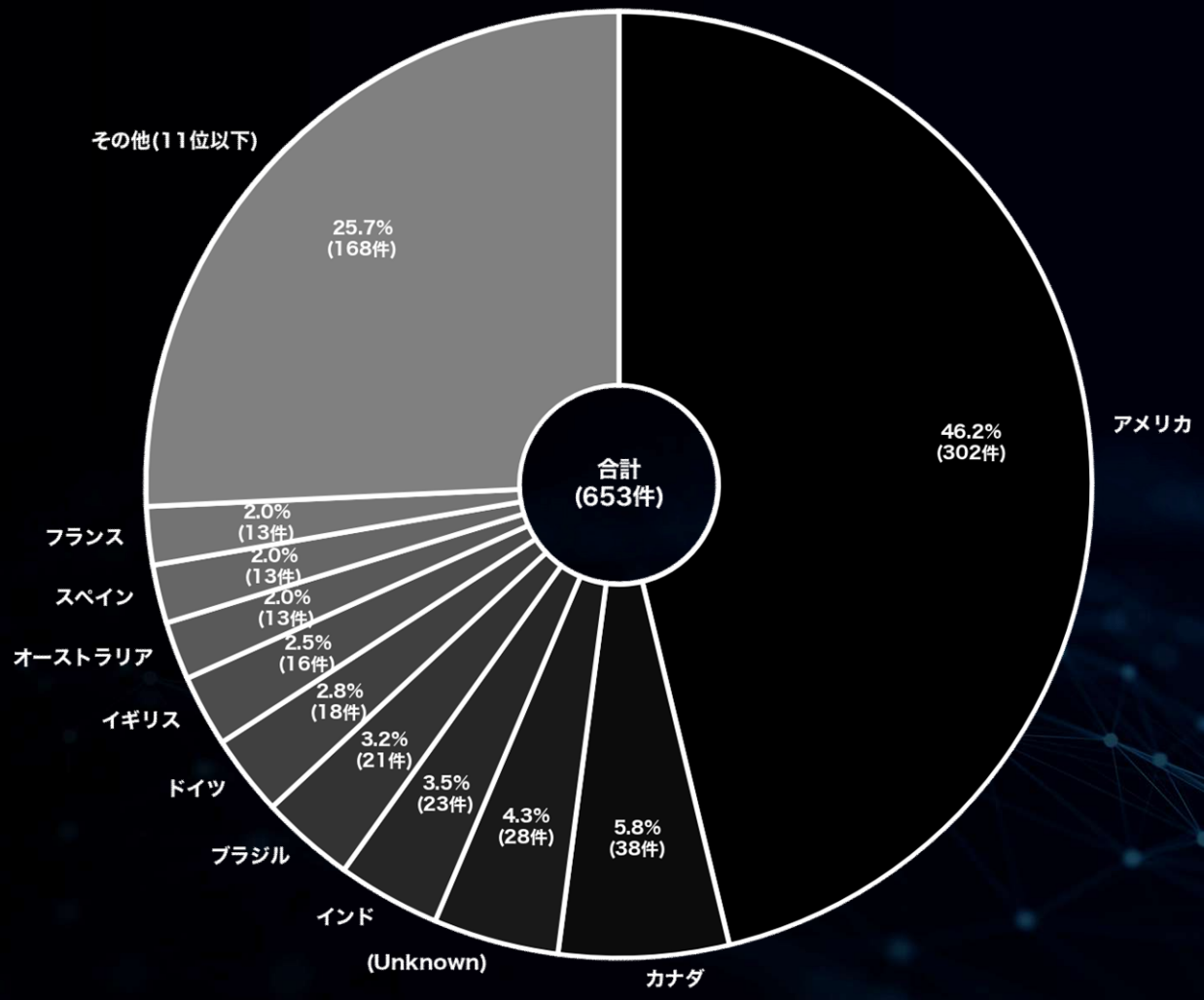
月別内訳 被害国TOP10（全世界）
（2024年 12 月）

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	302	46.2	- 59
カナダ	38	5.8	+ 17
(Unknown)	28	4.3	+ 13
インド	23	3.5	+ 9
ブラジル	21	3.2	+ 8
ドイツ	18	2.8	- 4
イギリス	16	2.5	- 6
オーストラリア	13	2.0	- 1
スペイン	13	2.0	+ 12
フランス	13	2.0	- 4

▼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

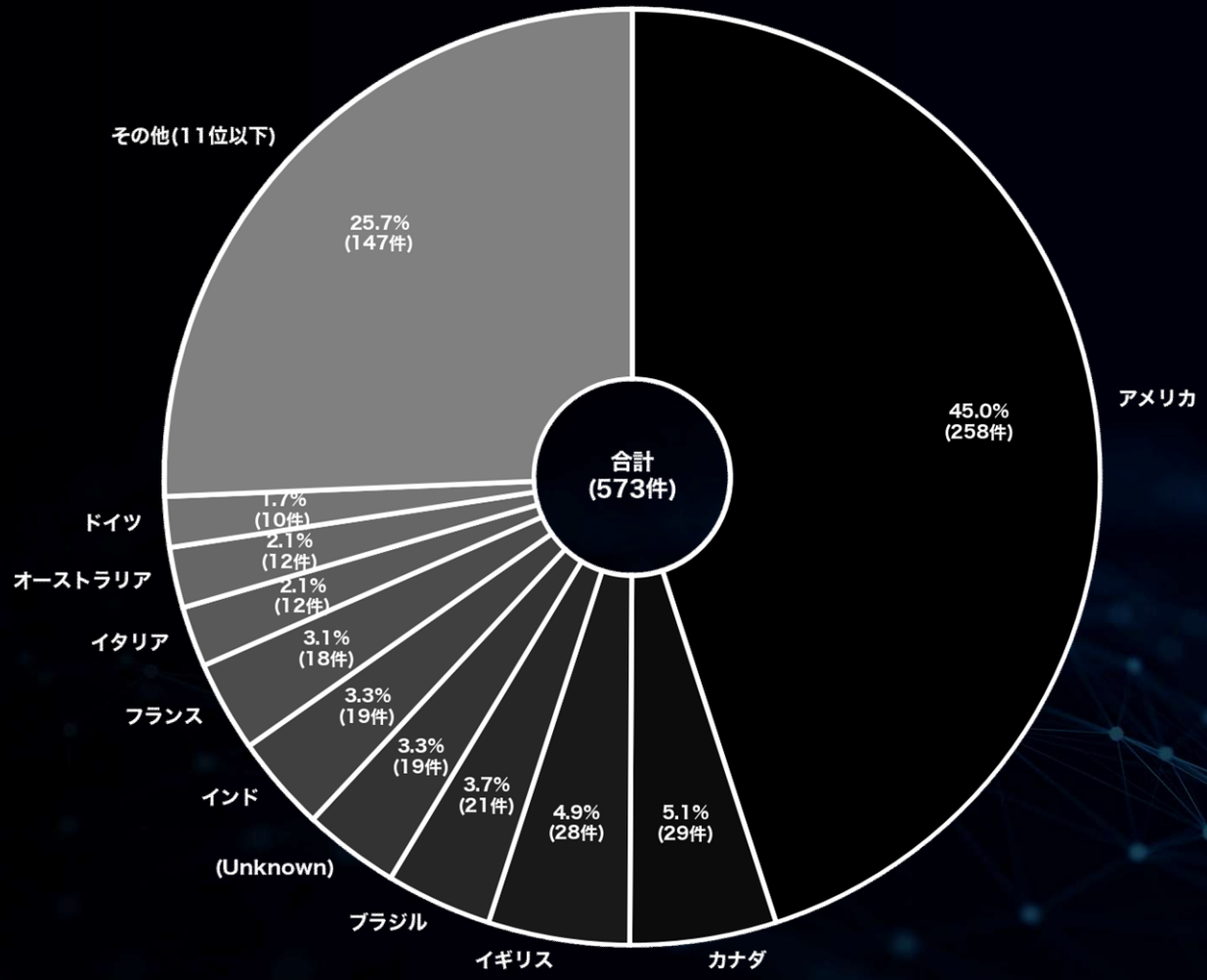
月別内訳 被害国TOP10（全世界）
（2025年 1 月）

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	258	45.0	- 44
カナダ	29	5.1	- 9
イギリス	28	4.9	+ 12
ブラジル	21	3.7	± 0
(Unknown)	19	3.3	- 9
インド	19	3.3	- 4
フランス	18	3.1	+ 5
イタリア	12	2.1	+ 2
オーストラリア	12	2.1	- 1
ドイツ	10	1.7	- 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（全世界）

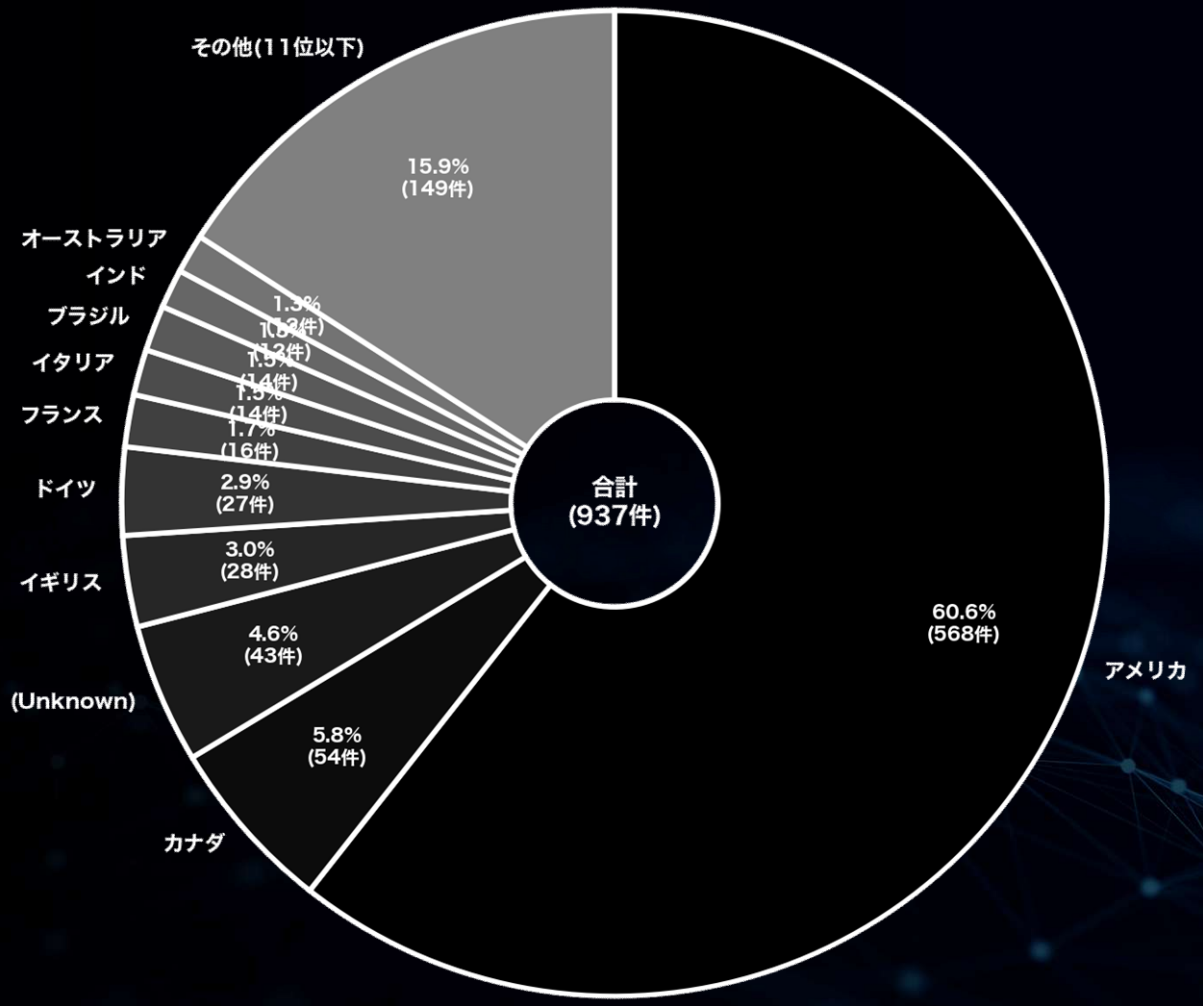
（2025年 2 月）

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	568	60.6	+ 310
カナダ	54	5.8	+ 25
(Unknown)	43	4.6	+ 24
イギリス	28	3.0	± 0
ドイツ	27	2.9	+ 17
フランス	16	1.7	- 2
イタリア	14	1.5	+ 2
ブラジル	14	1.5	- 7
インド	12	1.3	- 7
オーストラリア	12	1.3	± 0

▼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

2025

2

被害国 月別統計

（アジア）　（過去3ヶ月分）

月別内訳 被害国TOP10（アジア）

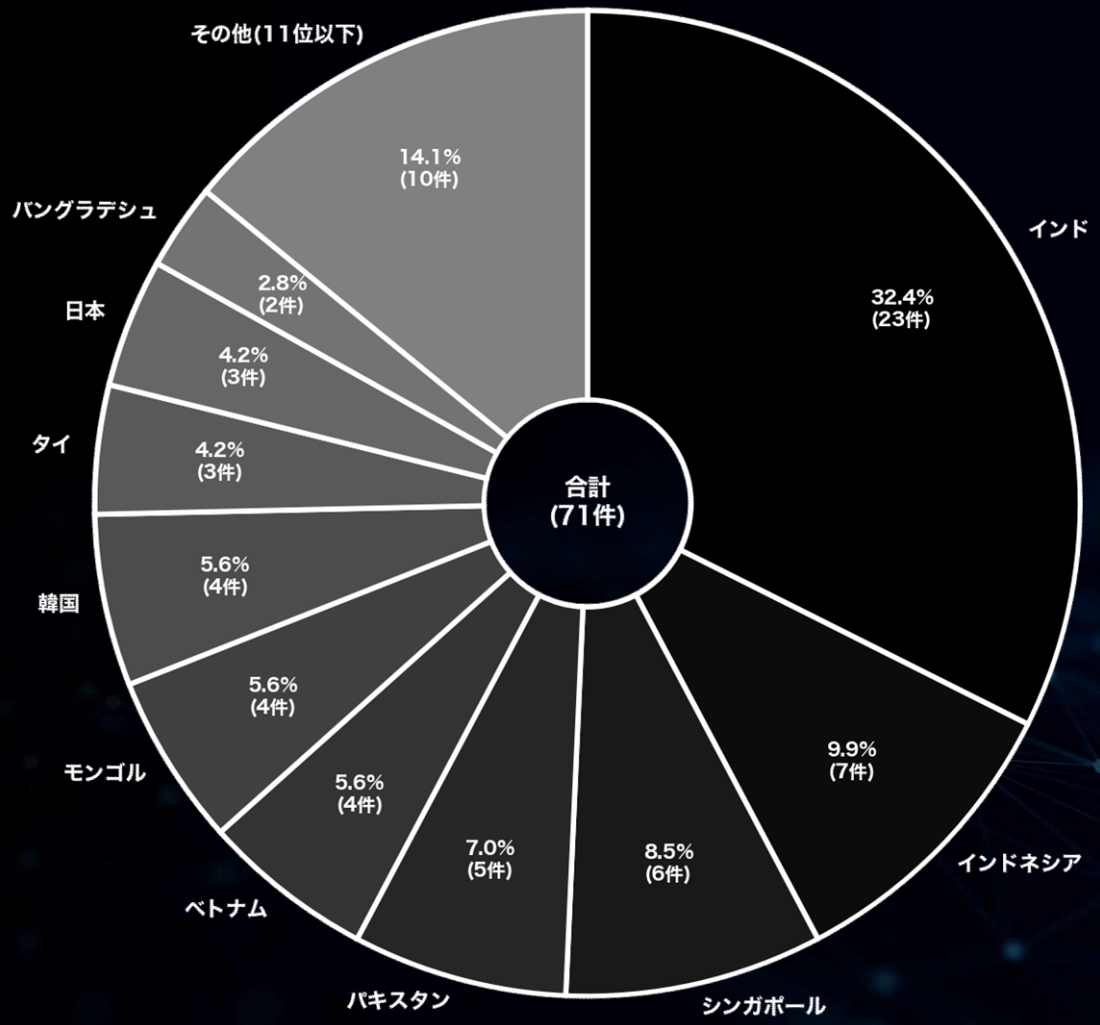
（2024年 12 月）

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	23	32.4	+ 9
インドネシア	7	9.9	+ 4
シンガポール	6	8.5	+ 4
パキスタン	5	7.0	+ 5
ベトナム	4	5.6	+ 3
モンゴル	4	5.6	+ 3
韓国	4	5.6	+ 3
タイ	3	4.2	+ 1
日本	3	4.2	- 4
バングラデシュ	2	2.8	± 0

▼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（アジア）

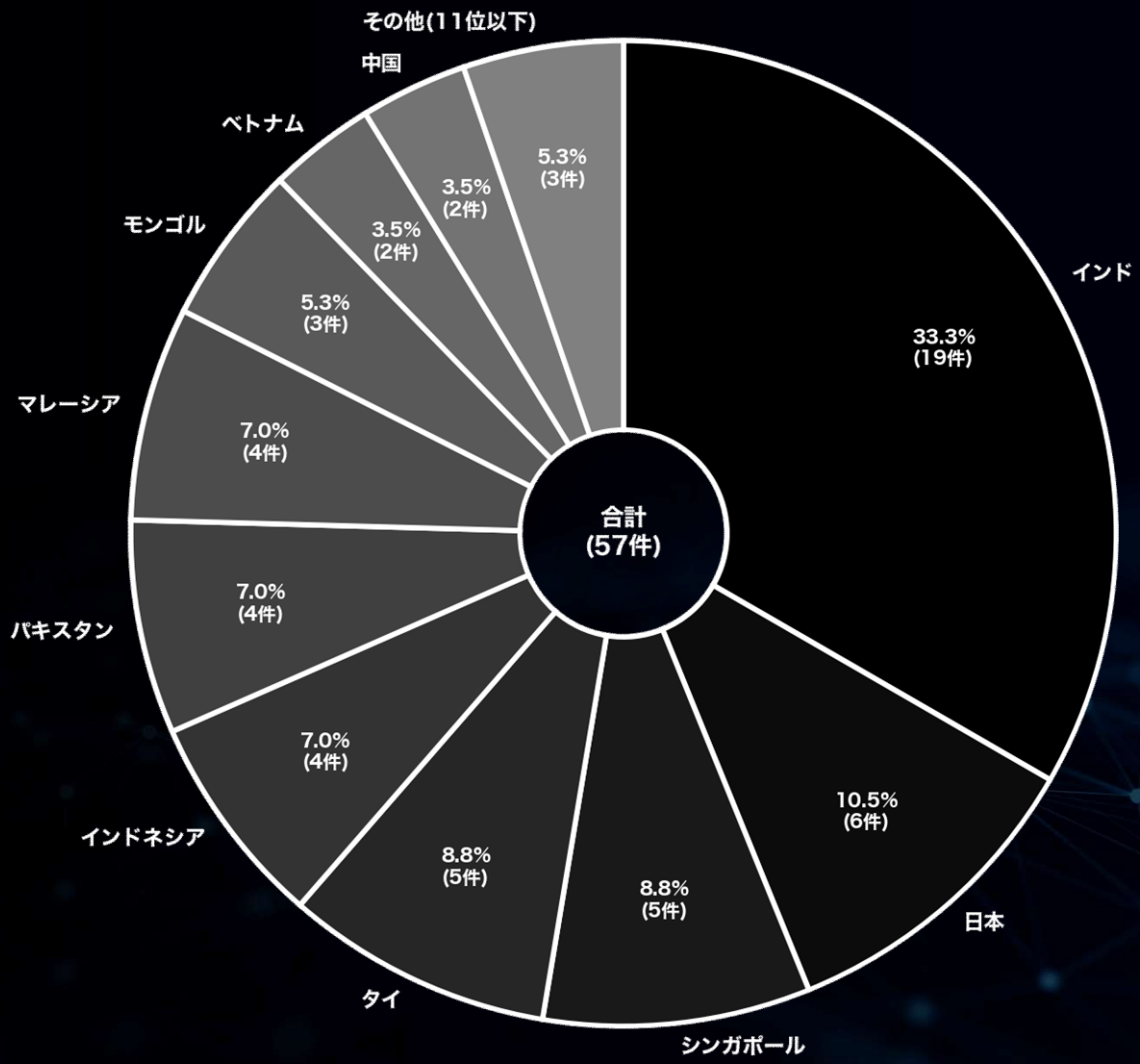
（2025年 1 月）

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	19	33.3	- 4
日本	6	10.5	+ 3
シンガポール	5	8.8	- 1
タイ	5	8.8	+ 2
インドネシア	4	7.0	- 3
パキスタン	4	7.0	- 1
マレーシア	4	7.0	+ 2
モンゴル	3	5.3	- 1
ベトナム	2	3.5	- 2
中国	2	3.5	± 0

▼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（アジア）

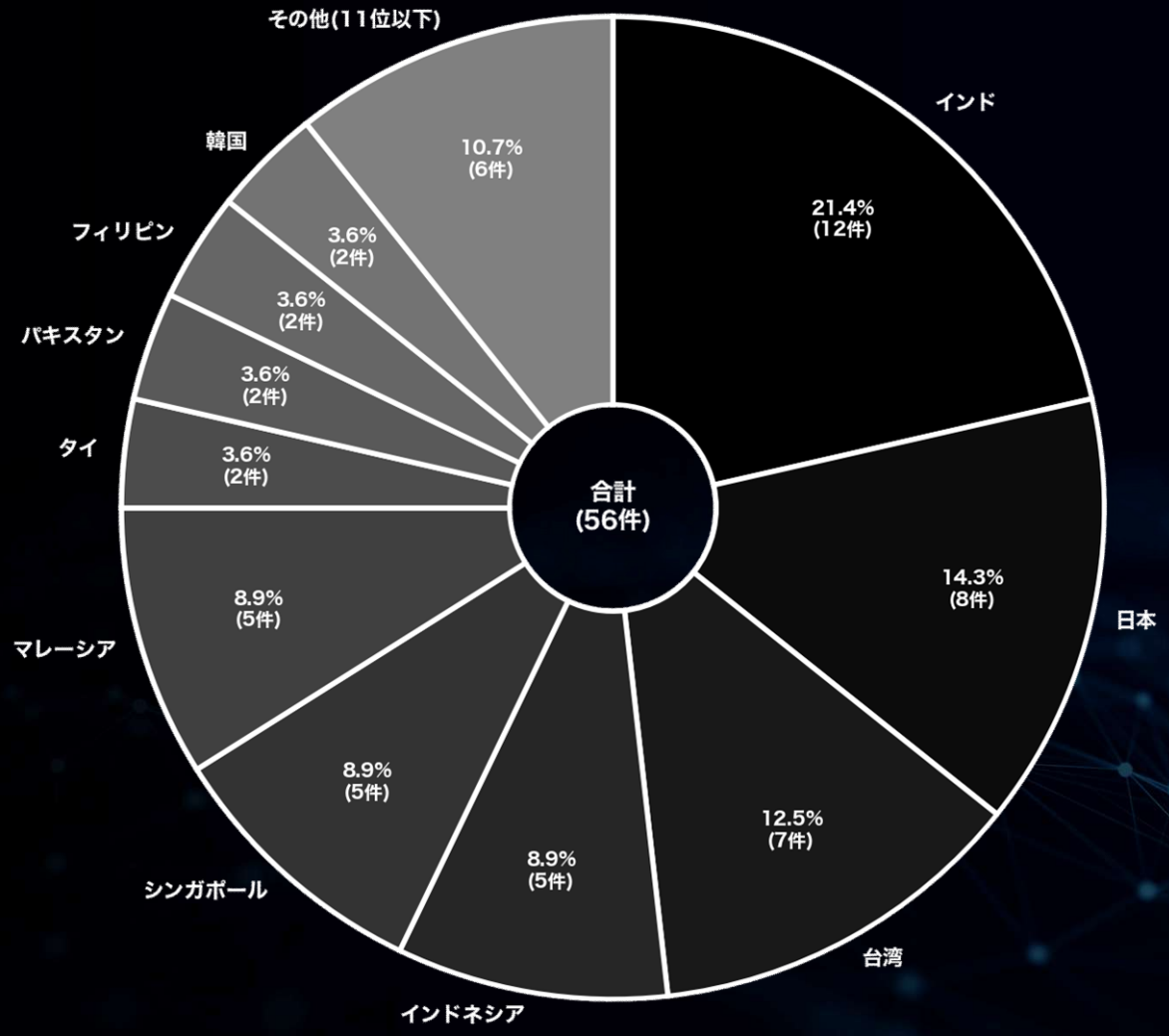
（2025年 2 月）

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	12	21.4	- 7
日本	8	14.3	+ 2
台湾	7	12.5	+ 6
インドネシア	5	8.9	+ 1
シンガポール	5	8.9	± 0
マレーシア	5	8.9	+ 1
タイ	2	3.6	- 3
パキスタン	2	3.6	- 2
フィリピン	2	3.6	+ 2
韓国	2	3.6	+ 1

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



※ 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

2025

2

業種 月別統計

（全世界） （過去3ヶ月分）

月別内訳 業種 TOP10（全世界）

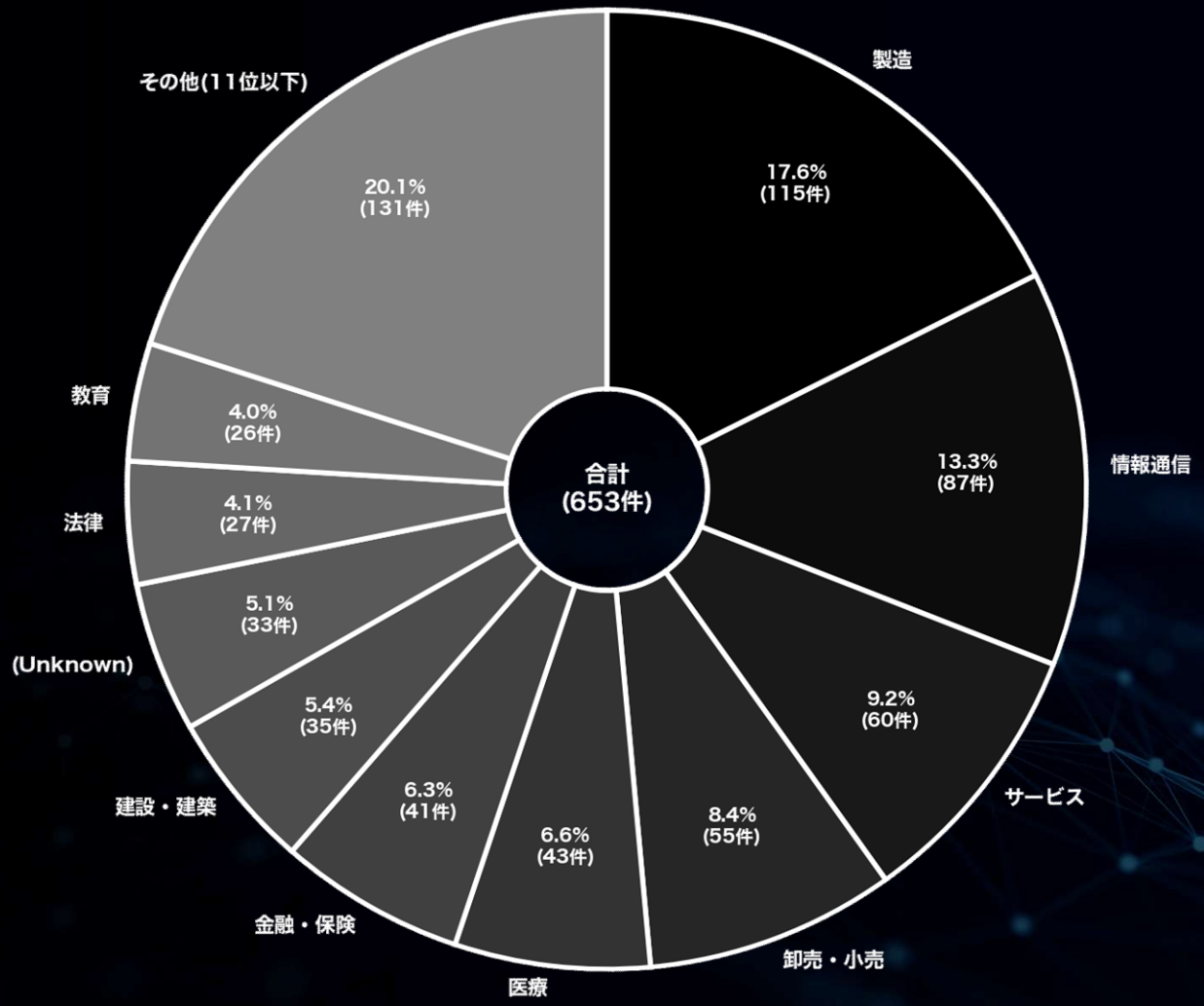
（2024年 12 月）

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	115	17.6	- 9
情報通信	87	13.3	+ 18
サービス	60	9.2	- 4
卸売・小売	55	8.4	+ 7
医療	43	6.6	- 14
金融・保険	41	6.3	+ 8
建設・建築	35	5.4	- 38
(Unknown)	33	5.1	+ 18
法律	27	4.1	+ 4
教育	26	4.0	- 10

▼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

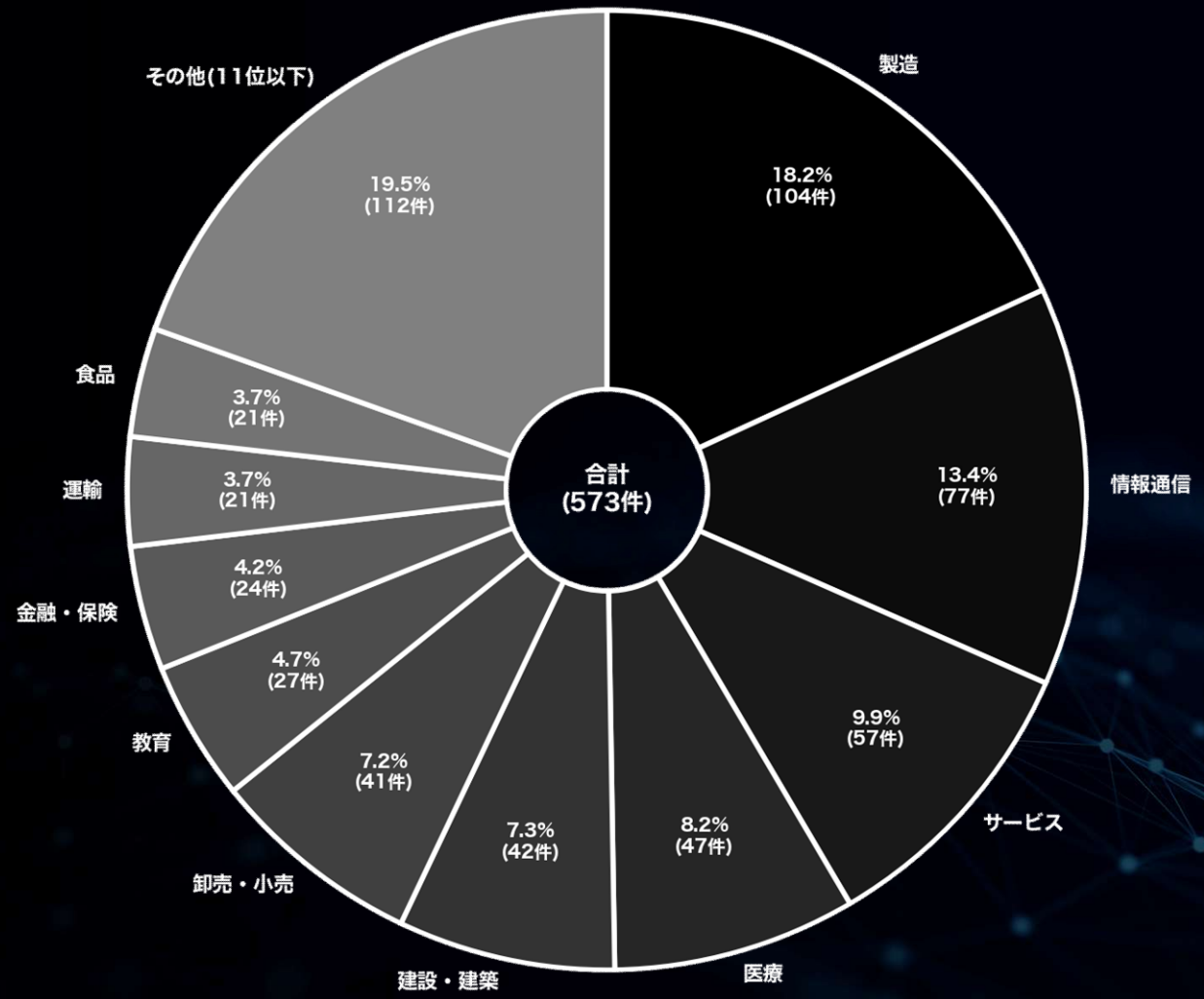
月別内訳 業種 TOP10（全世界）
（2025年 1 月）

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	104	18.2	- 11
情報通信	77	13.4	- 10
サービス	57	9.9	- 3
医療	47	8.2	+ 4
建設・建築	42	7.3	+ 7
卸売・小売	41	7.2	- 14
教育	27	4.7	+ 1
金融・保険	24	4.2	- 17
運輸	21	3.7	- 3
食品	21	3.7	+ 3

▼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（全世界）

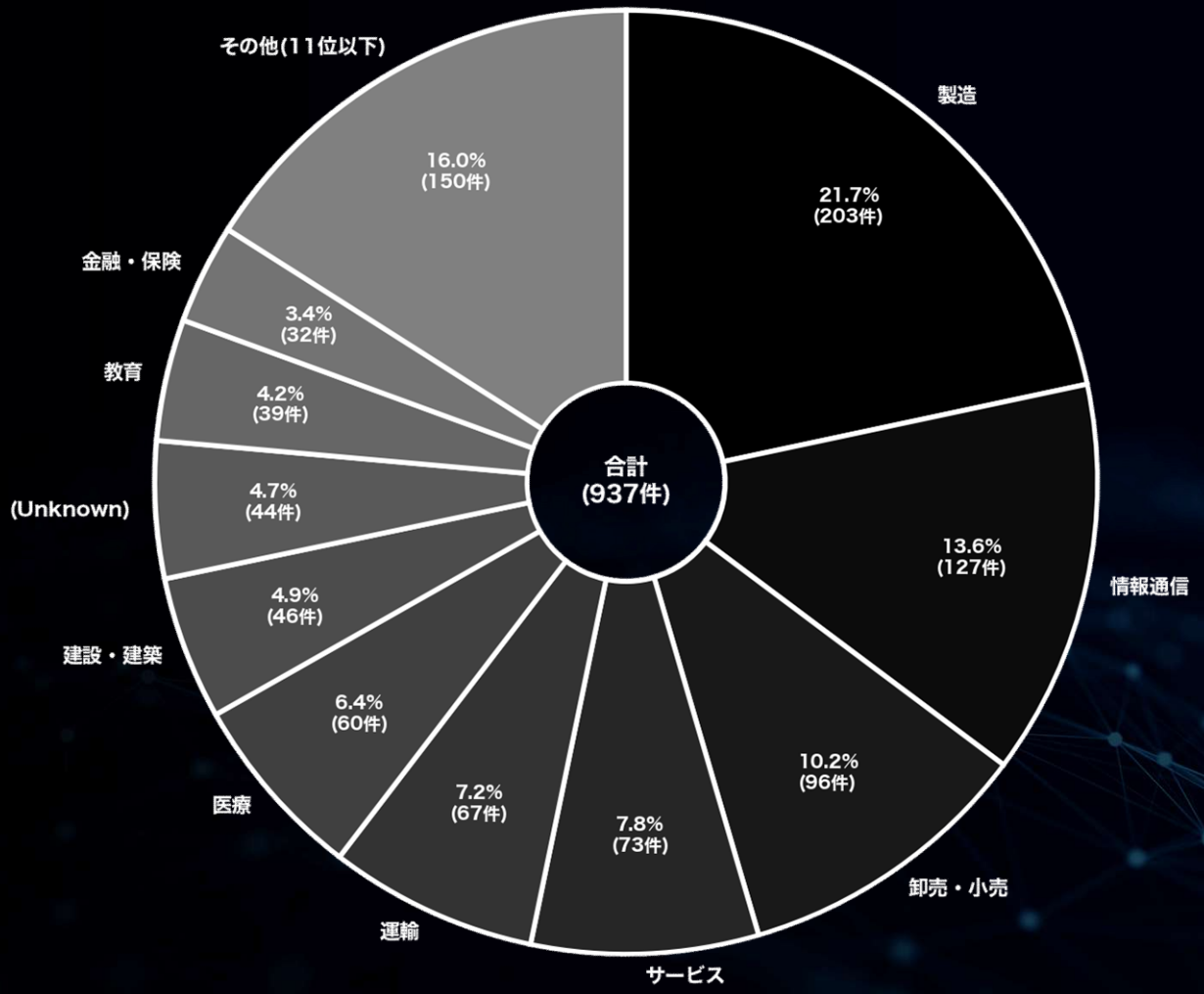
（2025年 2 月）

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	203	21.7	+ 99
情報通信	127	13.6	+ 50
卸売・小売	96	10.2	+ 55
サービス	73	7.8	+ 16
運輸	67	7.2	+ 46
医療	60	6.4	+ 13
建設・建築	46	4.9	+ 4
(Unknown)	44	4.7	+ 25
教育	39	4.2	+ 12
金融・保険	32	3.4	+ 8

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



※ 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

2025

2

被害数の推移に関する統計
（全世界及び国内）

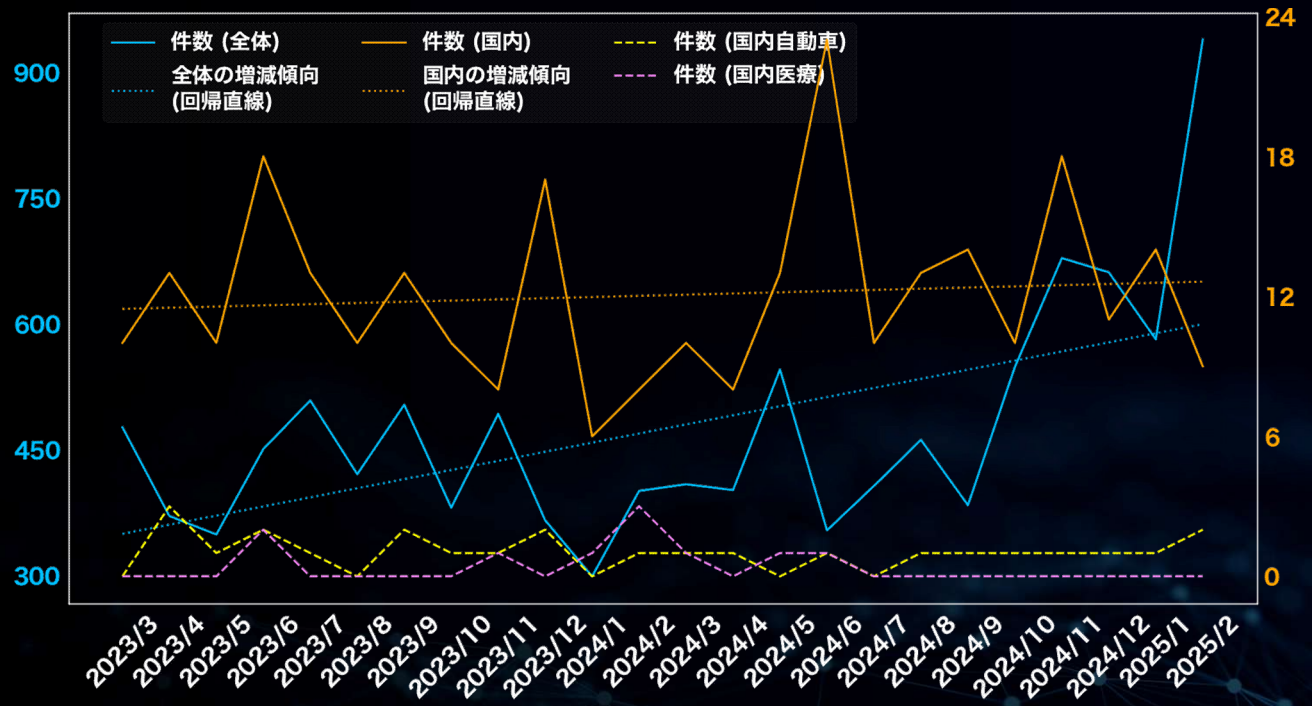
被害数の推移（全世界及び国内）
（過去2年間／2023年3月～2025年2月）

※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）
2023/3	476	10	0	0
2023/4	370	13	3	0
2023/5	348	10	1	0
2023/6	450	18	2	2
2023/7	508	13	1	0
2023/8	420	10	0	0
2023/9	503	13	2	0
2023/10	380	10	1	0
2023/11	492	8	1	1
2023/12	365	17	2	0
2024/1	298	6	0	1
2024/2	400	8	1	3
2024/3	408	10	1	1
2024/4	401	8	1	0
2024/5	545	13	0	1
2024/6	353	23	1	1
2024/7	406	10	0	0
2024/8	461	13	1	0
2024/9	383	14	1	0
2024/10	548	10	1	0
2024/11	678	18	1	0
2024/12	661	11	1	0
2025/1	581	14	1	0
2025/2	939	9	2	0
合計	11374	289	25	10

▼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）

2025

2

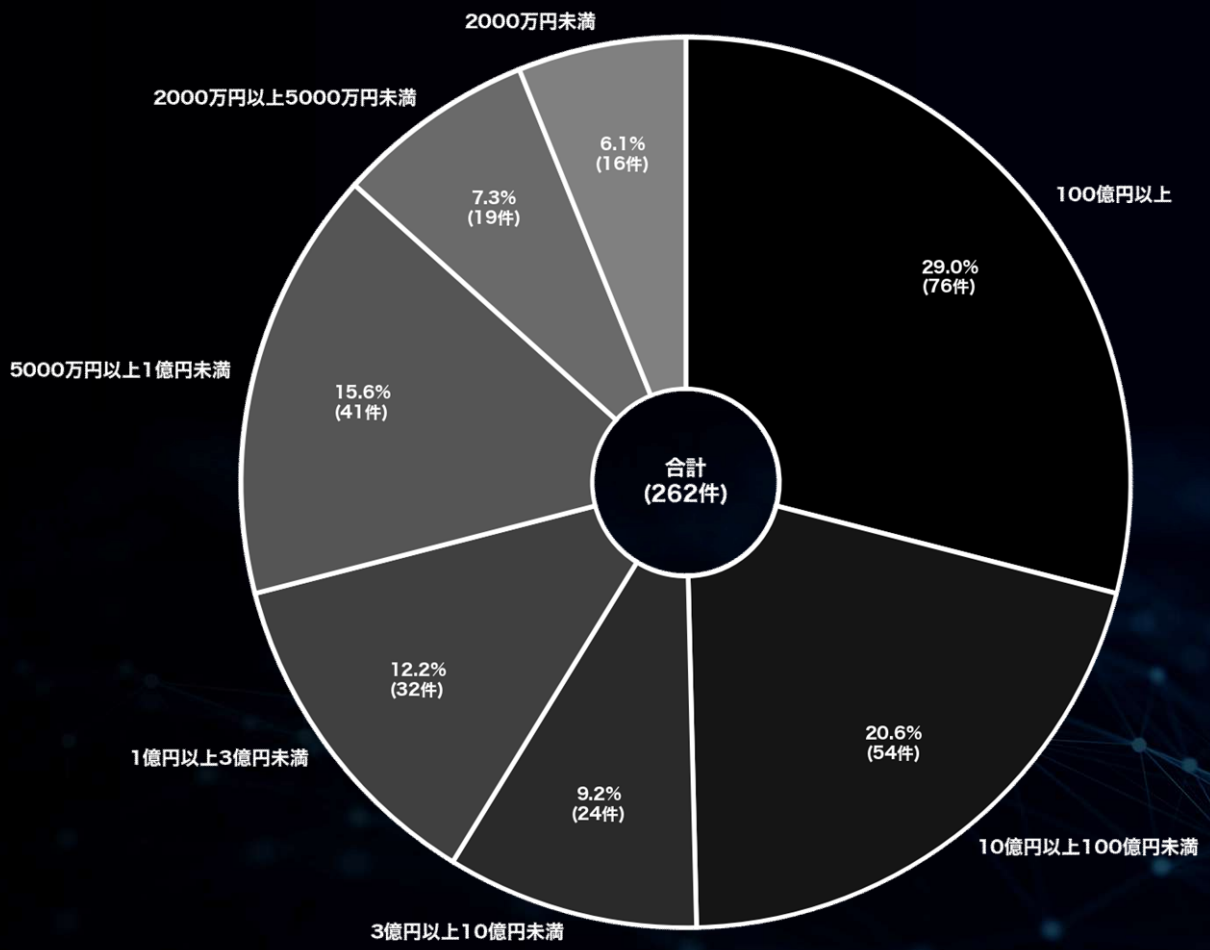
月別内訳 資本金別（国内）
（過去2年間／2023年3月～2025年2月）

Know your enemy. Defense leadership.

※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	76	29.0
10億円以上100億円未満	54	20.6
3億円以上10億円未満	24	9.2
1億円以上3億円未満	32	12.2
5000万円以上1億円未満	41	15.6
2000万円以上5000万円未満	19	7.3
2000万円未満	16	6.1

▼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）



中小企業に関する詳細な分析は
本レポート「中小企業における被害分析」を参照

（※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

2025

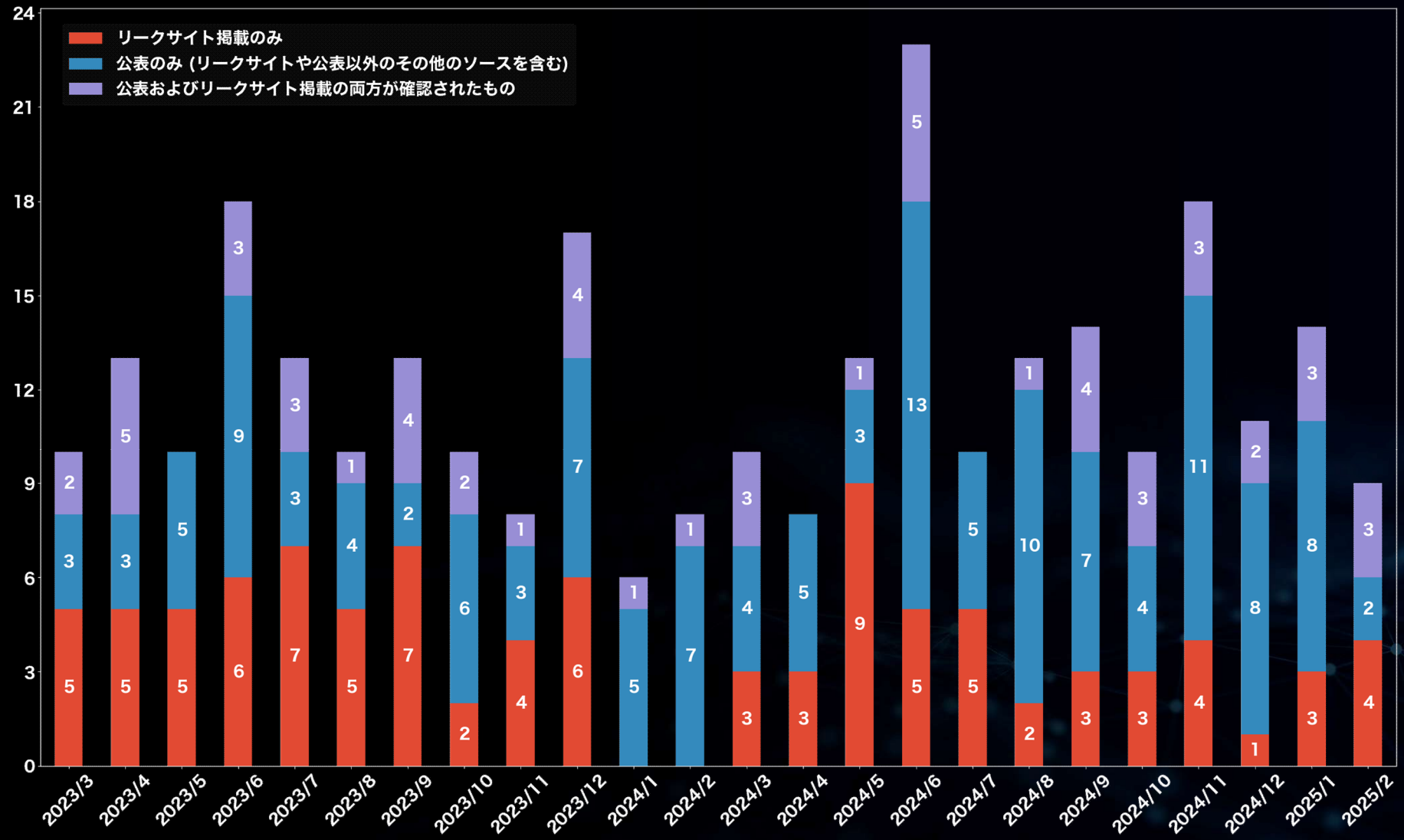
2

公表と暴露に関する統計
（国内）

公表割合 月別内訳（国内）

（過去2年間／2023年3月～2025年2月）

▼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

2025

2

公となった国内被害組織 概要一覧

公となった国内被害組織概要一覧（国内）
（過去1年間／2024年3月～2025年2月）

※（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	8BASE	自動車部品メーカー(海外拠点)
2024/3	LockBit	合成繊維製造会社
2024/3	LockBit	合成繊維製造会社
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	(Unknown)	不動産会社
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	(Unknown)	不動産管理会社

被害月	攻撃グループ	業種概要
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
2024/5	8BASE	税理士法人
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)	電子機器メーカー
2024/6	Phobos	総合ITサービス企業
2024/6	AKIRA	大手電機メーカー(海外拠点)
2024/6	(Unknown)	製薬会社
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	BlackSuit	大手出版社
2024/6	(Unknown)	総合会計・コンサルティンググループ
2024/6	(Unknown)	大手オフィス家具メーカー
2024/6	(Unknown)	通信機器販売業者
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	RS
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)	食品メーカー

被害月	攻撃グループ	業種概要
2024/6	(Unknown)	総合エンジニアリング会社
2024/6	(Unknown)	建設コンサルタント会社
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	Lockbit	レンタルサービス会社
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	(Unknown)	青果販売会社
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)
2024/8	(Unknown)	介護サービスプロバイダー
2024/8	Everest	精密機器メーカー(海外拠点)
2024/8	(Unknown)	システムインテグレーター
2024/8	(Unknown)	ペット用品メーカー
2024/8	(Unknown)	ヘルスケア用品メーカー
2024/8	(Unknown)	化学製品商社
2024/8	(Unknown)	海運技術ソリューションプロバイダー
2024/8	(Unknown)	学校法人
2024/8	(Unknown)	公益財団法人
2024/8	(Unknown)	保険サービスプロバイダー
2024/8	(Unknown)	電子機器メーカー
2024/8	Everest	大手化学メーカー
2024/8	RansomHub	大手自動車メーカー(海外拠点)
2024/9	RansomHub	アミューズメント機器メーカー

（※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（国内）
（過去1年間／2024年3月～2025年2月）

※（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
2024/9	Cicada3301	化学メーカー
2024/9	RansomHub	大手輸送用機器メーカー(海外拠点)
2024/9	(Unknown)	学校法人
2024/9	(Unknown)	情報通信サービス会社
2024/9	(Unknown)	物流サービス会社
2024/9	(Unknown)	物流サービス会社
2024/9	Brain Cipher	大手商社(海外拠点)
2024/9	(Unknown)	包装資材製造メーカー
2024/9	(Unknown)	食品輸入商社
2024/9	RansomHub	産業用機器メーカー
2024/9	RansomHub	産業ソリューションプロバイダー
2024/9	Medusa	情報通信サービス会社
2024/9	(Unknown)	保育サービスプロバイダー
2024/10	Qilin (Agenda)	空調機器メーカー(海外拠点)
2024/10	Underground	大手電機メーカー
2024/10	(Unknown)	公益財団法人
2024/10	SARCOMA	総合物流事業者
2024/10	MEOW	工具メーカー
2024/10	RansomHub	大手飲食サービス会社
2024/10	RansomHub	自動車部品メーカー
2024/10	(Unknown)	専門学校
2024/10	(Unknown)	総合商社
2024/10	(Unknown)	不動産会社
2024/11	KILLSEC	総合ゴム製品メーカー(海外拠点)
2024/11	(Unknown)	ソフトウエアメーカー
2024/11	(Unknown)	専門商社
2024/11	BianLian	大手スポーツ用品メーカー(海外拠点)
2024/11	BlackSuit	電子部品メーカー(海外拠点)
2024/11	(Unknown)	一般社団法人
2024/11	MEOW	電子部品メーカー(海外拠点)
2024/11	(Unknown)	家具メーカー
2024/11	(Unknown)	保険代理店
2024/11	SAFEPAY	建設会社
2024/11	(Unknown)	食品メーカー
2024/11	Argonauts	化学品メーカー
2024/11	(Unknown)	総合電機メーカー(海外拠点)
2024/11	(Unknown)	工作機械メーカー(海外拠点)
2024/11	(Unknown)	イベント企画制作会社
2024/11	(Unknown)	イベント企画制作会社
2024/11	BlackSuit	自動車部品メーカー(海外拠点)
2024/11	(Unknown)	水処理システムメーカー(海外拠点)
2024/12	(Unknown)	公益財団法人
2024/12	8BASE	農業機械メーカー
2024/12	PLAY	大手食品メーカー(海外拠点)
2024/12	(Unknown)	タンカー運送会社
2024/12	(Unknown)	鉄鋼加工メーカー
2024/12	(Unknown)	情報通信サービス会社
2024/12	(Unknown)	工業機械メーカー
2024/12	(Unknown)	教育委員会
2024/12	CL0P (CLOP)	大手食品メーカー(海外拠点)
2024/12	(Unknown)	印刷サービス会社
2024/12	(Unknown)	産業・建設機械メーカー
2025/1	(Unknown)	乳製品メーカー
2025/1	Hunters International	化学触媒メーカー
2025/1	(Unknown)	ソフトウエアメーカー
2025/1	Space Bears	不織布メーカー
2025/1	AKIRA	工業用繊維製品メーカー(海外拠点)
2025/1	Hunters International	大手香料メーカー(海外拠点)
2025/1	LYNX	輸入品卸売業(海外拠点)
2025/1	(Unknown)	総合美容商社
2025/1	(Unknown)	テーマパーク運営
2025/1	(Unknown)	保険代理店
2025/1	(Unknown)	報道関連会社
2025/1	(Unknown)	外航海運事業者
2025/1	(Unknown)	フッ素ポリマー製品製造
2025/1	Qilin (Agenda)	自動車部品メーカー
2025/2	Qilin (Agenda)	自動車部品メーカー
2025/2	Hunters International	住宅・施設建設
2025/2	FOG	ITサービス会社
2025/2	(Unknown)	保険代理店
2025/2	LYNX	ITサービス会社
2025/2	Cicada3301	システムインテグレーター
2025/2	(Unknown)	一般機械器具製造業
2025/2	Hunters International	緑化・造園業者
2025/2	CL0P (CLOP)	自動車部品メーカー

（※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（国内）

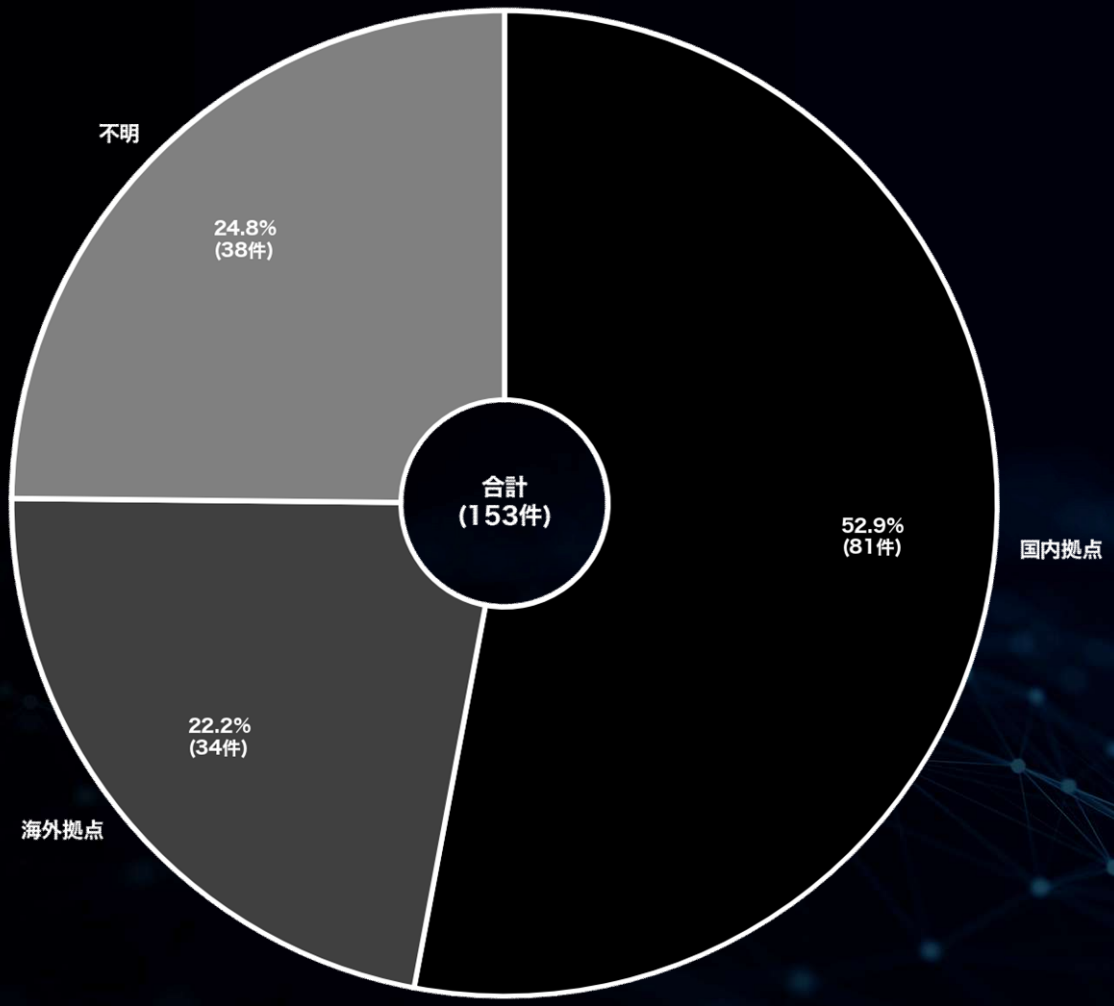
（過去1年間／2024年3月～2025年2月）

（※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	81	52.9
海外拠点	34	22.2
不明	38	24.8

▼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）

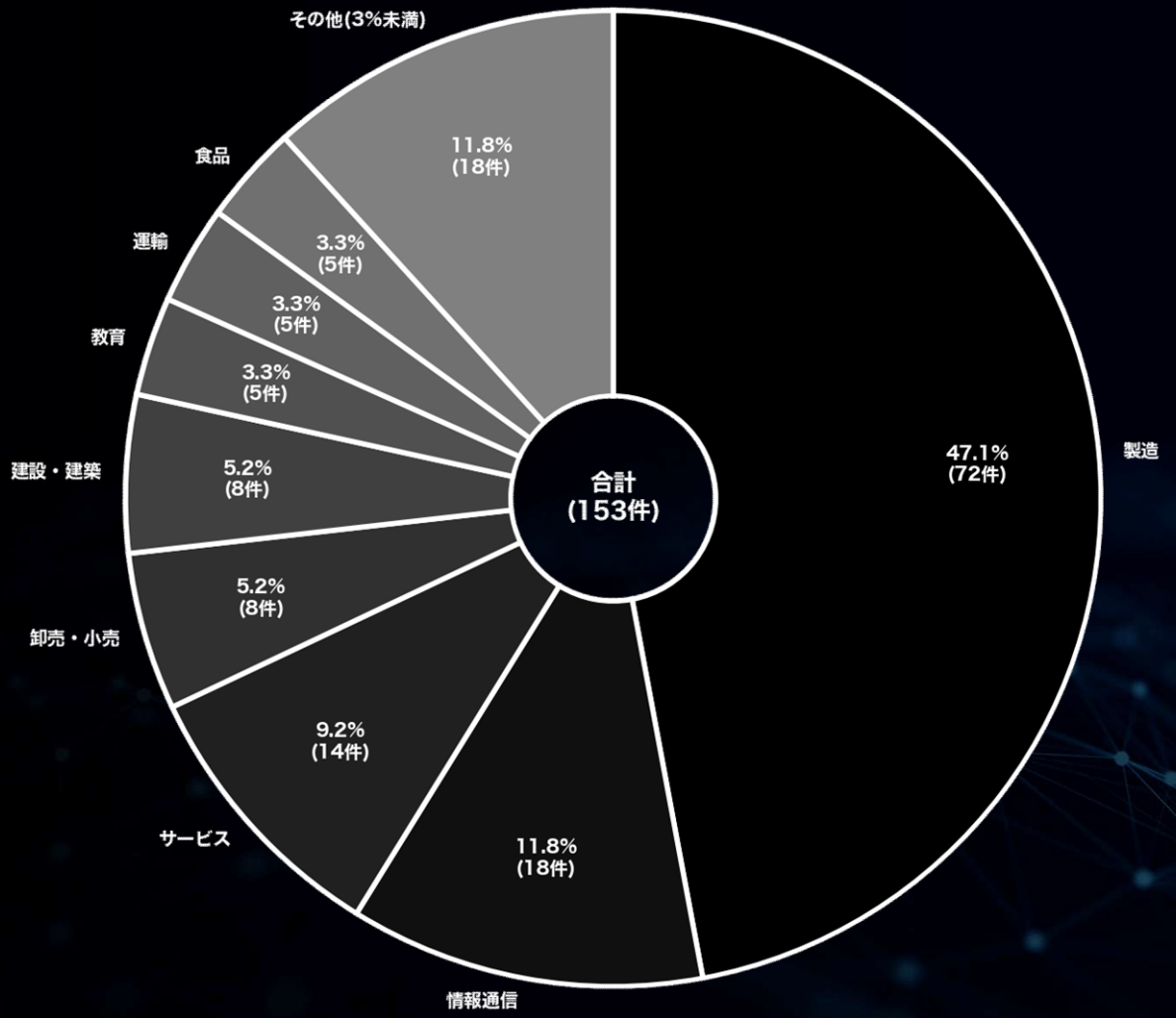
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

公となった国内被害組織における業種割合（国内）
（過去1年間／2024年3月～2025年2月）

Know your enemy.
Defense leadership.

業種	件数	割合(%)
製造	72	47.1
情報通信	18	11.8
サービス	14	9.2
卸売・小売	8	5.2
建設・建築	8	5.2
教育	5	3.3
運輸	5	3.3
食品	5	3.3
その他(3%未満)	18	11.8

▼ランサムウェア攻撃を受けた日本関連組織の業種別割合



（※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

2025

2

中小企業における被害分析
（国内）

中小企業の定義※は業種により法的に異なるが、本資料では中小企業を『資本金3億円未満の組織』と定義する。
※中小企業庁「中小企業・小規模企業者の定義」:https://www.chusho.meti.go.jp/soshiki/teigi.html

月別内訳 資本金別（国内-中小企業）

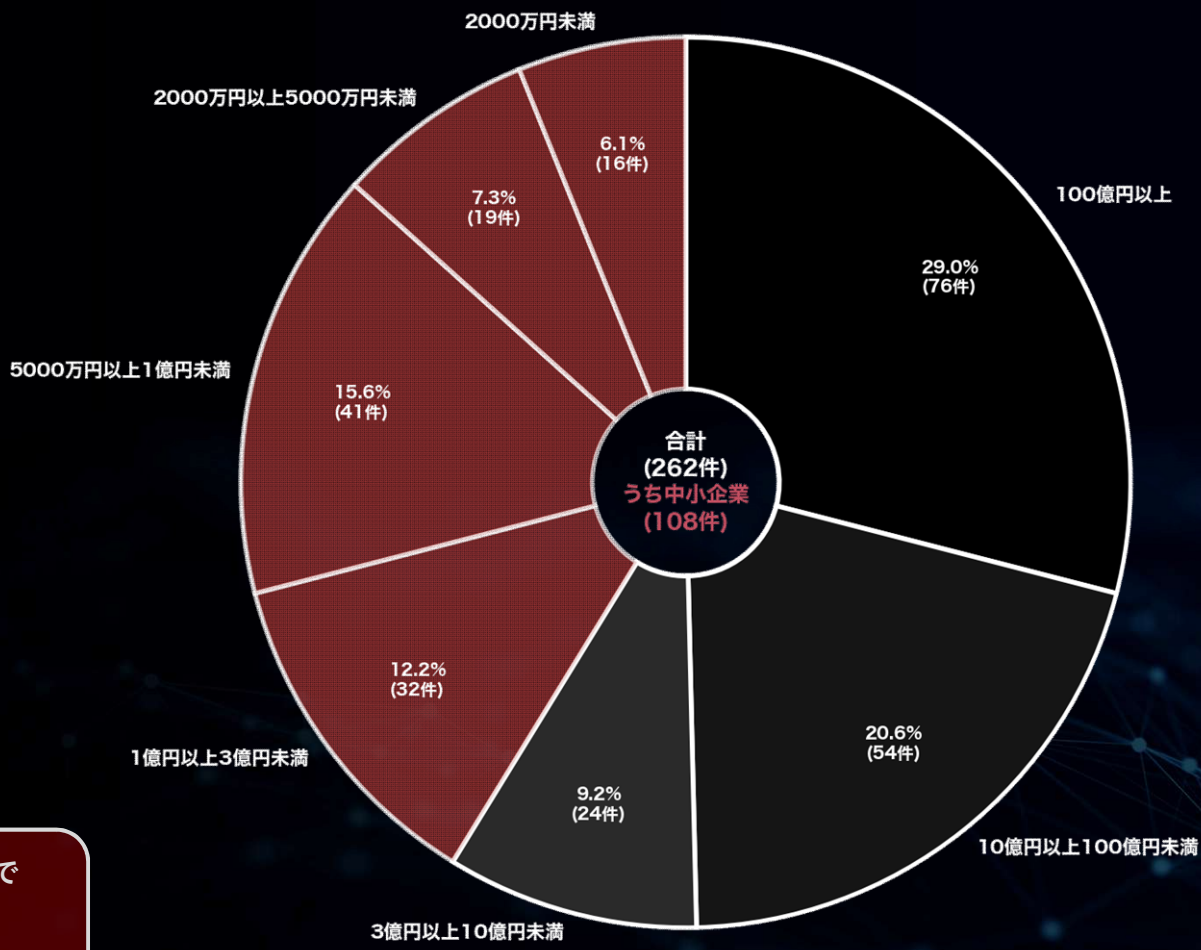
（過去2年間／2023年3月～2025年2月）

赤色は中小企業を示す

※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	76	29.0
10億円以上100億円未満	54	20.6
3億円以上10億円未満	24	9.2
1億円以上3億円未満	32	12.2
5000万円以上1億円未満	41	15.6
2000万円以上5000万円未満	19	7.3
2000万円未満	16	6.1

▼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）



日本関連組織の被害状況を見ると、中小企業の被害は過去2年間で108件にのぼり、全体の41.2%を占める。

これらの被害は、リークサイトへの掲載や公表から確認できたものだが、表面化していない被害も多数存在する可能性があり、実際の被害総数はさらに大きいと考えられる。

（※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）

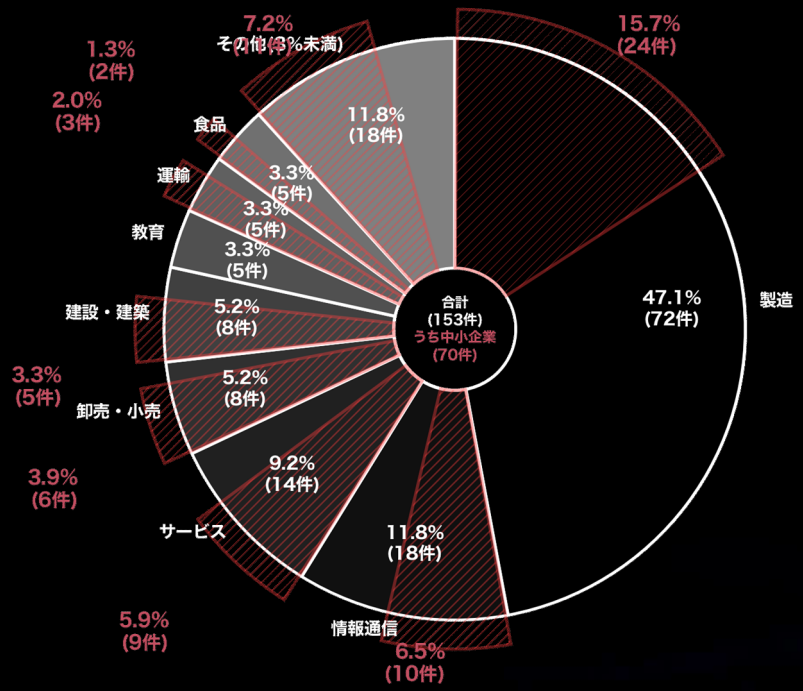
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

公となった国内被害組織における業種割合（国内-中小企業）

（過去1年間／2024年3月～2025年2月）

赤色は中小企業を示す

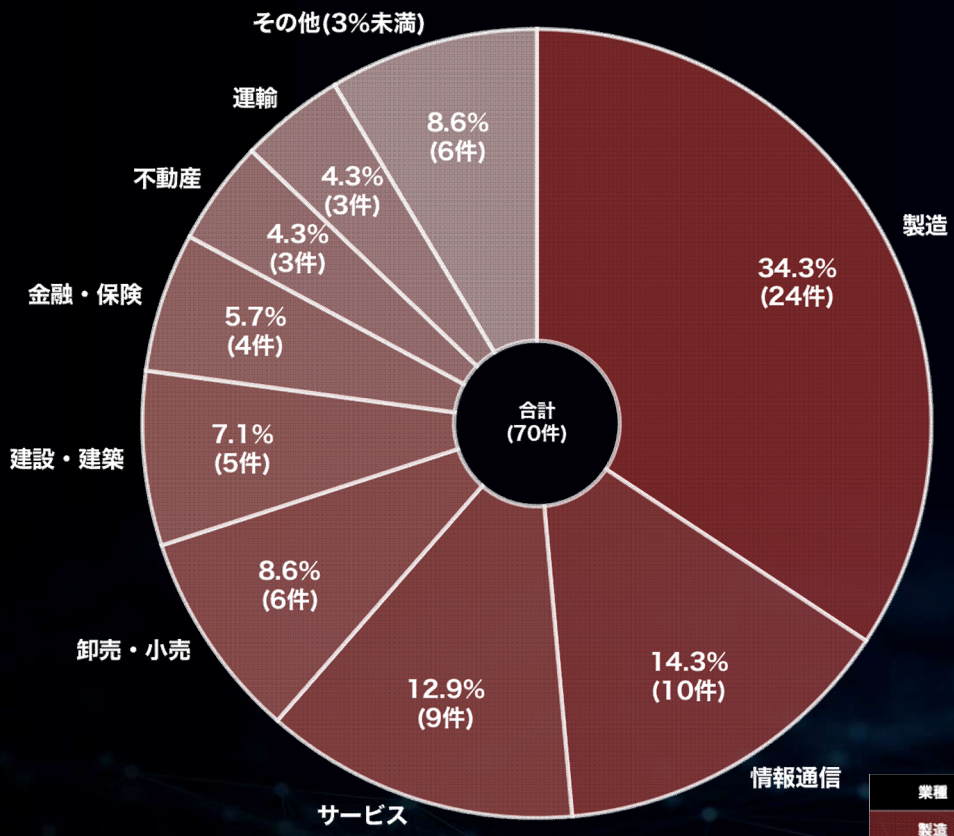
▼全体割合



※各数値の()内の数値は、資本金3億円未満の組織に対する集計結果を示す

業種	件数	割合(%)
製造	72 (24)	47.1 (15.7)
情報通信	18 (10)	11.8 (6.5)
サービス	14 (9)	9.2 (5.9)
卸売・小売	8 (6)	5.2 (3.9)
建設・建築	8 (5)	5.2 (3.3)
教育	5	3.3
運輸	5 (3)	3.3 (2.0)
食品	5 (2)	3.3 (1.3)
その他(3%未満)	18 (11)	11.8 (7.2)

▼中小企業のみの割合



業種	件数	割合(%)
製造	24	34.3
情報通信	10	14.3
サービス	9	12.9
卸売・小売	6	8.6
建設・建築	5	7.1
金融・保険	4	5.7
不動産	3	4.3
運輸	3	4.3
その他(3%未満)	6	8.6

過去1年間の業種別分析においては、中小企業のみに抜粋すると、被害件数の割合は業種問わず、より全体に分散していることがわかる。

※医療や教育、行政機関など資本金が不明な一部の組織については集計から除外

※ 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

（※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）

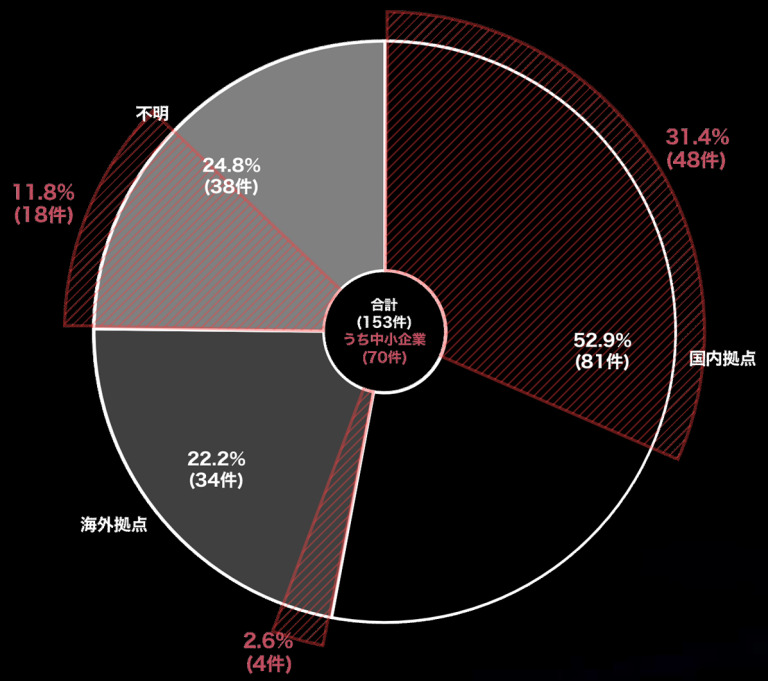
公となった国内被害組織における拠点割合（国内-中小企業）

（過去1年間／2024年3月～2025年2月）

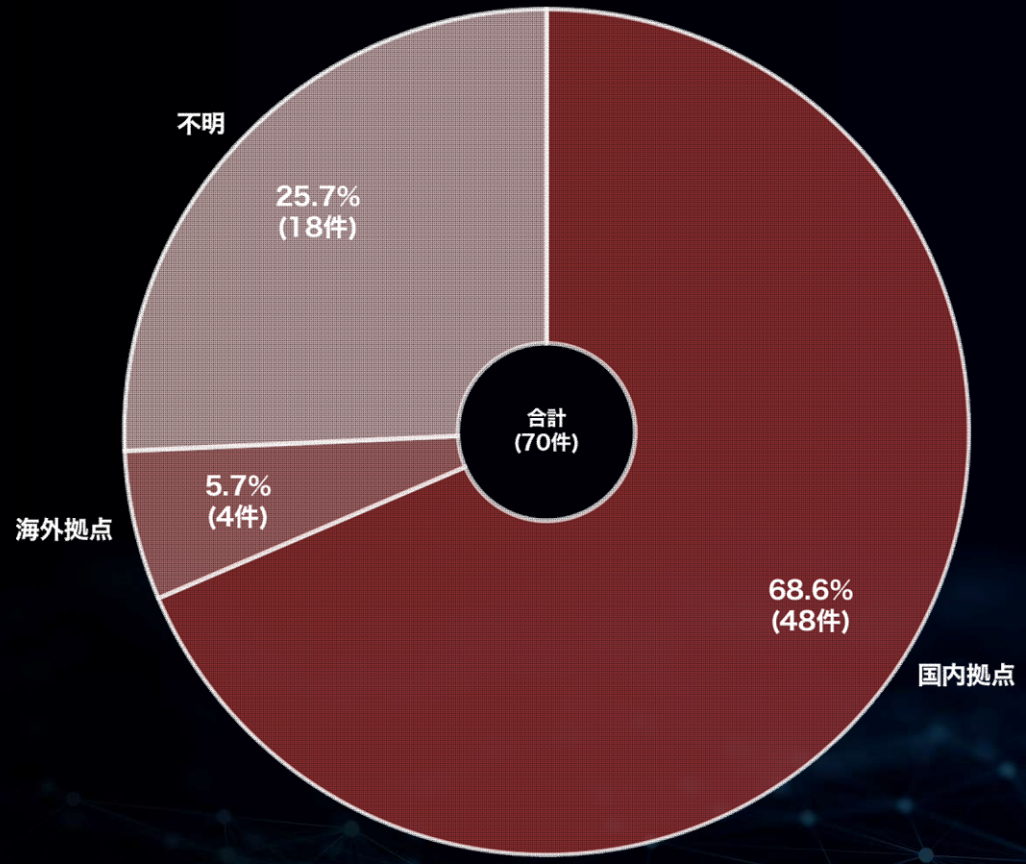
Know your enemy. Defense leadership.

赤色は中小企業を示す

▼全体割合



▼中小企業のみの割合



※
「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
※各数値の()内の数値は、資本金10億円未満の組織に対する集計結果を示す

拠点	件数 (中小企業)	割合(%)
国内拠点	81 (48)	52.9 (31.4)
海外拠点	34 (4)	22.2 (2.6)
不明	38 (18)	24.8 (11.8)
合計	153 (70)	100 (45.8)

過去1年間の被害拠点の分析では、中小企業の国内拠点における被害割合が、全体と比較して高い傾向にある。

※医療や教育、行政機関など資本金が不明な一部の組織については集計から除外

拠点	件数 (中小企業)	割合(%)
国内拠点	48	68.6
海外拠点	4	5.7
不明	18	25.7

※ 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

（※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）

公となった国内被害組織概要一覧（国内-中小企業）

（過去1年間／2024年3月～2025年2月）

赤色は中小企業を示す

Know your enemy. Defense leadership.

※（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	8BASE	自動車部品メーカー(海外拠点)
2024/3	LockBit	合成繊維製造会社
2024/3	LockBit	合成繊維製造会社
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	(Unknown)	不動産会社
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	(Unknown)	不動産管理会社

被害月	攻撃グループ	業種概要
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
2024/5	8BASE	税理士法人
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)	電子機器メーカー
2024/6	Phobos	総合ITサービス企業
2024/6	AKIRA	大手電機メーカー(海外拠点)
2024/6	(Unknown)	製薬会社
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	BlackSuit	大手出版社
2024/6	(Unknown)	総合会計・コンサルティンググループ
2024/6	(Unknown)	大手オフィス家具メーカー
2024/6	(Unknown)	通信機器販売業者
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	RS
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)	食品メーカー

被害月	攻撃グループ	業種概要
2024/6	(Unknown)	総合エンジニアリング会社
2024/6	(Unknown)	建設コンサルタント会社
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	Lockbit	レンタルサービス会社
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	(Unknown)	青果販売会社
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)
2024/8	(Unknown)	介護サービスプロバイダー
2024/8	Everest	精密機器メーカー(海外拠点)
2024/8	(Unknown)	システムインテグレーター
2024/8	(Unknown)	ペット用品メーカー
2024/8	(Unknown)	ヘルスケア用品メーカー
2024/8	(Unknown)	化学製品商社
2024/8	(Unknown)	海運技術ソリューションプロバイダー
2024/8	(Unknown)	学校法人
2024/8	(Unknown)	公益財団法人
2024/8	(Unknown)	保険サービスプロバイダー
2024/8	(Unknown)	電子機器メーカー
2024/8	Everest	大手化学メーカー
2024/8	RansomHub	大手自動車メーカー(海外拠点)
2024/9	RansomHub	アミューズメント機器メーカー

（※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（国内-中小企業）

（過去1年間／2024年3月～2025年2月）

赤色は中小企業を示す

※（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
2024/9	Cicada3301	化学メーカー
2024/9	RansomHub	大手輸送用機器メーカー(海外拠点)
2024/9	(Unknown)	学校法人
2024/9	(Unknown)	情報通信サービス会社
2024/9	(Unknown)	物流サービス会社
2024/9	(Unknown)	物流サービス会社
2024/9	Brain Cipher	大手商社(海外拠点)
2024/9	(Unknown)	包装資材製造メーカー
2024/9	(Unknown)	食品輸入商社
2024/9	RansomHub	産業用機器メーカー
2024/9	RansomHub	産業ソリューションプロバイダー
2024/9	Medusa	情報通信サービス会社
2024/9	(Unknown)	保育サービスプロバイダー
2024/10	Qilin (Agenda)	空調機器メーカー(海外拠点)
2024/10	Underground	大手電機メーカー
2024/10	(Unknown)	公益財団法人
2024/10	SARCOMA	総合物流事業者
2024/10	MEOW	工具メーカー
2024/10	RansomHub	大手飲食サービス会社
2024/10	RansomHub	自動車部品メーカー
2024/10	(Unknown)	専門学校
2024/10	(Unknown)	総合商社
2024/10	(Unknown)	不動産会社
2024/11	KILLSEC	総合ゴム製品メーカー(海外拠点)
2024/11	(Unknown)	ソフトウエアメーカー
2024/11	(Unknown)	専門商社
2024/11	BianLian	大手スポーツ用品メーカー(海外拠点)
2024/11	BlackSuit	電子部品メーカー(海外拠点)
2024/11	(Unknown)	一般社団法人
2024/11	MEOW	電子部品メーカー(海外拠点)
2024/11	(Unknown)	家具メーカー
2024/11	(Unknown)	保険代理店
2024/11	SAFEPAY	建設会社
2024/11	(Unknown)	食品メーカー
2024/11	Argonauts	化学品メーカー
2024/11	(Unknown)	総合電機メーカー(海外拠点)
2024/11	(Unknown)	工作機械メーカー(海外拠点)
2024/11	(Unknown)	イベント企画制作会社
2024/11	(Unknown)	イベント企画制作会社
2024/11	BlackSuit	自動車部品メーカー(海外拠点)
2024/11	(Unknown)	水処理システムメーカー(海外拠点)
2024/12	(Unknown)	公益財団法人
2024/12	8BASE	農業機械メーカー
2024/12	PLAY	大手食品メーカー(海外拠点)
2024/12	(Unknown)	タンカー運送会社
2024/12	(Unknown)	鉄鋼加工メーカー
2024/12	(Unknown)	情報通信サービス会社
2024/12	(Unknown)	工業機械メーカー
2024/12	(Unknown)	教育委員会
2024/12	CLOP (CLOP)	大手食品メーカー(海外拠点)
2024/12	(Unknown)	印刷サービス会社
2024/12	(Unknown)	産業・建設機械メーカー
2025/1	(Unknown)	乳製品メーカー
2025/1	Hunters International	化学触媒メーカー
2025/1	(Unknown)	ソフトウエアメーカー
2025/1	Space Bears	不織布メーカー
2025/1	AKIRA	工業用繊維製品メーカー(海外拠点)
2025/1	Hunters International	大手香料メーカー(海外拠点)
2025/1	LYNX	輸入品卸売業(海外拠点)
2025/1	(Unknown)	総合美容商社
2025/1	(Unknown)	テーマパーク運営
2025/1	(Unknown)	保険代理店
2025/1	(Unknown)	報道関連会社
2025/1	(Unknown)	外航海運事業者
2025/1	(Unknown)	フッ素ポリマー製品製造
2025/1	Qilin (Agenda)	自動車部品メーカー
2025/2	Qilin (Agenda)	自動車部品メーカー
2025/2	Hunters International	住宅・施設建設
2025/2	FOG	ITサービス会社
2025/2	(Unknown)	保険代理店
2025/2	LYNX	ITサービス会社
2025/2	Cicada3301	システムインテグレーター
2025/2	(Unknown)	一般機械器具製造業
2025/2	Hunters International	緑化・造園業者
2025/2	CLOP (CLOP)	自動車部品メーカー

過去1年間、中小企業でのランサムウェア被害が継続的に発生している状況が確認されている。特に近年の国内事例では、取引先企業にまで被害が広がるサプライチェーン攻撃が見受けられる。各企業の事業継続性を守ると同時に、サプライチェーン全体の安全性を高めるため、企業規模に関わらずセキュリティ対策を日々アップデートしていくことが望ましい。

※二次被害を受けた被害組織については本資料に記載していない

（※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）

※ 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

2025

2

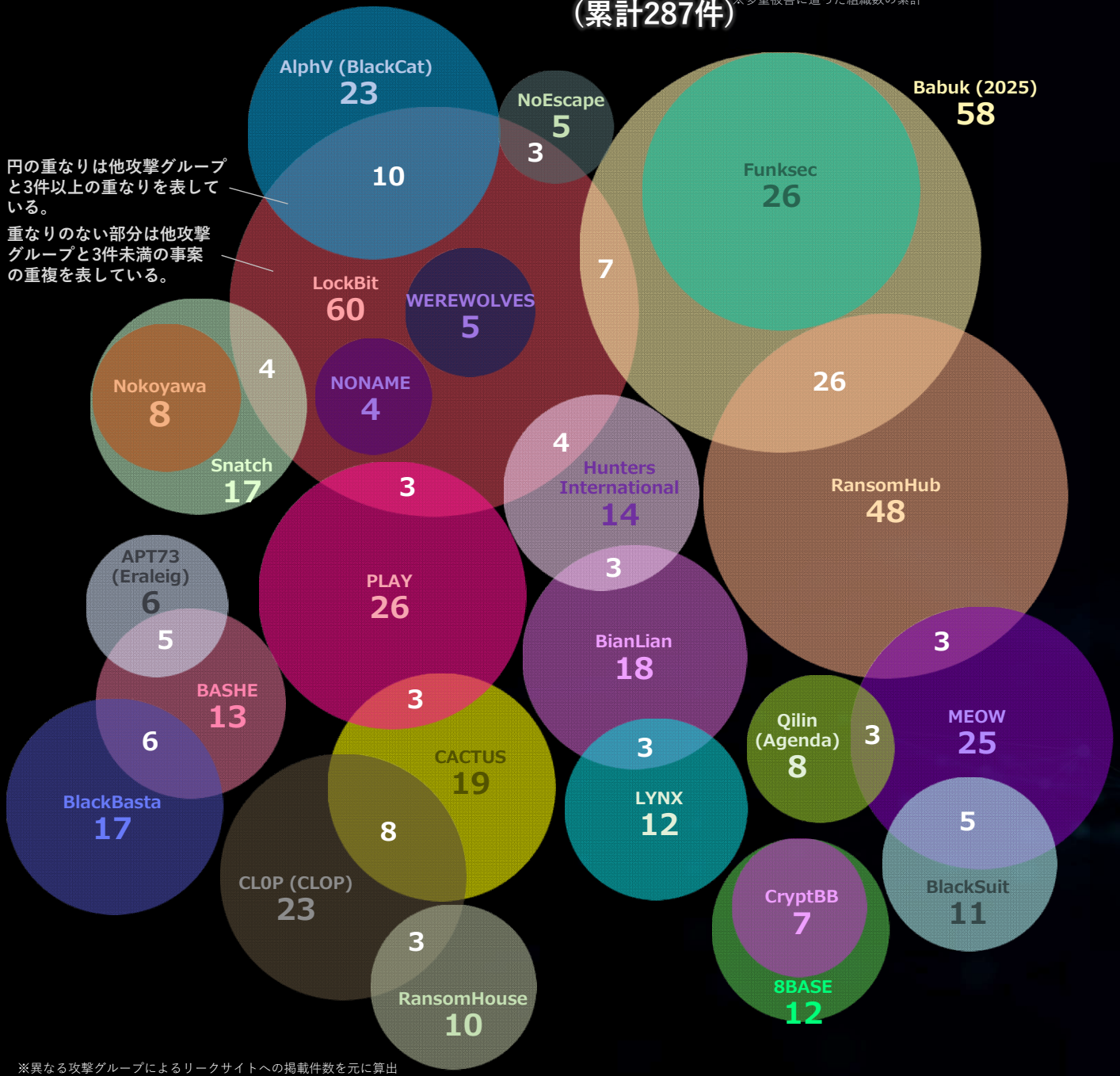
多重被害に関する分析

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（全世界）

（累計287件）※多重被害に遭った組織数の累計

※ 円の重なりは他攻撃グループと3件以上の重なりを表している。

※ 重なりのない部分は他攻撃グループと3件未満の事案の重複を表している。



※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。

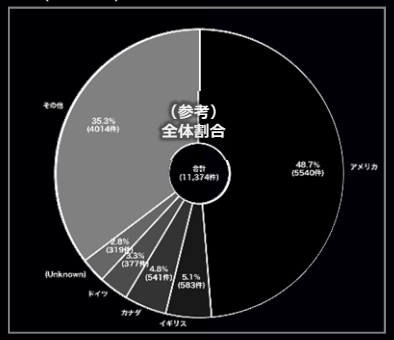
一度盗まれたデータの流用を完全に防ぐことは困難だが、複数回の侵入による多重被害は、インシデント発生時の適切な対応とその後の対策により、防御の可能性を大幅に高めることができる。
ランサムウェア被害発生を想定し、有事の際に冷静な対応ができるよう、対策のための情報の一つとして多重被害の実態を把握しておくことも重要である。

多重被害に遭った被害組織の傾向と分析（全世界）

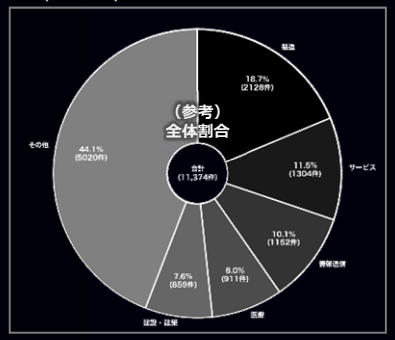
（過去2年間／2023年3月～2025年2月）

※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

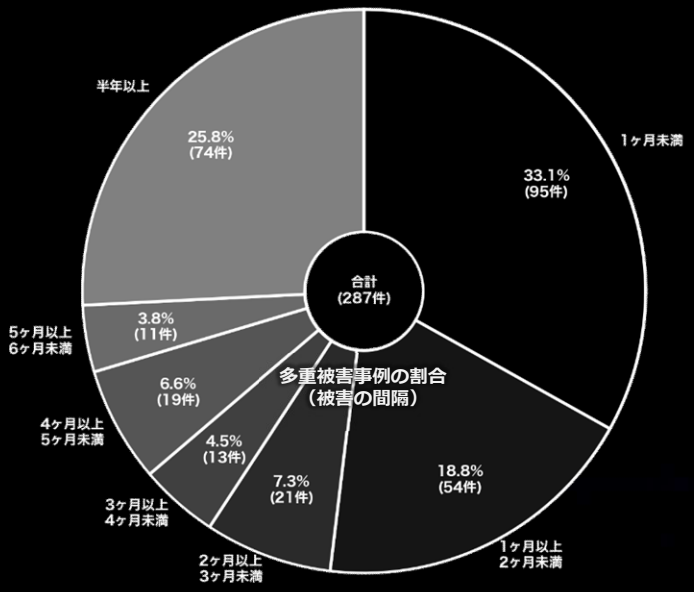


（参考比較）同期間の全データにおける割合

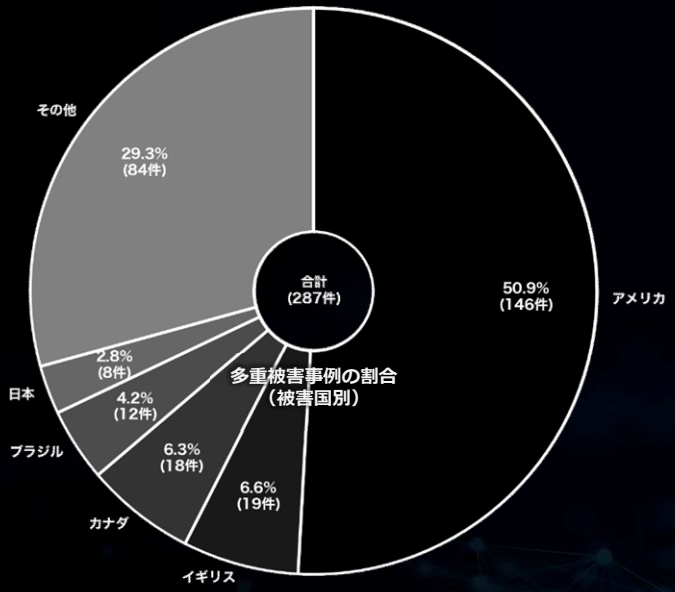


▼被害の間隔

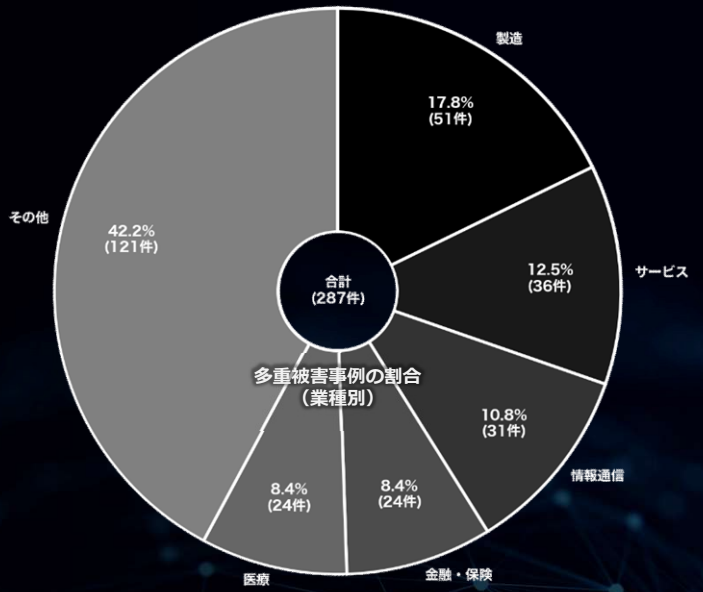
（一度目の被害から二度目の被害までの間隔）



▼被害国別



▼業種別



▶多重被害に遭った組織数の累計：287件（全体11374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

2025

2

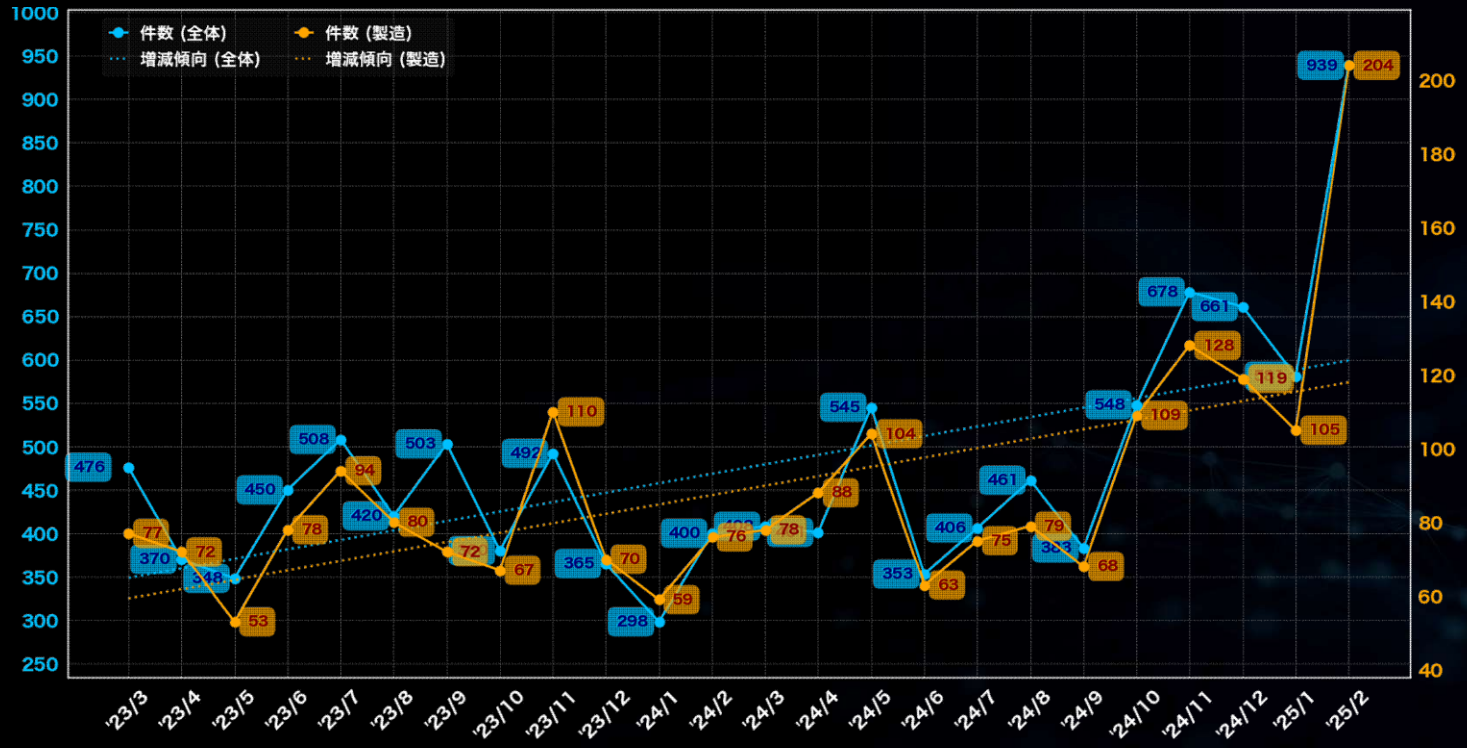
業種に関する分析

（過去2年間のリークサイト掲載上位10業種）

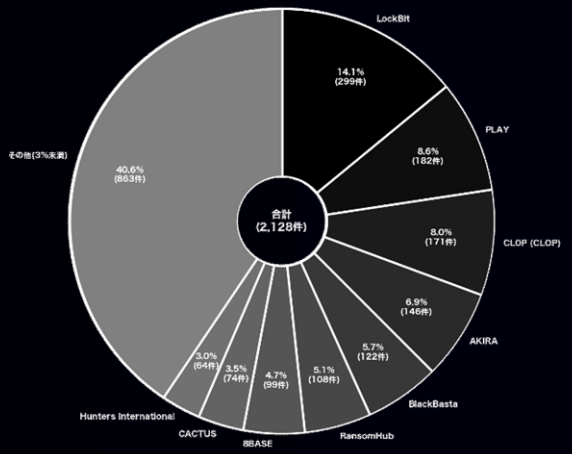
業種に関する分析（全世界）
（過去2年間／2023年3月～2025年2月）

製造

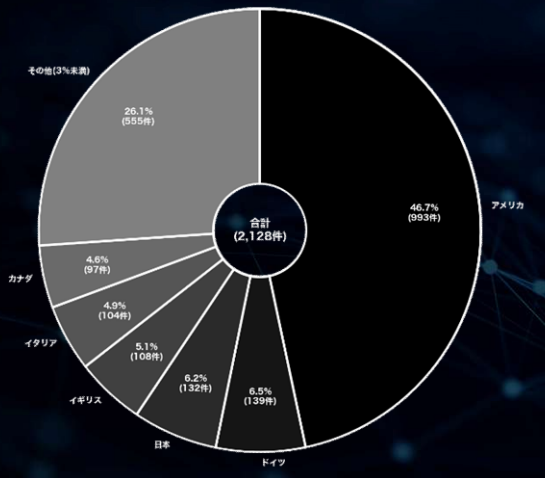
「製造」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、204件の掲載があった。一方、最も少なかった月は2023年5月で、53件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いで日本とドイツがそれぞれ約7%と約6%である。攻撃グループについては、少なくとも100のグループが関与しており、特に「LockBit」が299件のリークサイト掲載を実施している。次いで「PLAY」と「CL0P (CLOP)」がそれぞれ182件と171件の掲載を行っている。製造関連の件数は全体件数に対して高い割合で推移しており、全体件数を引き上げている。全世界的に被害が多い業種であるが、日本関連組織においても多くの被害が出ている状況や、長期に渡り増加傾向にあることから、今後も国内外問わず被害が増加する可能性がある。



▼攻撃グループ別



▼国別



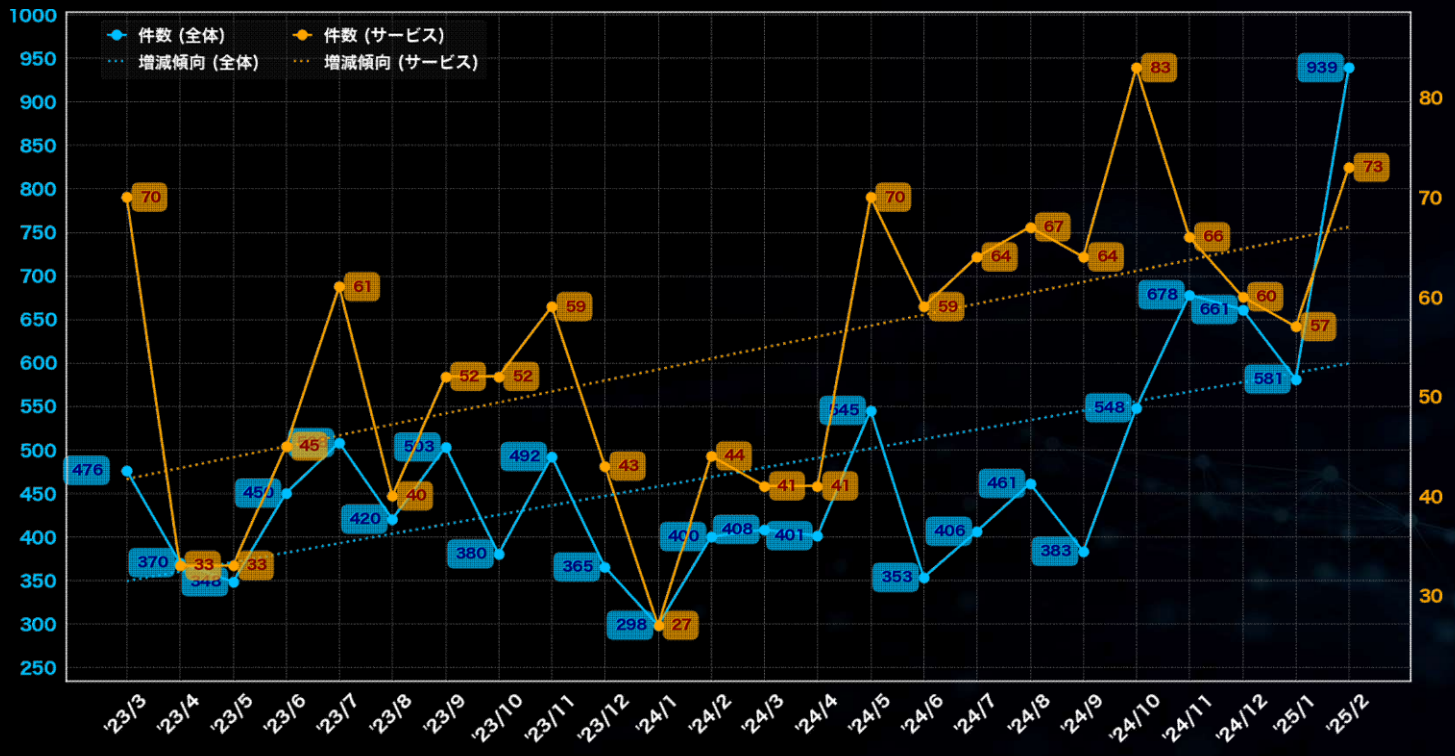
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

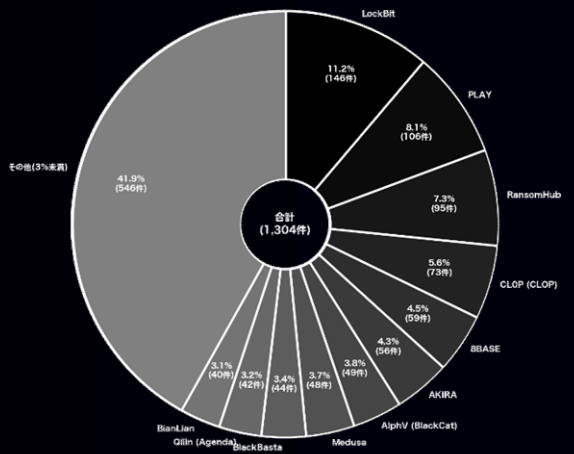
業種に関する分析（全世界）
（過去2年間／2023年3月～2025年2月）

サービス

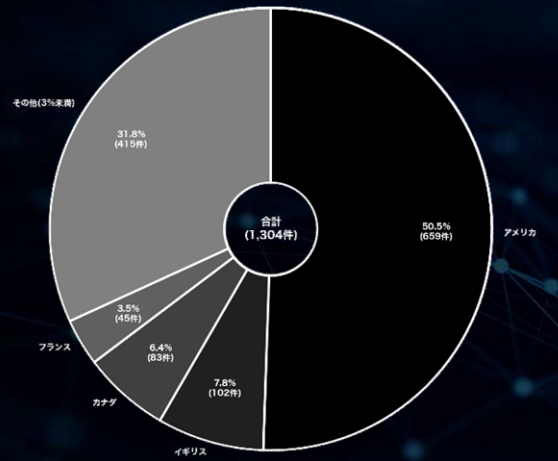
「サービス」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2024年10月で、83件の掲載があった。一方、最も少なかった月は2024年1月で、27件であった。被害組織の所在国の割合では、アメリカが約51%と最も多く、次いでイギリスとカナダがそれぞれ約8%と約6%である。攻撃グループについては、少なくとも92のグループが関与しており、特に「LockBit」が146件のリークサイト掲載を実施している。次いで「PLAY」と「RansomHub」がそれぞれ106件と95件の掲載を行っている。サービス関連の件数は製造関連と同じく全体件数に対し、高い割合をキープしており、年々その割合は高まっている。



▼攻撃グループ別



▼国別



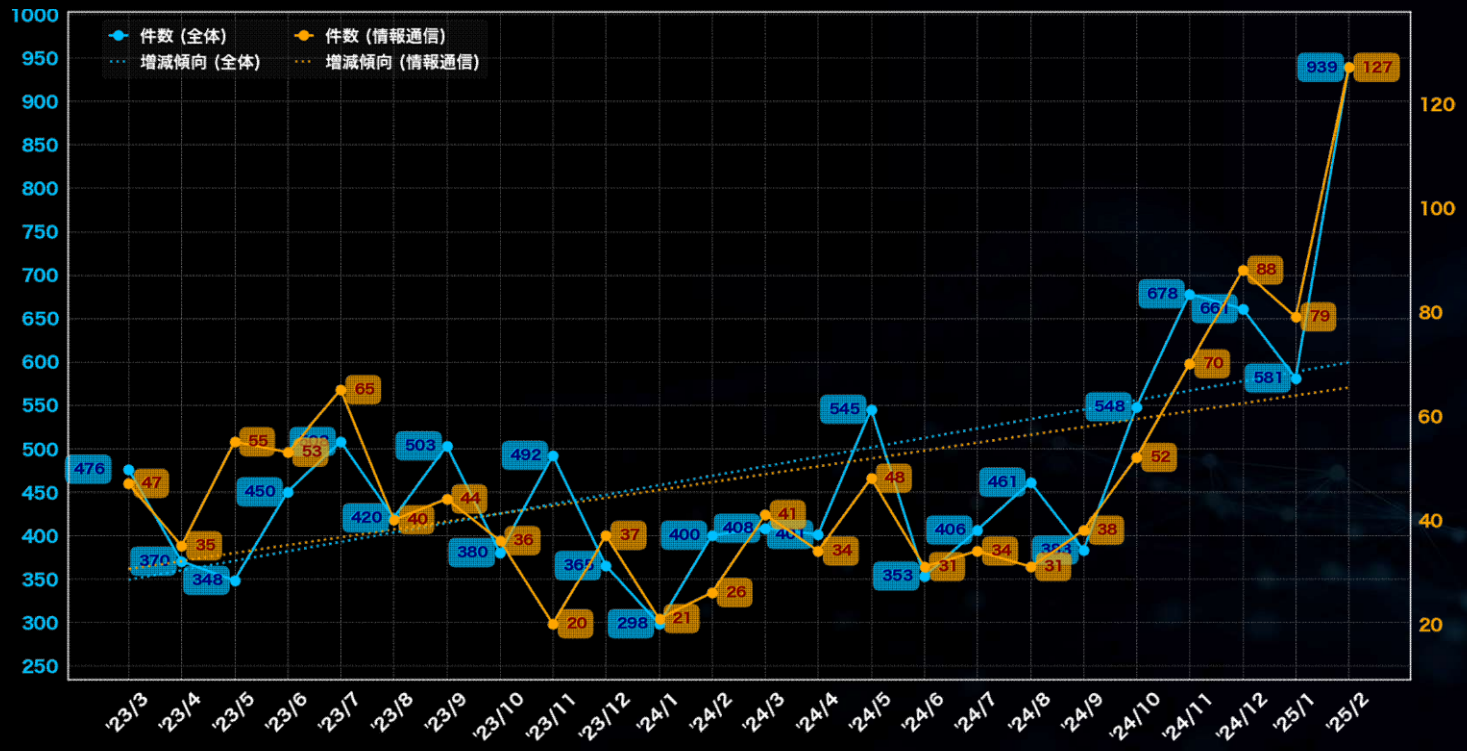
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

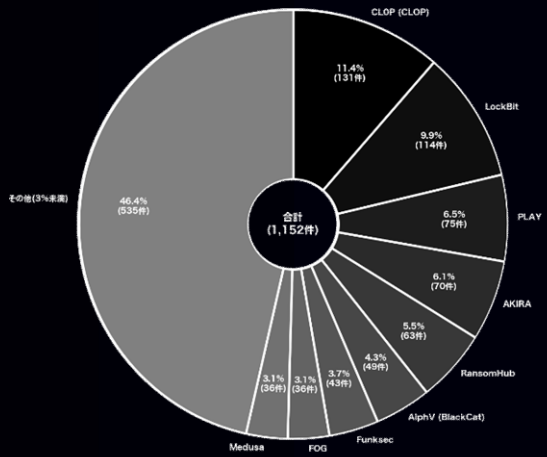
業種に関する分析（全世界）
（過去2年間／2023年3月～2025年2月）

情報通信

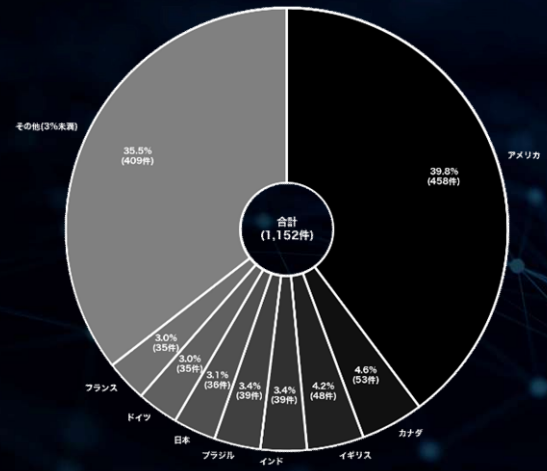
「情報通信」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、127件の掲載があった。一方、最も少なかった月は2023年11月で、20件であった。被害組織の所在国の割合では、アメリカが約40%と最も多く、次いでイギリスとカナダがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも91のグループが関与しており、特に「CL0P (CLOP)」が131件のリークサイト掲載を実施している。次いで「LockBit」と「PLAY」がそれぞれ114件と75件の掲載を行っている。過去2年間におけるリークサイト掲載件数の上位2種である「製造」、「サービス」と比較すると緩やかではあるが、増加傾向にある。



▼攻撃グループ別



▼国別



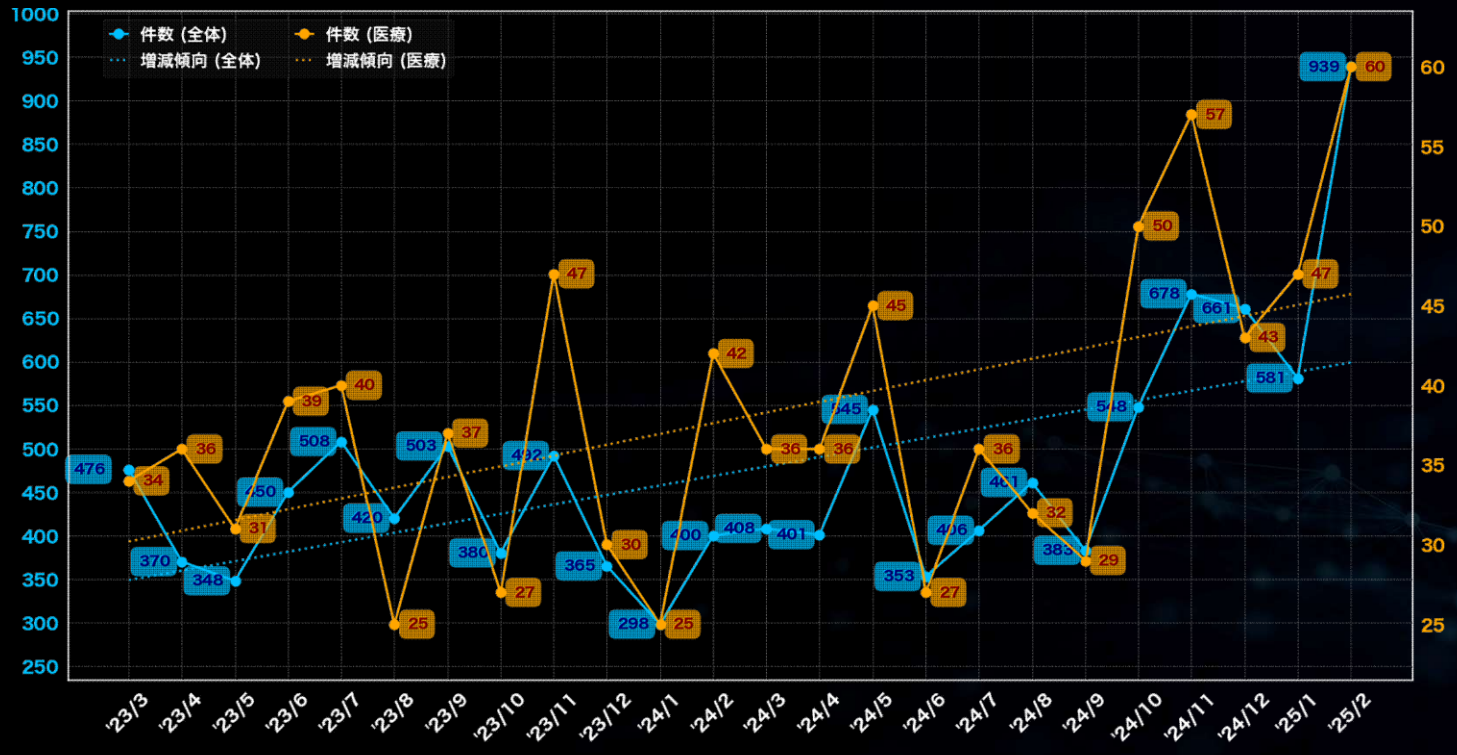
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

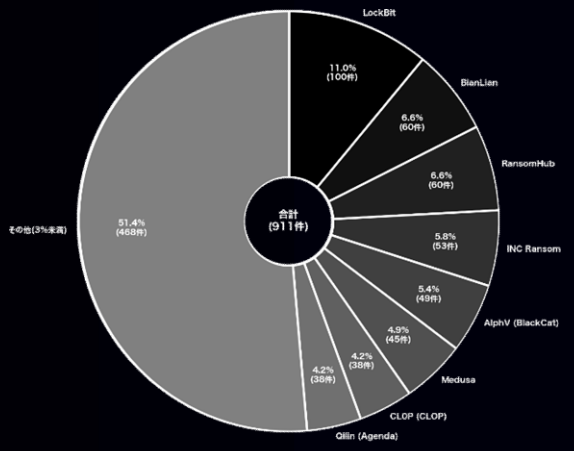
業種に関する分析（全世界）
（過去2年間／2023年3月～2025年2月）

医療

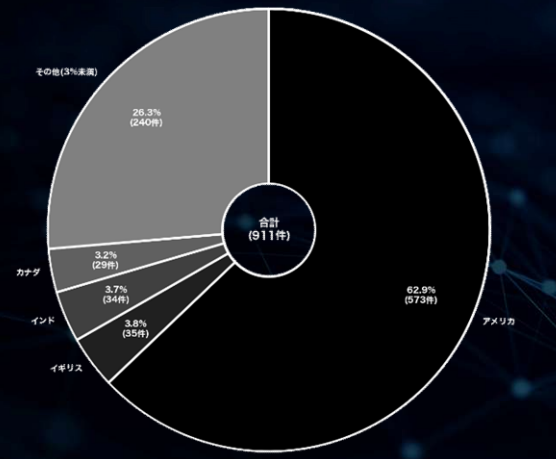
「医療」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、60件の掲載があった。一方、最も少なかった月は2023年8月および2024年1月で、25件であった。被害組織の所在国の割合では、アメリカが約63%と最も多く、次いでイギリス、インドがそれぞれ約4%である。攻撃グループについては、少なくとも83のグループが関与しており、特に「LockBit」が100件のリークサイト掲載を実施している。次いで「BianLian」と「INC Ransom」がそれぞれ60件の掲載を行っている。かつては低水準だった医療関連の被害数は2023年3月頃に増加し、その後も高い水準が維持が継続している。この変化の背景には、攻撃グループが生存競争の中で業種を問わない攻撃へと方針を転換していった可能性も否定できない。また、国別に見る傾向としてアメリカにおける被害が非常に高い割合を占めている点が顕著である。



▼攻撃グループ別



▼国別



（※本ページの「掲載件数」には、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含んでいる）

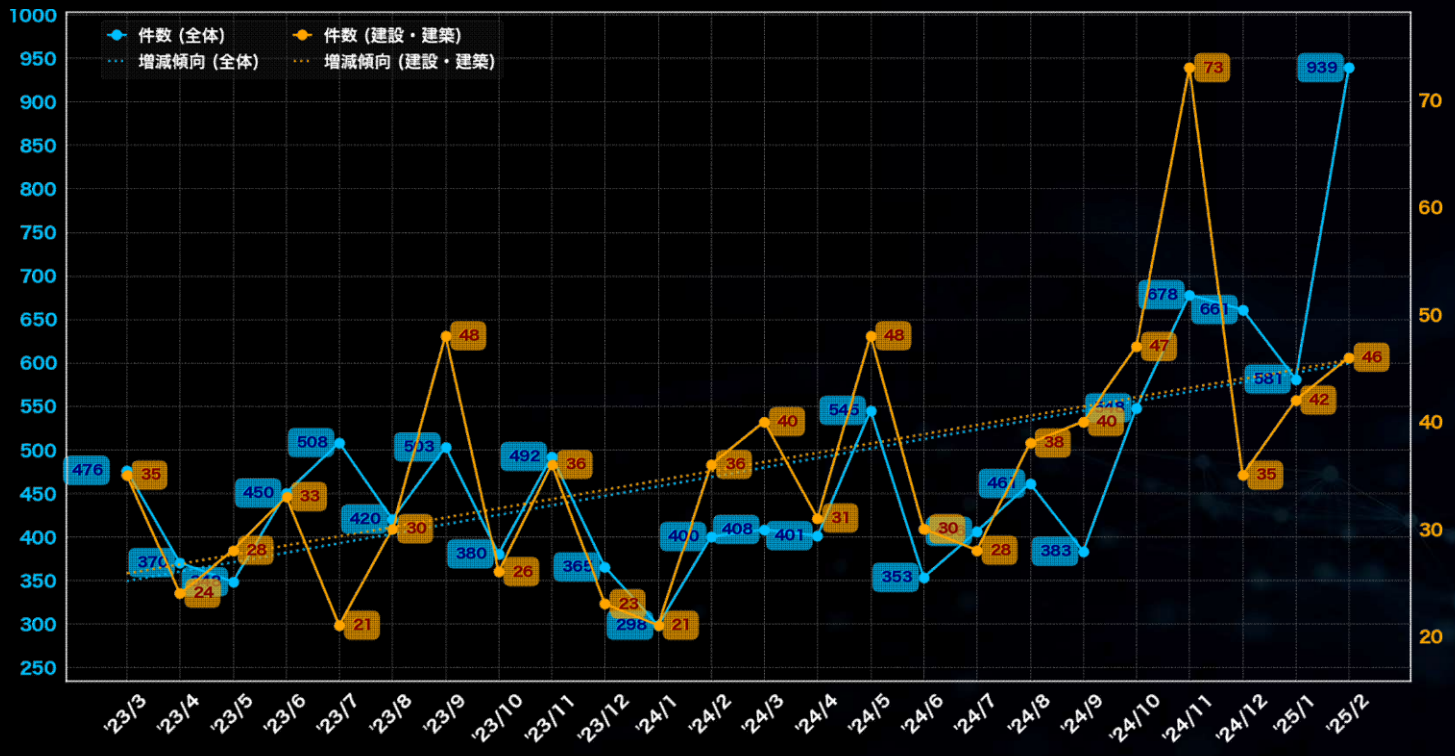
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

業種に関する分析（全世界）
（過去2年間／2023年3月～2025年2月）

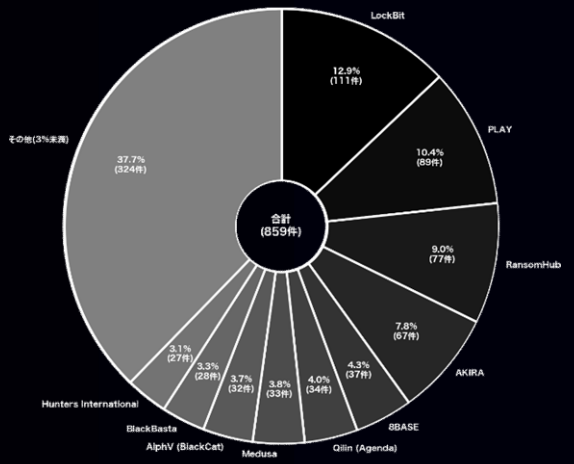
Know your enemy. Defense leadership.

建設・建築

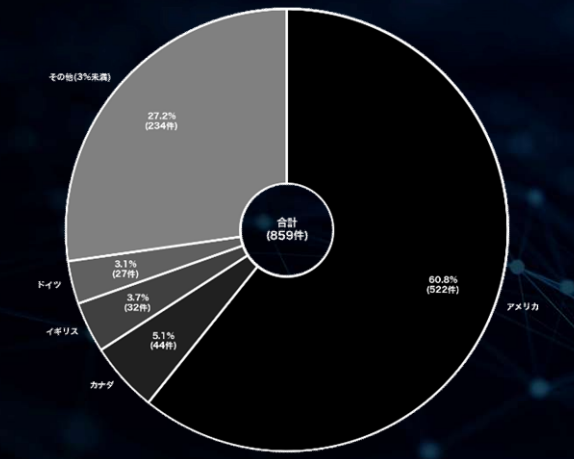
「建設・建築」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2024年11月で、73件の掲載があった。一方、最も少なかった月は2023年7月および2024年1月で、21件であった。被害組織の所在国の割合では、アメリカが約61%と最も多く、次いでカナダとイギリスがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも79のグループが関与しており、特に「LockBit」が111件のリークサイト掲載を実施している。次いで「PLAY」と「RansomHub」がそれぞれ89件と77件の掲載を行っている。建設・建築関連の被害数は高い水準を維持しており、引き続き増加傾向にある。製造関連などと比べると件数は少ないものの、全体件数とほぼ同様の上昇傾向を見せている。



▼攻撃グループ別



▼国別



（※本ページの「掲載件数」には、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含んでいる）

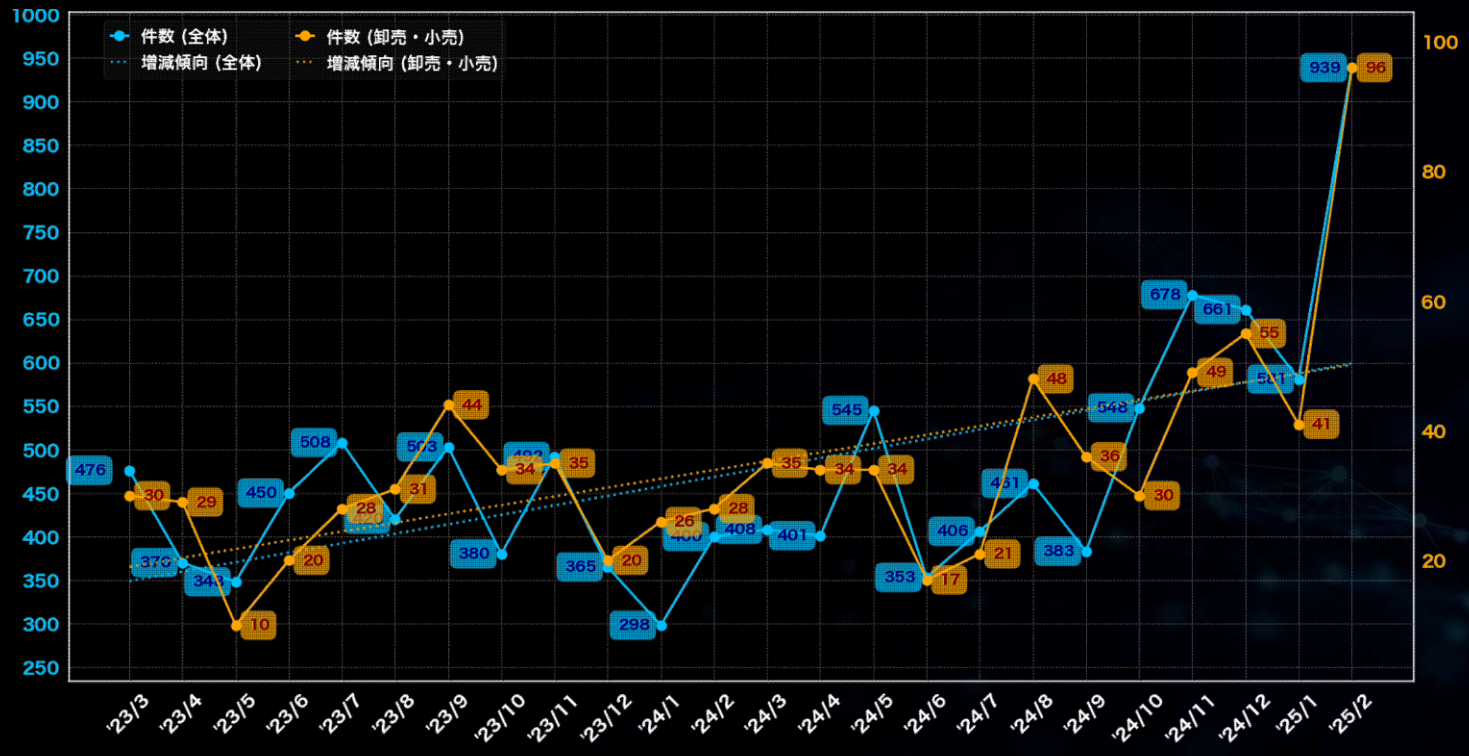
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

業種に関する分析（全世界）
（過去2年間／2023年3月～2025年2月）

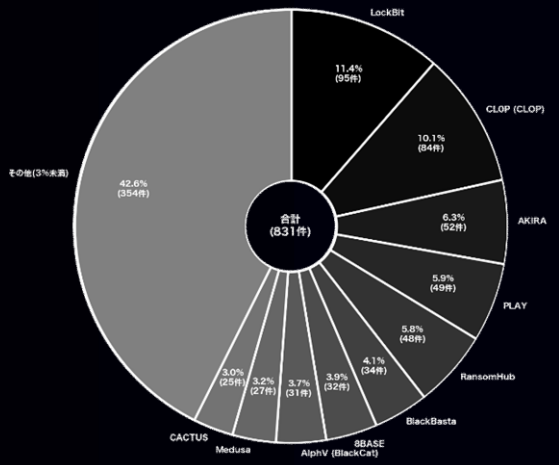
Know your enemy. Defense leadership.

卸売・小売

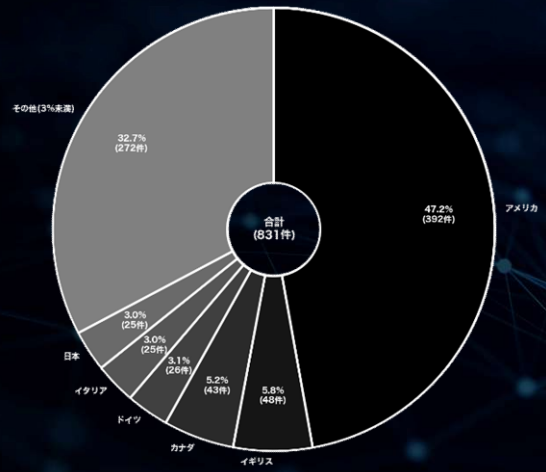
「卸売・小売」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、96件の掲載があった。一方、最も少なかった月は2023年5月で、10件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いでイギリスとカナダがそれぞれ約6%と約5%である。攻撃グループについては、少なくとも80のグループが関与しており、特に「LockBit」が95件のリークサイト掲載を実施している。次いで「CL0P (CLOP)」と「AKIRA」がそれぞれ84件と52件の掲載を行っている。卸売・小売関連は大きな増減の波があるものの、過去2年間の推移としては明確な増加傾向がある。



▼攻撃グループ別



▼国別



（※本ページの「掲載件数」には、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含んでいる）

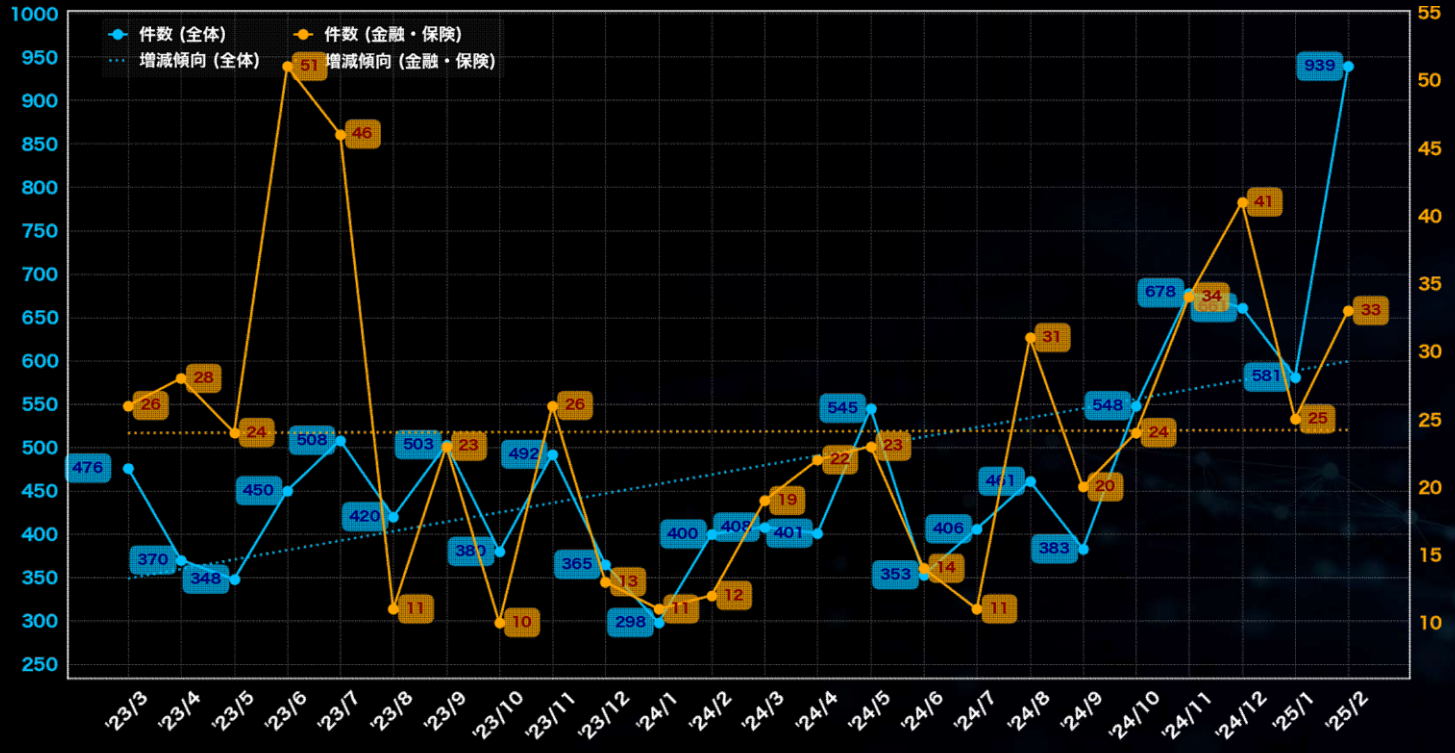
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

業種に関する分析（全世界）
（過去2年間／2023年3月～2025年2月）

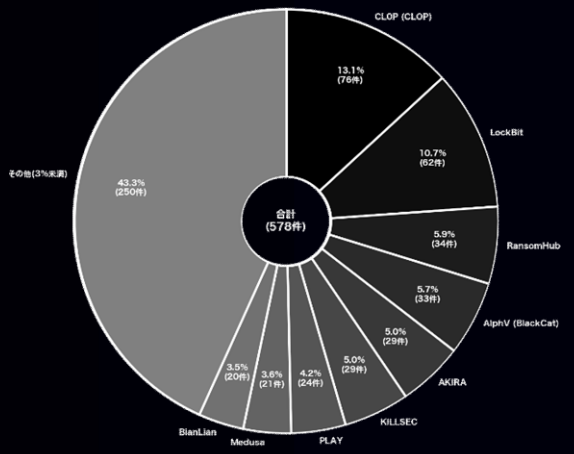
Know your enemy. Defense leadership.

金融・保険

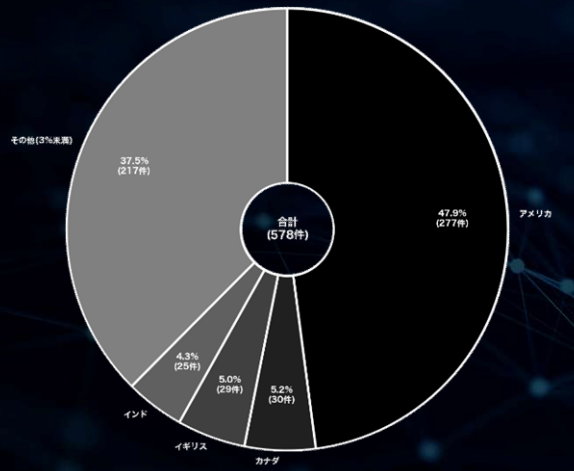
「金融・保険」業界に対するランサムウェア攻撃のリークサイト掲載件数は、最も多かった月が2023年6月で、51件の掲載があった。一方、最も少なかった月は2023年10月で、10件であった。被害組織の所在国の割合では、アメリカが約48%と最も多く、次いでイギリスとカナダがそれぞれ約5%である。攻撃グループについては、少なくとも78のグループが関与しており、特に「CL0P (CLOP)」が76件のリークサイト掲載を実施している。次いで「LockBit」と「RansomHub」がそれぞれ62件と34件の掲載を行っている。金融・保険関連は、他の業種と比較すると全体件数に対する割合が低くほぼ横ばいの推移を見せている。同業界の被害は特にCL0Pによる影響が大きく、全体推移を見てもゼロディ攻撃が目立った2023年の5月から7月にかけて被害数の増加が顕著に見られる。CL0Pはこのようにゼロディ攻撃を多用する点に加え、そうした状況下において同業界への攻撃傾向が見られる点に、今後も注意が必要である。



▼攻撃グループ別



▼国別



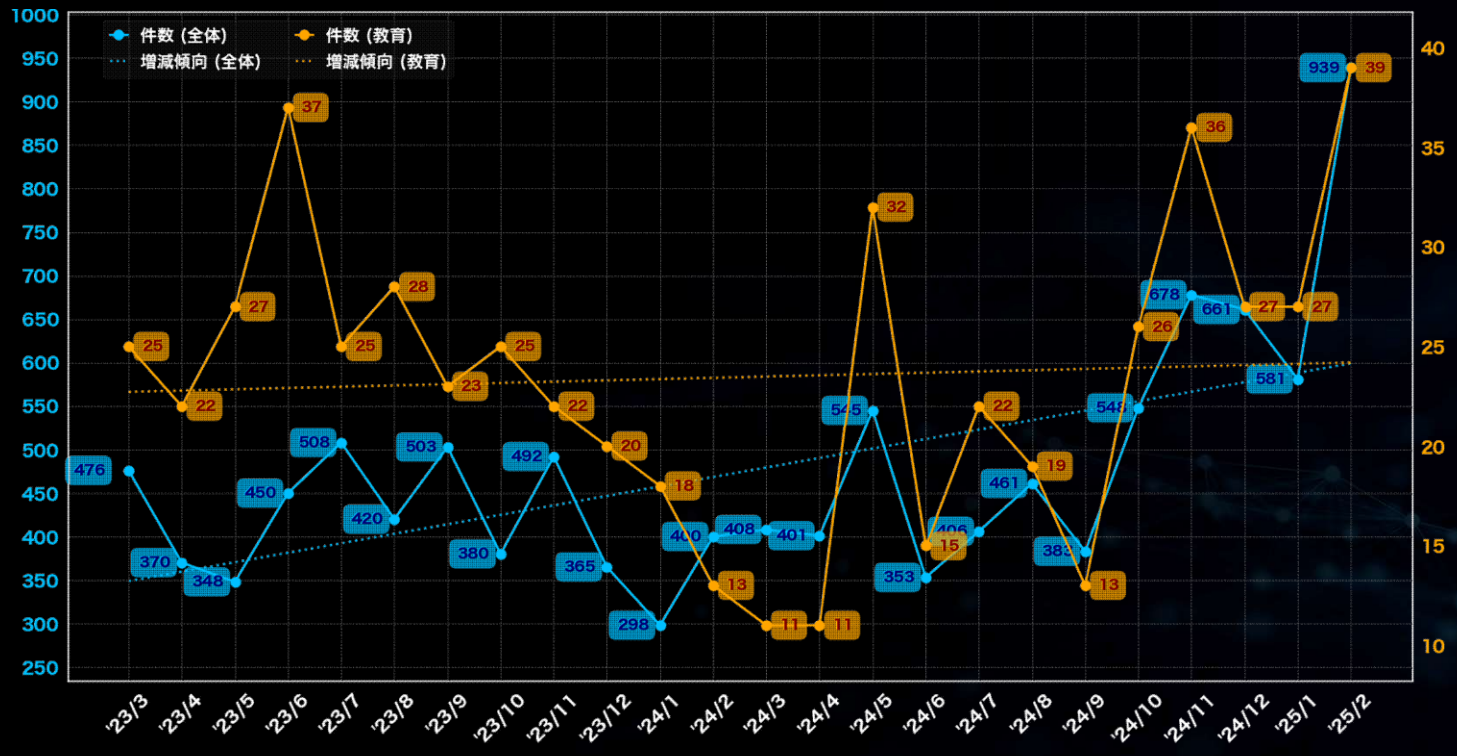
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

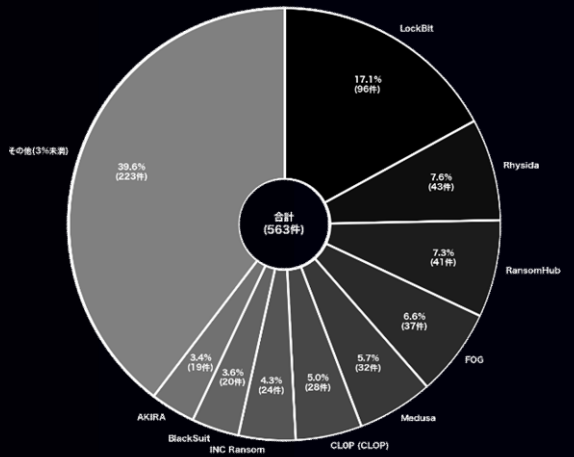
業種に関する分析（全世界）
（過去2年間／2023年3月～2025年2月）

教育

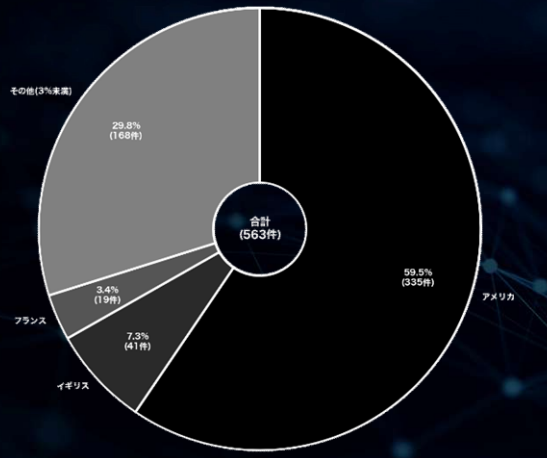
「教育」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、39件の掲載があった。一方、最も少なかった月は2024年3月と4月で、11件であった。被害組織の所在国の割合では、アメリカが約60%と最も多く、次いでイギリスとフランスがそれぞれ約7%と約3%である。攻撃グループについては、少なくとも69のグループが関与しており、特に「LockBit」が96件のリークサイト掲載を実施している。次いで「Rhysida」と「RansomHub」がそれぞれ43件と41件の掲載を行っている。教育業界は、攻撃グループ別で見ると、同業界を主な標的の一つとするRhysidaや「FOG」が上位に現れる点が特徴的である。過去2年間の推移は緩やかな増加傾向となっている。



▼攻撃グループ別



▼国別



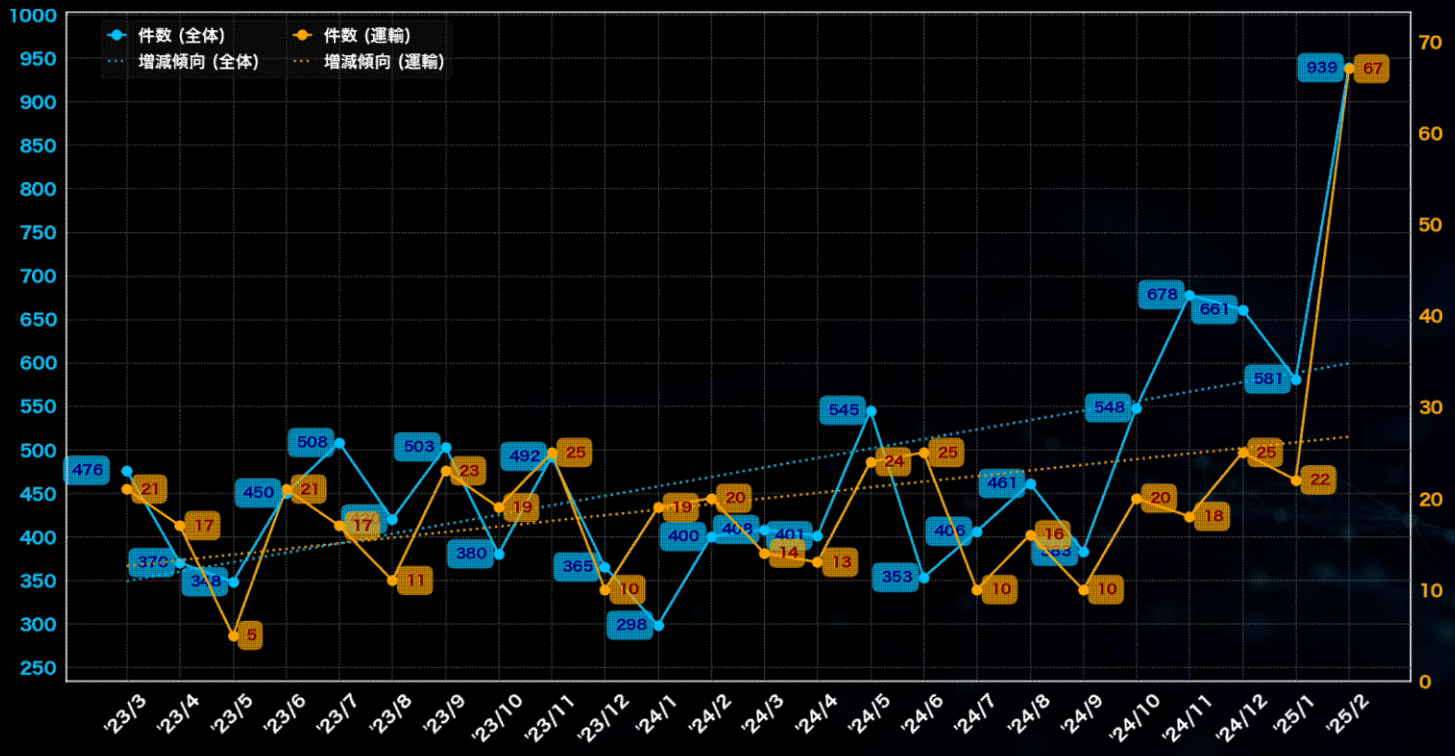
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

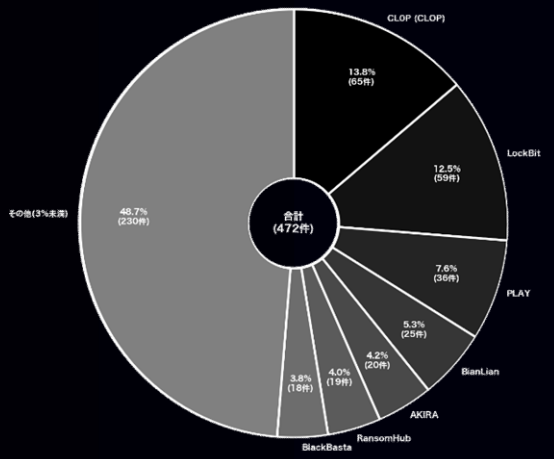
業種に関する分析（全世界）
（過去2年間／2023年3月～2025年2月）

運輸

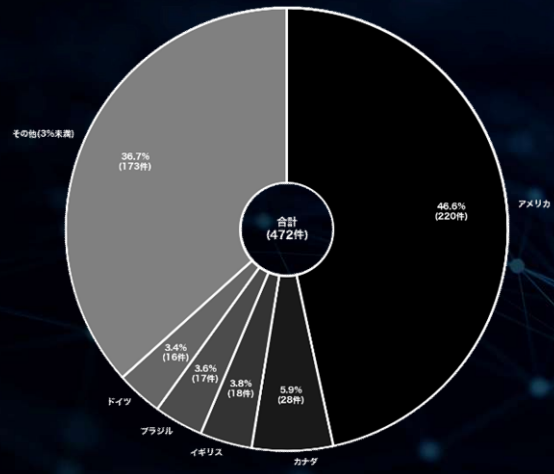
「運輸」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、67件の掲載があった。一方、最も少なかった月は2023年5月で、5件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いでカナダとイギリスがそれぞれ約6%と約4%である。攻撃グループについては、少なくとも74のグループが関与しており、特に「CL0P (CLOP)」が65件のリークサイト掲載を実施している。次いで「LockBit」と「PLAY」がそれぞれ59件と36件の掲載を行っている。運輸関係は全体件数に対する割合こそ低く、過去2年間では著しく被害が減少するケースもある一方で、緩やかな増加傾向が続いている。



▼攻撃グループ別



▼国別



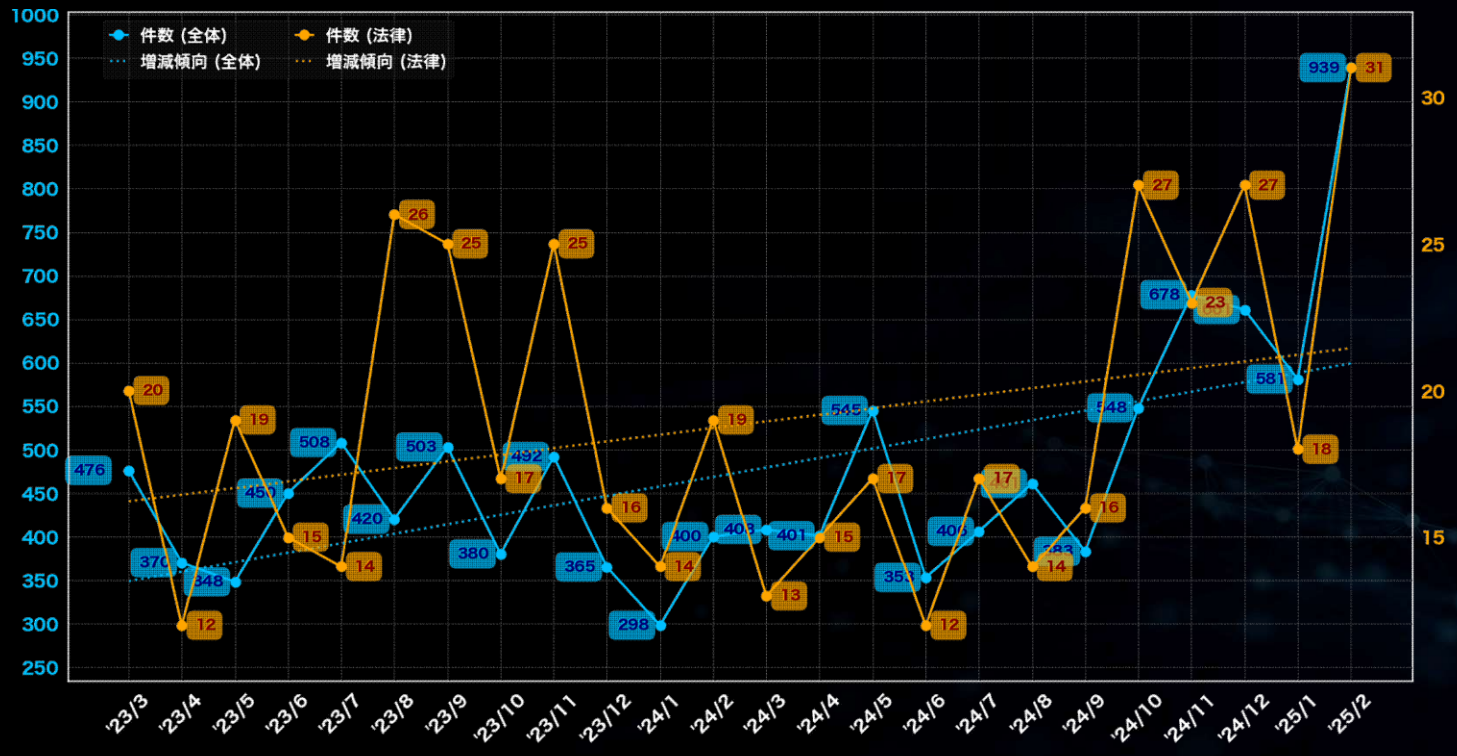
（※本ページの「掲載件数」には、リークサイト上の掲載数に加えて国内被害組織からの公表や報道から判明した数も含んでいる）

※ 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

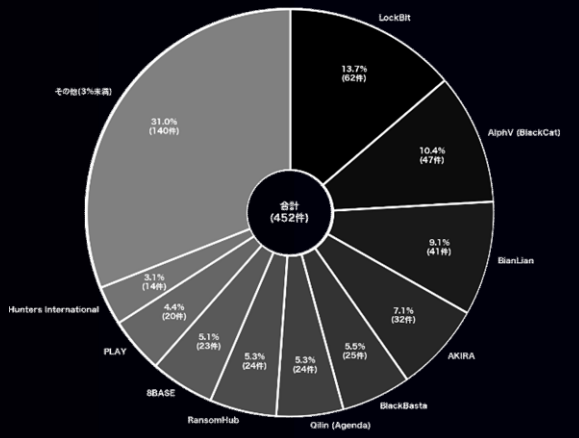
業種に関する分析（全世界）
（過去2年間／2023年3月～2025年2月）

法律

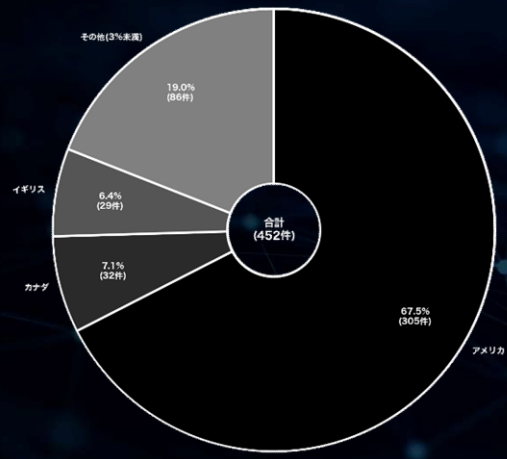
「法律」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、31件の掲載があった。一方、最も少なかった月は2023年4月および2024年6月で、12件であった。被害組織の所在国の割合では、アメリカが約68%と最も多く、次いでカナダとイギリスがそれぞれ約7%と約6%である。攻撃グループについては、少なくとも62のグループが関与しており、特に「LockBit」が62件のリークサイト掲載を実施している。次いで「AlphV (BlackCat)」と「BianLian」がそれぞれ47件41件の掲載を行っている。法律関連は2023年末以降、減少傾向が見られたが、 2023年7月から8月や、2024年9月から10月のように突発的に大きく件数を伸ばす時期があることを確認している。過去2年間においては明確な加傾向にある。



▼攻撃グループ別



▼国別



（※本ページの「掲載件数」には、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含んでいる）

※ 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

CIGのコンテンツ紹介

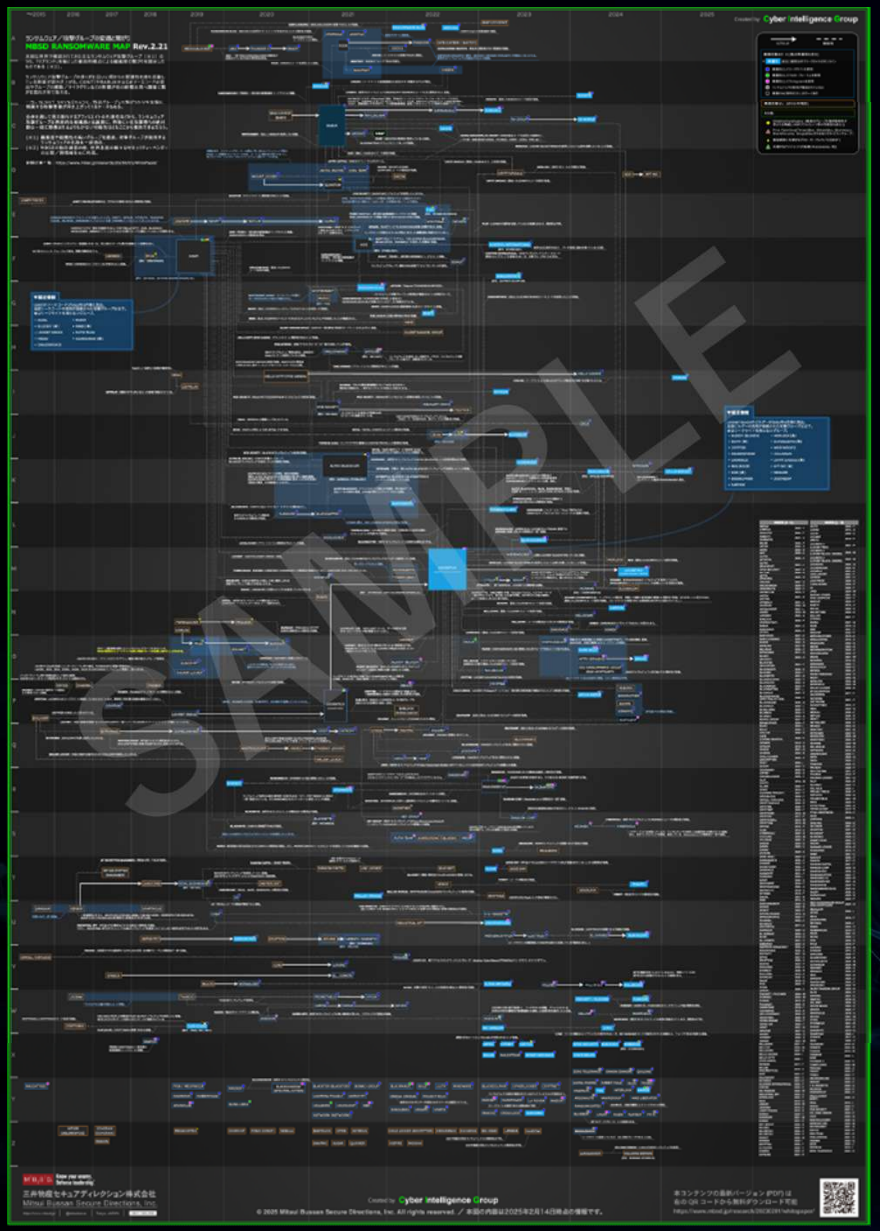
Cyber Intelligence Group（CIG）では、ランサムウェアに関する様々な観点からの分析結果を情報発信しています。ぜひとも皆様の脅威情報の把握にご活用ください。

● 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)



※ 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

本資料に関する留意事項及び二次利用について

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）

・本レポートにおける「国」データは、被害組織の本社所在地情報を元に集計しています。
ただし、本社所在地情報が確認できない場合は、”攻撃された拠点の所在国”もしくは”(Unknown)”として集計しています。

・ 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