CIG
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

2026年11月号 Rev 1.00
(2026年10月分)

2026
10



三井物産セキュアディレクション株式会社
Mitsui Bussan Secure Directions, Inc.

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

目次

総括と監視対象（レポート① ~ ④）

今月のハイライト p.3
ランサムウェア関連記事 | 今月のピックアップ p.4
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） p.5
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） p.6

グローバル統計（レポート⑤ ~ ⑰）

年間統計（全世界） ..... p.7 ~ 8
攻撃グループTOP10（全世界） ..... p.9 ~ 12
被害国TOP10（全世界） ..... p.13 ~ 16
被害国TOP10（アジア） ..... p.17 ~ 20
業種TOP10（全世界） ..... p.21 ~ 24

日本関連組織を対象とした統計（レポート⑱ ~ ㉓）

被害数の推移に関する統計（全世界及び国内） ..... p.25 ~ 26
資本金別の統計（国内） ..... p.27 ~ 28
公表と暴露に関する統計（国内） ..... p.29 ~ 30
公となった国内被害組織 概要一覧 ..... p.31 ~ 33
公となった国内被害組織における拠点割合 p.34
公となった国内被害組織における業種割合 p.35

中小企業における被害分析（レポート㉔ ~ ㉗）

資本金別（中小企業） p.37
公となった国内被害組織における業種割合（中小企業） p.38
公となった国内被害組織における拠点割合（中小企業） p.39
公となった国内被害組織 概要一覧（中小企業） ..... p.40 ~ 41

多重被害に関する分析（レポート㉘ ~ ㉙）

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 p.43
多重被害に遭った被害組織の傾向と分析 p.44

業種に関する分析（レポート㉚）

業種に関する分析 - 製造 p.46
業種に関する分析 - サービス p.47
業種に関する分析 - 情報通信 p.48
業種に関する分析 - 卸売・小売 p.49
業種に関する分析 - 建設・建築 p.50
業種に関する分析 - 医療 p.51
業種に関する分析 - 金融・保険 p.52
業種に関する分析 - 法律 p.53
業種に関する分析 - 運輸 p.54
業種に関する分析 - 教育 p.55

その他

CIGのコンテンツ紹介 p.56
本資料に関する留意事項及び二次利用について p.57

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

総括と監視対象

2026

10

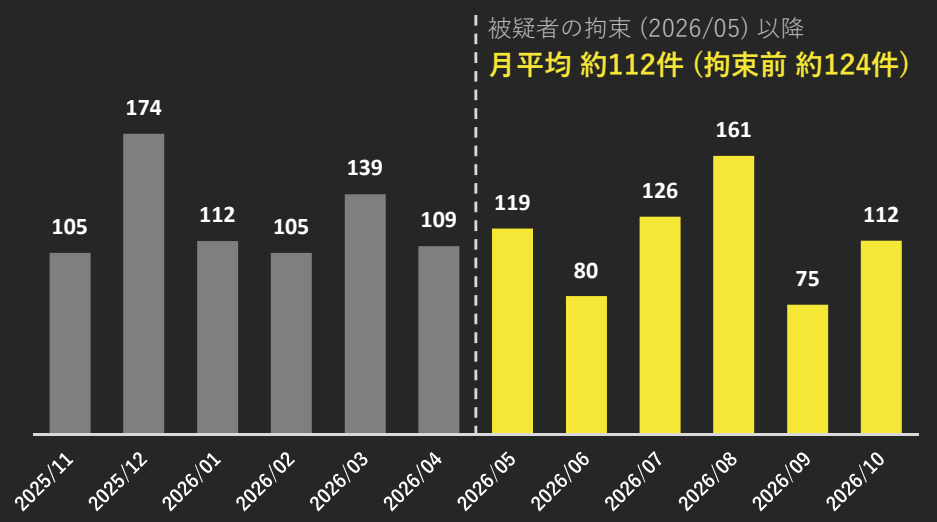
© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

今月のハイライト

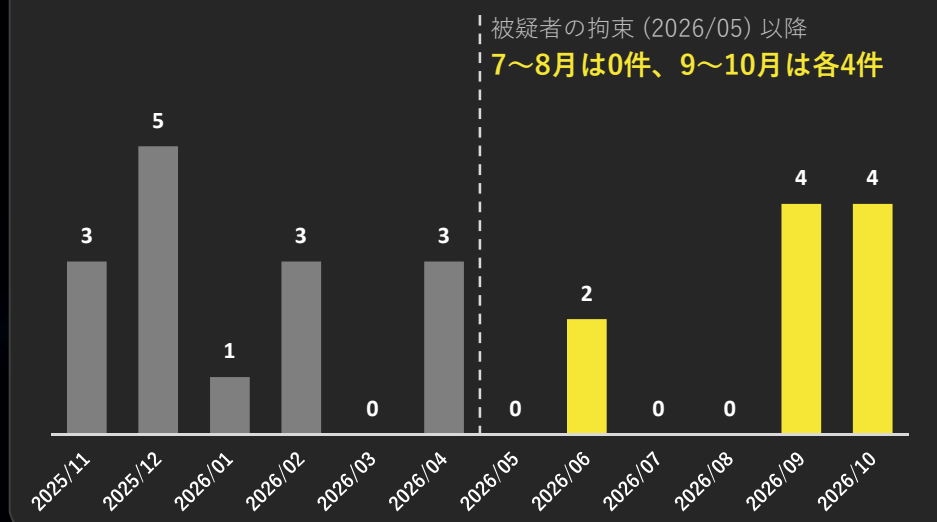
● Qilinランサムウェア攻撃グループのコアメンバーを拘束

警察庁は2026年10月8日にQilinランサムウェア攻撃グループを主導していたとされる被疑者を日本で拘束し、ドイツへ引き渡したと発表した※1。なお、拘束自体は2026年5月に行われていたと報じられている。Qilinは勢いのあるランサムウェア攻撃グループの一つであり、2026年に入ってから多数の日本関連企業に被害を与えたグループでもある。CIGの観測では、被疑者の拘束後もリークサイトへの被害企業の掲載件数に目立った減少は現時点で確認できていない。こうした現状を踏まえると、今後もQilinランサムウェアによる被害は続くものと想定して対策を講じる必要がある。

Qilinによる被害組織の掲載数の推移（グローバル版）



Qilinによる被害組織の掲載数の推移（日本関連組織に限定）



対策の一つは、攻撃に悪用される脆弱性への迅速な対処である。実際に、Qilinのアフィリエイトは、VPN機器（CVE-2026-0257）やファイアウォール管理製品（CVE-2026-20316）の脆弱性を悪用して初期侵入に成功したと報告されている※2、※3。また、初期侵入後にバックアップ製品の脆弱性（CVE-2023-27532）を悪用する攻撃ツールが用いられ、横展開やバックアップ基盤への侵害が試みられたとの報告もある※4。これらの脆弱性の修正にとどまらず、侵入されることを前提に、監視運用によって被害を限定することも重要である。海外の事例ではあるものの、盗まれた認証情報によるSSL VPN経由の侵入を許し、さらにEDRを回避される状況でも、MDRのSOCが不審な挙動を検知して感染端末を隔離し、暗号化の完了前に封じ込めた実例が報告されている※5。最近では、攻撃側によるAIの悪用により、数多くの被害事例が報告されている。このような状況では、パッチ適用による対処に加え、防御側もAIを積極的に活用し、異常な動作の検知と適切な対応によって被害を抑制することが求められる。

※1: (参考情報) https://www.npa.go.jp/news/release/2026/20261008news.pdf
※2: (参考情報) https://arcticwolf.com/resources/blog/exploitation-of-cve-2026-0257-leads-to-qilin-ransomware/
※3: (参考情報) https://blog.talosintelligence.com/fmc-ongoing-exploitation/
※4: (参考情報) https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Linux%2FQilin!rfn
※5: (参考情報) https://blackpointcyber.com/blog/qilin-ransomware-and-the-hidden-dangers-of-byovd/?trk=article-ssr-frontend-pulse_little-text-block

※ 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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

ランサムウェア関連記事 | 今月のピックアップ （期間: 2026年10月6日～2026年11月12日）

【インターネットに公開されたシステムを狙うFortiBleed攻撃が継続、締め出し被害も報告】（出典: FBI・米シークレットサービス（USSS） 2026/10/06）
FBIと米シークレットサービスは、Fortinet機器への大規模な不正アクセス活動「FortiBleed」が続いていると警告。管理者が機器を使えなくなった例や、侵入先のアクセス権がランサムウェア実行犯に渡った例を挙げた。
https://www.ic3.gov/CSA/2026/261006.pdf

【フロリダ州のランサムウェア復旧企業の経営者、顧客を欺いたとして起訴】（出典: 米ニューヨーク東部地区連邦検事局 2026/10/07）
米検察は、ランサムウェア復旧業者MonsterCloudの代表を通信詐欺罪で起訴したと公表。身代金を払わず復旧すると宣伝しながら、ある例では攻撃者に約8,200ドルを支払い、顧客に約15万ドルを請求した疑いがある。
https://www.justice.gov/usao-edny/pr/owner-florida-ransomware-remediation-company-charged-defrauding-clients

【ロシア国籍ランサムウェア被疑者逮捕に関するドイツの広報について】（出典: 警察庁 2026/10/08）
警察庁は、ランサムウェア攻撃グループQilinを主導していたとみられるロシア国籍の被疑者について、来日後に日本国内で身柄を拘束し、関係機関と連携してドイツに引き渡したと公表した。
https://www.npa.go.jp/news/release/2026/20261008news.pdf

【Semperis 2026年ランサムウェアレポート：AI駆動型攻撃の増加と、経営幹部およびその家族に対する身体的脅威の高まりが明らかに】（出典: Semperis 2026/10/14）
Semperis社は、ランサムウェア被害を受けた組織を対象とした調査を公表。攻撃におけるAIの悪用に加え、従業員やその家族への身体的危害をほのめかす脅迫など、手口がデジタル上にとどまらない実態を示した。
https://www.semperis.com/press-release/semperis-2026-ransomware-report-reveals-increases-in-ai-driven-attacks-and-a-rise-in-physical-threats-against-executives-and-their-families

【#StopRansomware：SafePayランサムウェア】（出典: CISA 2026/10/20）
CISAやFBIなどは、2024年8月から活動するSafePayの合同勧告を公表。重要インフラの複数分野で少なくとも600の組織が被害を受けており、侵入手口には脆弱性やパスワードの悪用などがあるという。
https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-293a

【1億ドル超の損害をもたらしたランサムウェア攻撃で病院や企業、政府機関への侵入に関与したウクライナ国籍の人物に判決】（出典: 米司法省 2026/10/27）
米司法省は、NefilimとHiveのランサムウェア攻撃にアフィリエイトとして関与したウクライナ国籍の人物に、禁錮70か月が言い渡されたと発表した。
https://www.justice.gov/opa/pr/ukrainian-national-sentenced-role-hacking-hospitals-businesses-and-governments-part

【n0nランサムウェア：AIを活用した恐喝活動の内情】（出典: SOCRadar 2026/10/28）
SOCRadar社は、n0nランサムウェアの攻撃者がAIツール「opencode」で攻撃スクリプトを作成・修正したと報告。なお、調査では完全自律型の攻撃システムは確認されず、人間が主導していたとみられる。
https://socradar.io/blog/n0n-ransomware-ai-assisted-extortion/

【GhostFrame：Settraランサムウェアに関連する新たなESXi用インプラント】（出典: Recorded Future（Insikt Group） 2026/11/10）
Recorded Future社は、Settraランサムウェアと関連する攻撃グループTAG-218が、侵害済みのESXiホストから複数の仮想マシンを操作できる新たなツール「GhostFrame」を使っていると報告した。
https://www.recordedfuture.com/blog/ghostframe-esxi-implant-settra-ransomware

【インシデント調査報告書チェックリスト公開のお知らせ】（出典: JPCERT/CC 2026/11/11）
JPCERT/CCは、ランサムウェア被害などの調査を外部に依頼する組織と、報告書を作成する担当者に向けて「インシデント調査報告書チェックリスト」を公開した。
https://www.jpcert.or.jp/ir_report_checklist_20261111.html

【Citrus Ransomware：通信にVLESS、暗号化にSn00py、さらにLLMも一役】（出典: Kaspersky（Securelist） 2026/11/11）
Kaspersky社は「Citrus Ransomware」の手口を報告。調査では、委託先従業員から盗んだ認証情報による侵入や、LLMで作成・編集したとみられるスクリプト、不正なグループポリシーの使用を確認した。
https://securelist.com/citrus-ransomware/121879/

【国際サイバー作戦でGootloaderマルウェアの活動を妨害】（出典: 米司法省 2026/11/12）
米司法省は、国際作戦でGootloaderの配布に使われたドメインを差し押さえ、100台超のサーバーからマルウェアを除去したと発表した。運営者は感染端末へのアクセスをランサムウェア攻撃者に販売していたとされる。
https://www.justice.gov/opa/pr/gootloader-malware-disrupted-international-cyber-operation

※ 外国語で発表されたニュースタイトルは日本語へ翻訳済み
※ 本レポート記載の各ニュース概要は生成AIにより作成
※ 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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

監視中のランサムウェア攻撃グループ情報（拠点数と一覧）

● 当月監視対象の攻撃グループ数（※1）：391（※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：84

※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）

0APT
0DAY
0mega (Omega)
● 0X00
8BASE
Abyss
AiLock
AKIRA
AKO
ALP-001
Alpha (MYDATA)
AlphV (BlackCat)
Anubis
Apos Security
APT73 (Eraleig)
ARACHNA
ARCUS MEDIA
Argonauts
Arkana
ARVINCLUB
Astro (Astra)
AtomSilo
AUDIT
AUR0RA
Avaddon
AvosLocker
AWARE
Axxes
AzzaSec
Babuk
Babuk (2025)
BARRACUDA
BASHE
BAVACAI
BEAST
Benzona
BERT
BianLian
BL0ODY (BLOODY)
BL4CKT0R (BLACKTOR)
Black Basta
BlackByte
BLACKDOLPHIN
BlackField
BlackLock
BLACKLOCKS
BlackMatter
Black Nevas
Blackout
BLACKSHRANTAC
BlackSuit
BLACKWATER
Black X
BLUEBOX
BLUESKY
BLUEWHALE
BOOBA
BQTLOCK
Brain Cipher
BRAVOX
Brotherhood
Bully
BUSINESS DATA LEAKS
● BYOD
CACTUS
Cephalus
CHAOS (2025)
CHEERS
CHILELOCKER (ARCRYPTER)
CHORT
Cicada3301
CiphBit
CipherForce
CipherLocker
CL0P (CLOP)
Cloak
CMD ORGANIZATION
COINBASE CARTEL
Conti
Cooming Project
Crazy Hunter Team
CROSSLOCK
CRPX0
CRY0
CryptBB
CRYPTNET
CRYPTO24
CryptOn
Cuba
CYBERLEEK
CYCLOPS
D1R
D4RK4RMY
DAGON
DAIXIN
dAn0n (danon)
Dark Angels
Darkbit
DARKMATTER
DARKPOWER
DARK PROJECT
DarkRace
DarkRypt
DARK SHINIGAMIS
DarkSide
Dark Vault
DataCarry
DATAKEEPER
DEADLOCK
Desolator
DEVMAN
DEVMAN 2.0
Dire Wolf
DISPOSSESSOR[DATABROKER]
Donex
Donut Leaks
DOOMMAGEDDON
DoppelPaymer
dotAdmin
DragonForce
DragonRansomware
DREAMFYRE
DUNGHILL
DYSPHOR1A
eCh0raix (eChoraix)
ECLIPSE
EL_COMETA
EL DORADO
EMBARGO
EMPERADOR
Endurance
ENDZONE
ENTROPY
ETHICS
Everest
● EVERSTAKE
EXFILSQUAD
EXITIUM
FALCON
FOG
FOXSEC
Frag
FSOCIETY / FLOCKER
FSTEAM
FulcrumSec
Funksec
GAMMAX
GD LockerSec
Genesis
GLOBAL
GLOBAL CYBERNETIC COLLECTIVE
GLOBAL SECRET GROUP
Grief
Groove
Gunra / Fresh Gunra
HANDARA [HACKTIVIST]
Haron
HELIX
HELLCAT
Helldown
HelloGookie
HITLER (AGL0BGVYCG)
Hive
HolyGhost
Hotarus
Hunters International
HYFLOCK
IAH647
IAMNOTAVILLAIN
ICARUS
ICEFIRE
IMN Crew
INC Ransom
Insane
INSOMNIA
INTERLOCK
J GROUP
KAIROS
Karakurt
Karma
Kawa4096
Kazu
KILLSEC
Kittykatkrew
Knight
Kraken (HelloKitty)
KRYBIT
Kryptos
Kyber
LAMASHTU
LAMBDA
La Piovra
LAPSUS$
LAPSUS$ Group
LEAK BAZAAR
LeakedData (Silent Ransom Group)
LEAKNET
L GROUP
LILITH
Linkc
LockBit
LOKI
Lorenz
LostTrust
LunaLock
LV
Lynx
M3RX
MADCAT
MAD LIBERATOR
MAJINAHANASHI
MALAS
MALEKTEAM
Mallox
MAMONA RIP
MBC
Medusa
MEDUZALOCKER
MEDUZA LOCKER BLOG
MEOW
MEOWCIETY403
Metaencryptor
MIDAS
MIGA
● MIMORI
Mindware
Minteye
MNT6
MOGILEVICH [FRAUD]
MOISHA
Money Message
Monti
Morpheus
MORTAR
MOUNT LOCKER
MS13-089
N0N
N3TW0RM (NETWORM)
N4UGHTYSEC (NAUGHTYSEC)
NASIR SECURITY
Nefilim
NetRunner
NEVADA
NightSky
NightSpire
NITROGEN
NoEscape
Nokoyawa
NONAME (VFOKX)
NONAME [2023年確認]
Nova
NULLBULGE
Obscura
Obscura 2.0
ONYX
Orca
Orion Leaks
OROVA
OSIRIS PROJECT
Pandora
PANZER
Pay2Key
Payload
Payload.bin
Payouts King
PEAR
PLAY
PLAYBOY
PRINZ EUGEN
Prometheus
PRYX
PUTIN TEAM
Pysa / Mespinoza
Qilin (Agenda)
QILULONG
Quantum
RABBIT HOLE
RADAR
RADIANT
Ragnar Locker
Ragnarok
RA GROUP
RALord
Rancoz
RANSOMBAY
Ransom Cartel
RANSOM CORP
RANSOMCORTEX
Ransomed.vc
Ransom EXX
RansomHouse
RansomHub
Ransomware Blog
RANZY
RA WORLD
Raznatovic
REDACT
RedAlert (N13V)
Red Ransomware Group (Red CryptoApp)
Relic
REVIL (SODINOKIBI)
Reynolds
Rhysida
RISEN
ROOK
root
Royal
Rransom
RunSomeWares
RUSTY LOCKER
SABBATH (54BB47H)
SAFEPAY
SARCOMA
SATAN LOCK
SATANLOCK V2
● SCARLETTGROUP
Scattered LAPSUS$ Hunters
Secp0
SECTION9
Securotrop
SenSayQ
SETTRA
SEVYWARE
SHADOWBYT3$
Shaoleaks
SHIBA
SHINYHUNTERS
Sicarii
SIEGEDSEC
Silent
Sinobi
SKIRA TEAM
SLUG
Snatch
SOLIDBIT
SOVCALI
Space Bears
Sparta
SPIRALS
Spook
SPY CORPORATE
STORM
STORMOUS
SUGAR
Suncrypt
SYNACK
● SYNTAX
TeamXXX
TENGU
Termite
The Gentlemen
THE GREEN BLOOD GROUP
● THE SEVEN DEADLY SINS
ThreeAM (3AM)
TIMC
TITAN
TridentLocker
TRIGONA
TRINITY
Triple X
TRISEC
ULOSE
● UMBRA
Underground
UnSafe
Valencia
VanHelsing
VanirGroup
Vect
VEXY
Vice Society
V IS VENDETTA
VLADIVOSTOK
VSOP
● VYPR
Wallstreet
WALocker
Warlock
WEREWOLVES
Weyhro
● WHITEARMOR
WORLD LEAKS
x001xs
XING TEAM
XP95
XPL0ITRS
Yanluowang
Yurei
ZAWOO
Zeon
Zero Tolerance

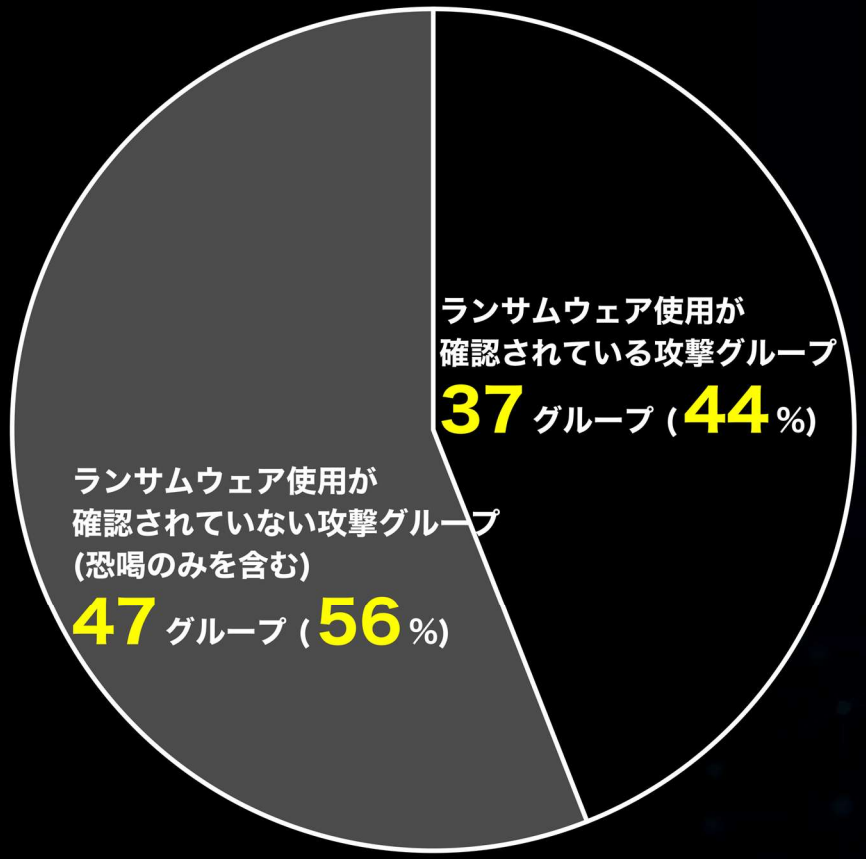
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

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）

●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（2026年 10月）

（※当月にリークサイト掲載を確認した攻撃グループ全 84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CL0P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、2026年10月に活動中である事が確認された全84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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

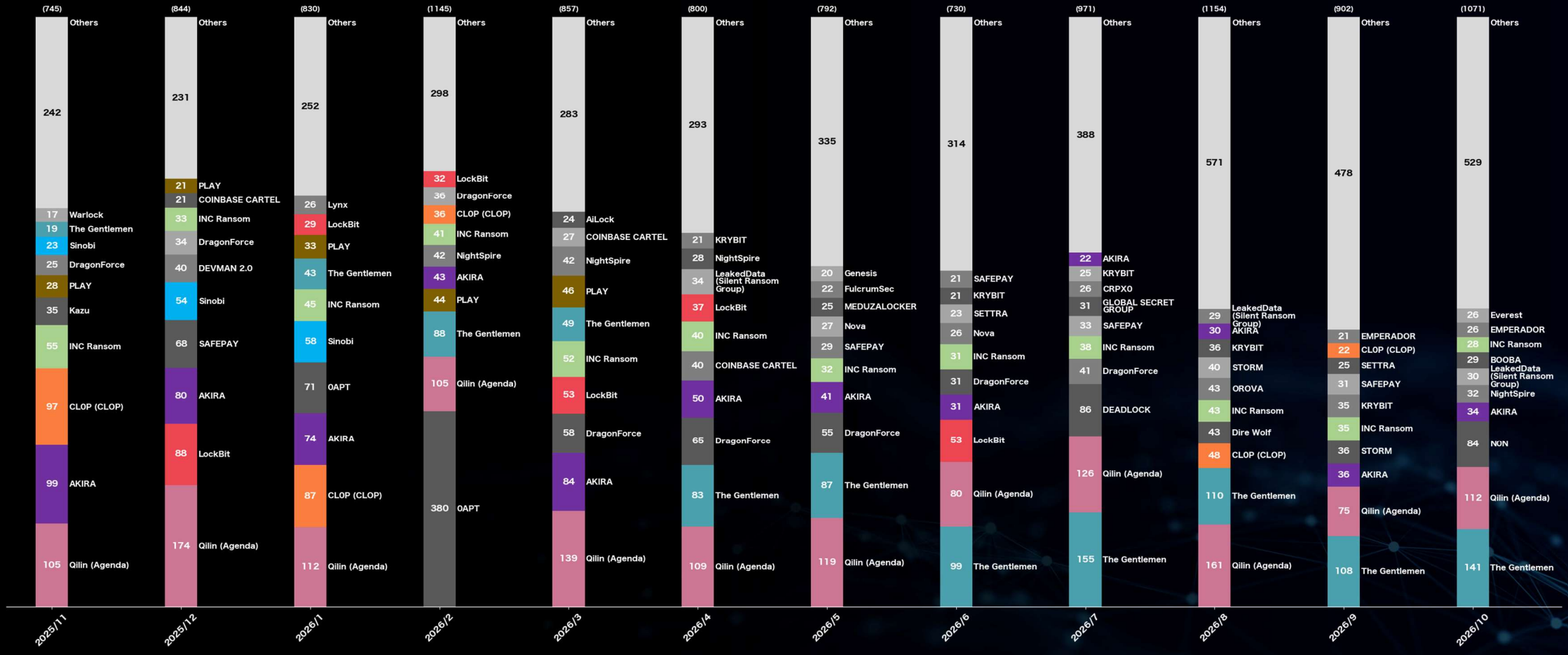
年間 統計
（全世界）

2026
10

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

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／2025年11月～2026年10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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

攻撃グループ 月別統計
（全世界）（過去3ヶ月分）

2026
10

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

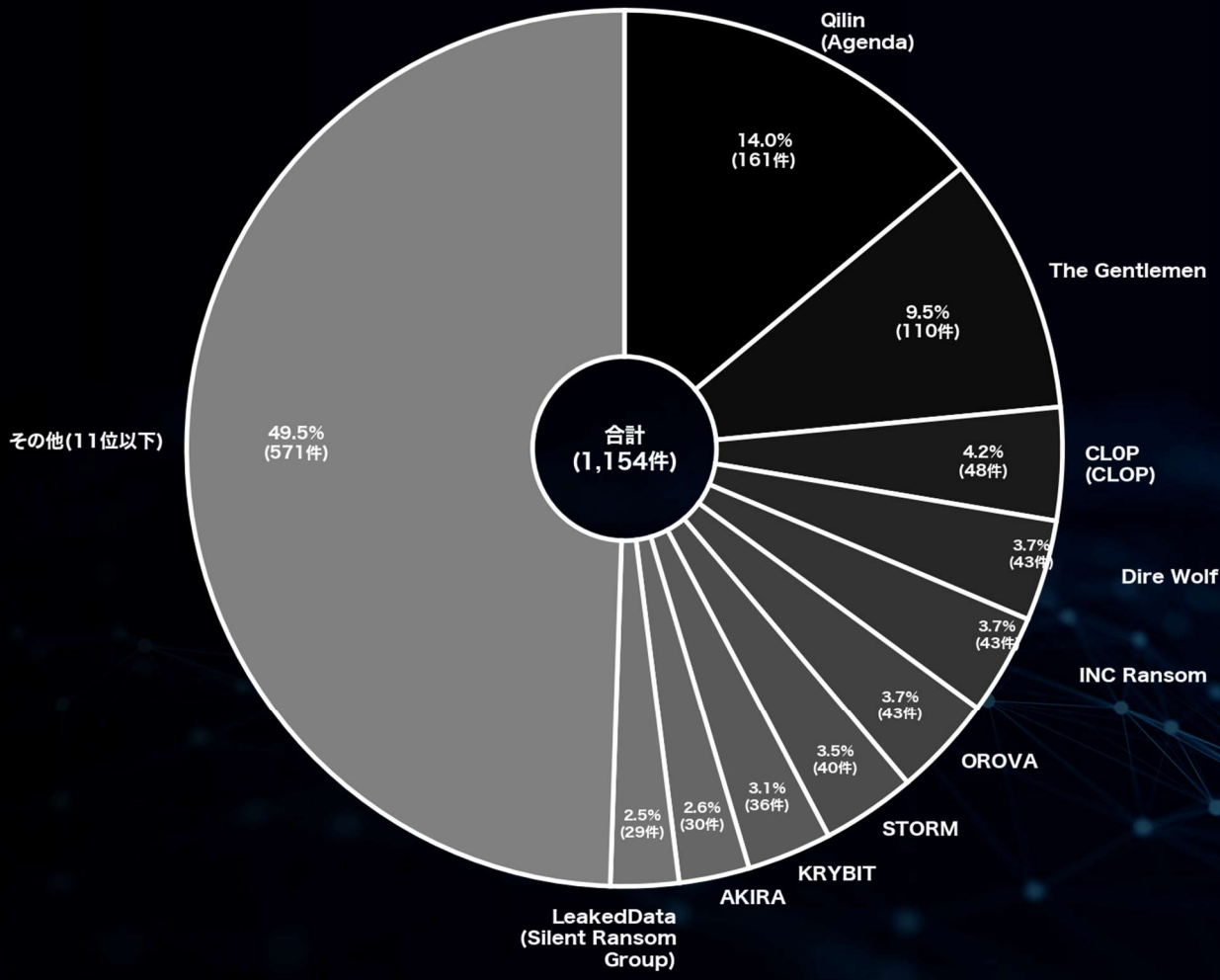
月別内訳 攻撃グループ TOP10（全世界）

（2026年 8 月）

※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)
Qilin (Agenda)	161	14.0	+ 35
The Gentlemen	110	9.5	- 45
CL0P (CLOP)	48	4.2	+ 47
Dire Wolf	43	3.7	+ 43
INC Ransom	43	3.7	+ 5
OROVA	43	3.7	+ 43
STORM	40	3.5	+ 40
KRYBIT	36	3.1	+ 11
AKIRA	30	2.6	+ 8
LeakedData (Silent Ransom Group)	29	2.5	+ 29

▼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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

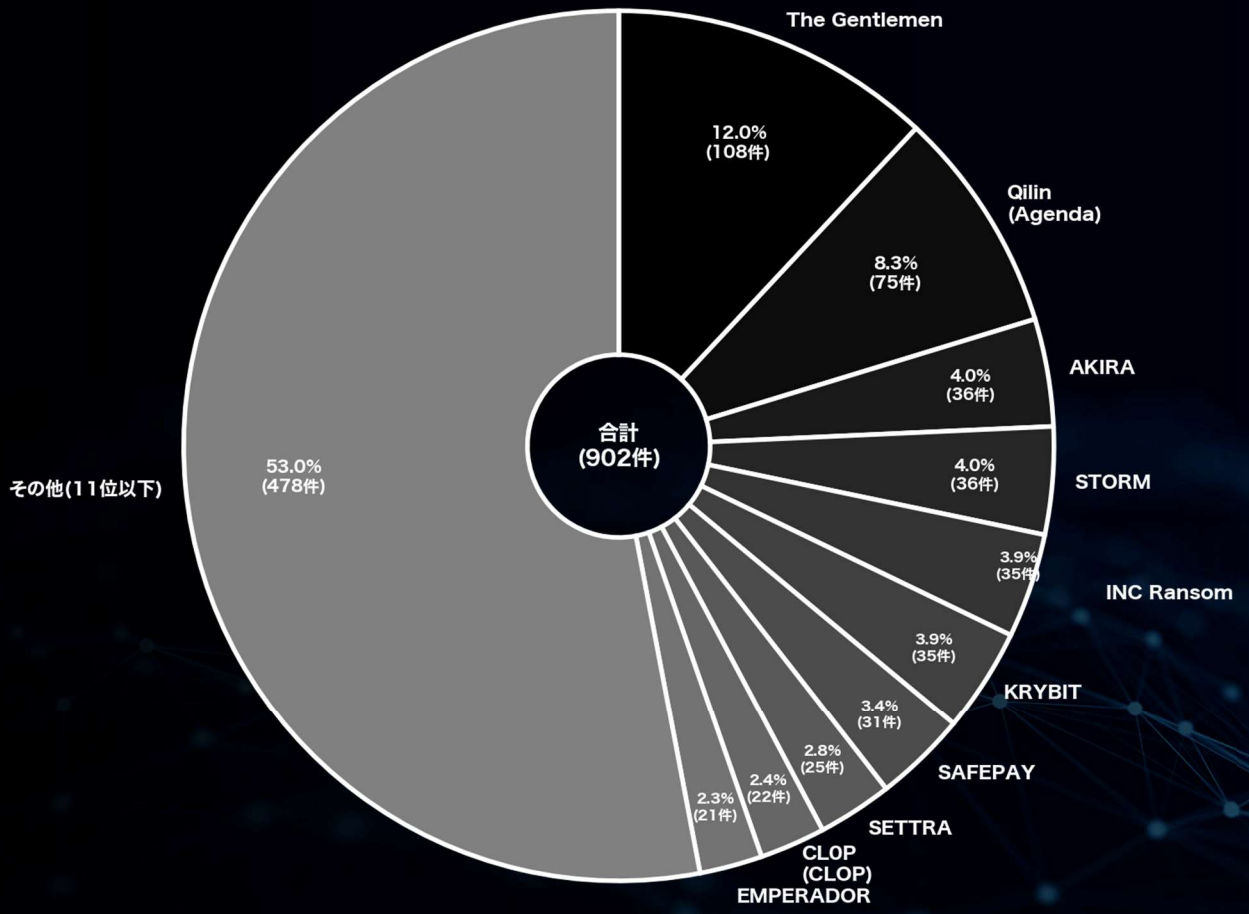
月別内訳 攻撃グループ TOP10（全世界）

（2026年 9 月）

※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)
The Gentlemen	108	12.0	- 2
Qilin (Agenda)	75	8.3	- 86
AKIRA	36	4.0	+ 6
STORM	36	4.0	- 4
INC Ransom	35	3.9	- 8
KRYBIT	35	3.9	- 1
SAFEPAY	31	3.4	+ 19
SETTRA	25	2.8	+ 3
CL0P (CLOP)	22	2.4	- 26
EMPERADOR	21	2.3	+ 11

▼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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

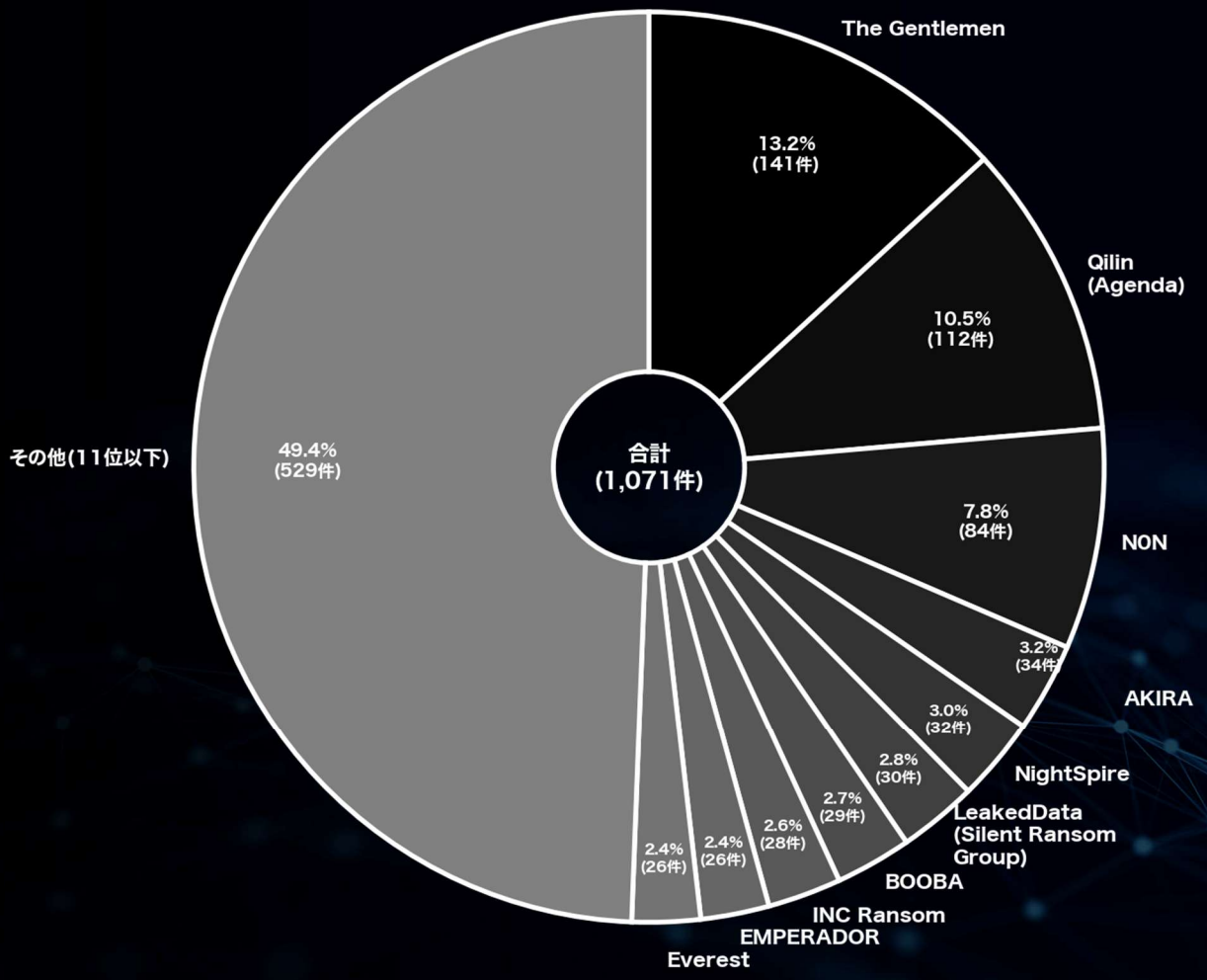
月別内訳 攻撃グループ TOP10（全世界）

（2026年 10 月）

※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)
The Gentlemen	141	13.2	+ 33
Qilin (Agenda)	112	10.5	+ 37
N0N	84	7.8	+ 67
AKIRA	34	3.2	- 2
NightSpire	32	3.0	+ 22
LeakedData (Silent Ransom Group)	30	2.8	+ 9
BOOBA	29	2.7	+ 21
INC Ransom	28	2.6	- 7
EMPERADOR	26	2.4	+ 5
Everest	26	2.4	+ 14

▼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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

被害国 月別統計
（全世界）（過去3ヶ月分）

2026
10

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

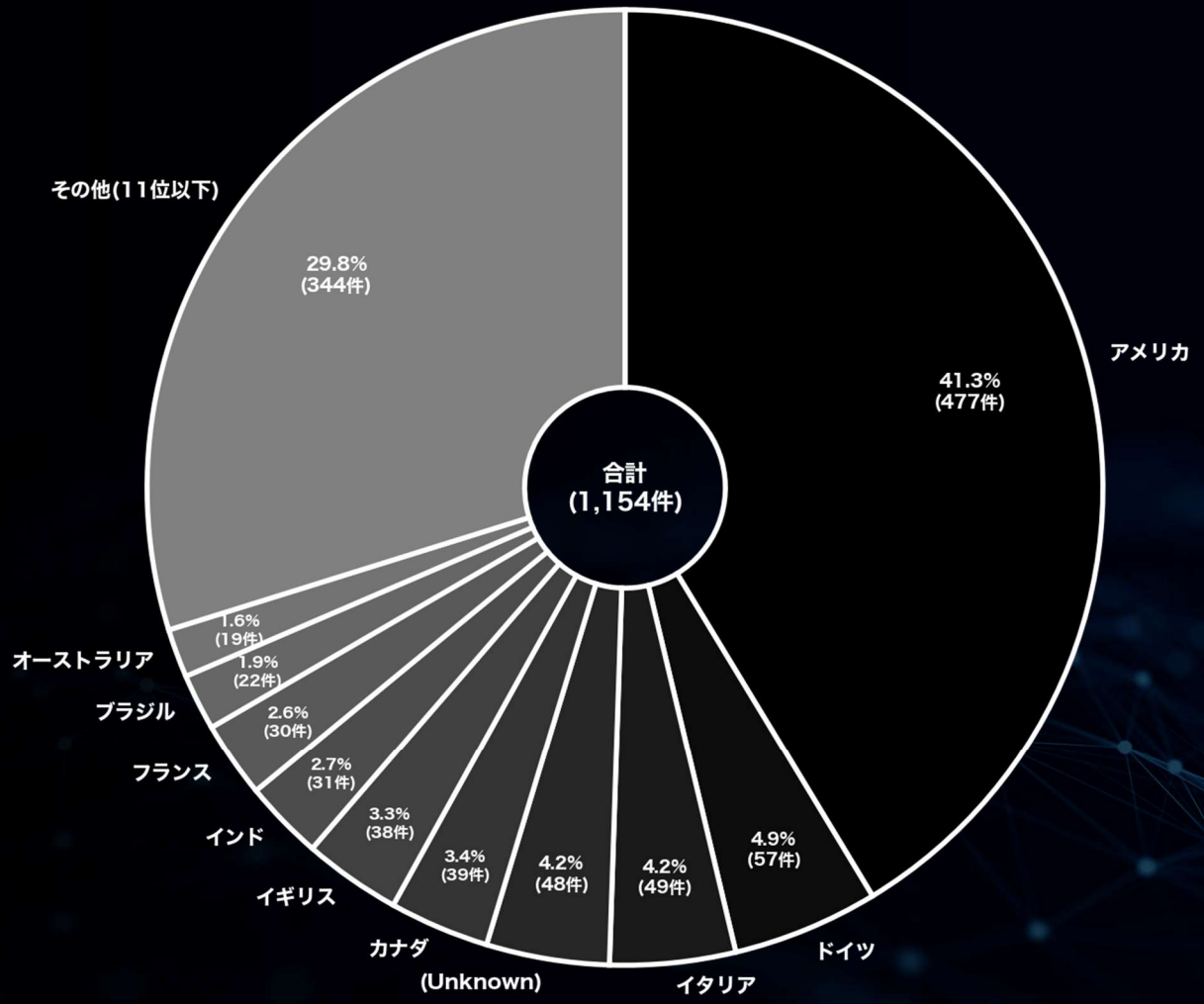
月別内訳 被害国TOP10（全世界）

（2026年 8 月）

※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	477	41.3	+ 121
ドイツ	57	4.9	+ 9
イタリア	49	4.2	+ 20
(Unknown)	48	4.2	+ 22
カナダ	39	3.4	- 5
イギリス	38	3.3	+ 7
インド	31	2.7	- 1
フランス	30	2.6	+ 2
ブラジル	22	1.9	+ 2
オーストラリア	19	1.6	+ 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）



※ 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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

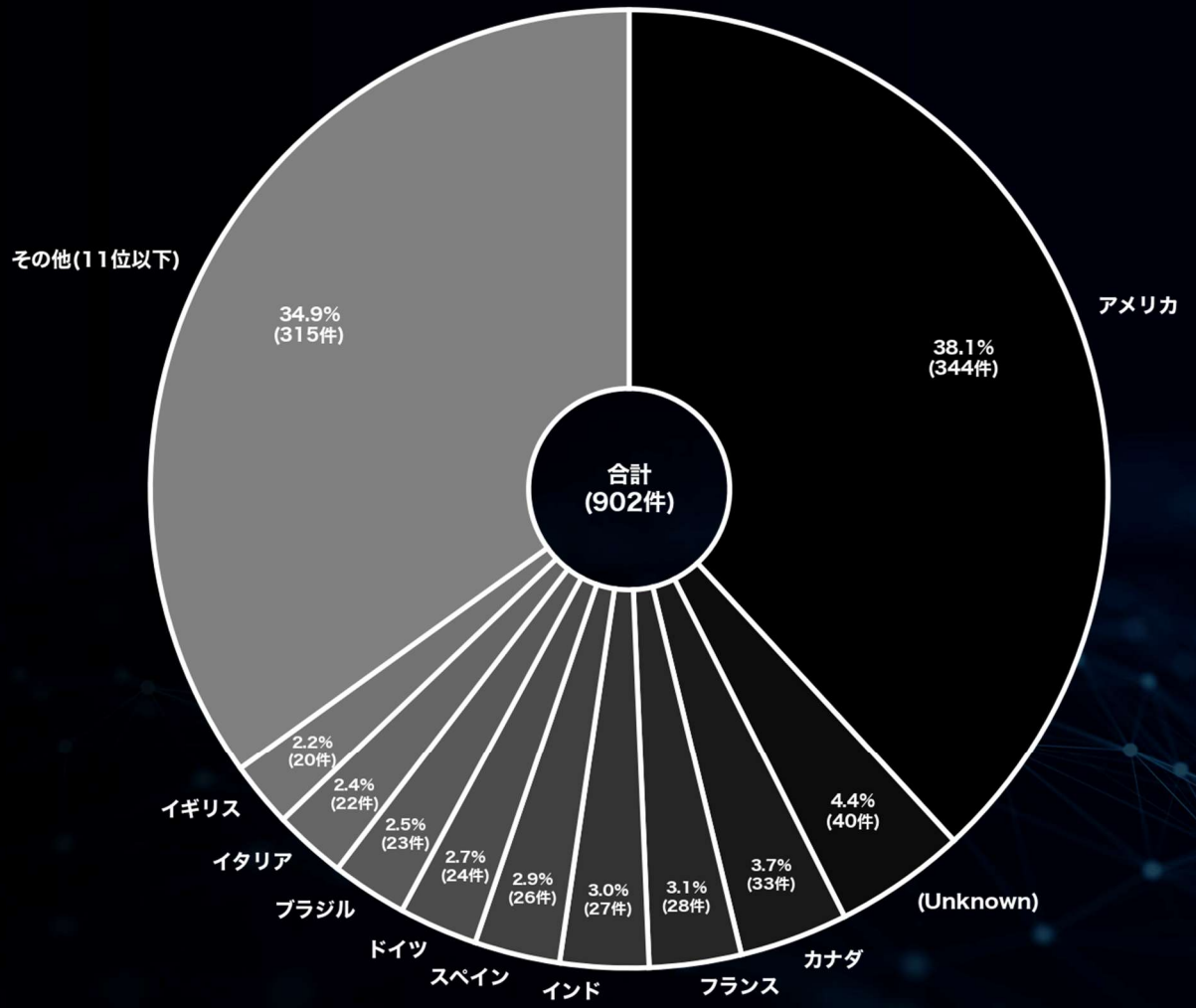
月別内訳 被害国TOP10（全世界）

（2026年 9 月）

※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	344	38.1	- 133
(Unknown)	40	4.4	- 8
カナダ	33	3.7	- 6
フランス	28	3.1	- 2
インド	27	3.0	- 4
スペイン	26	2.9	+ 8
ドイツ	24	2.7	- 33
ブラジル	23	2.5	+ 1
イタリア	22	2.4	- 27
イギリス	20	2.2	- 18

▼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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

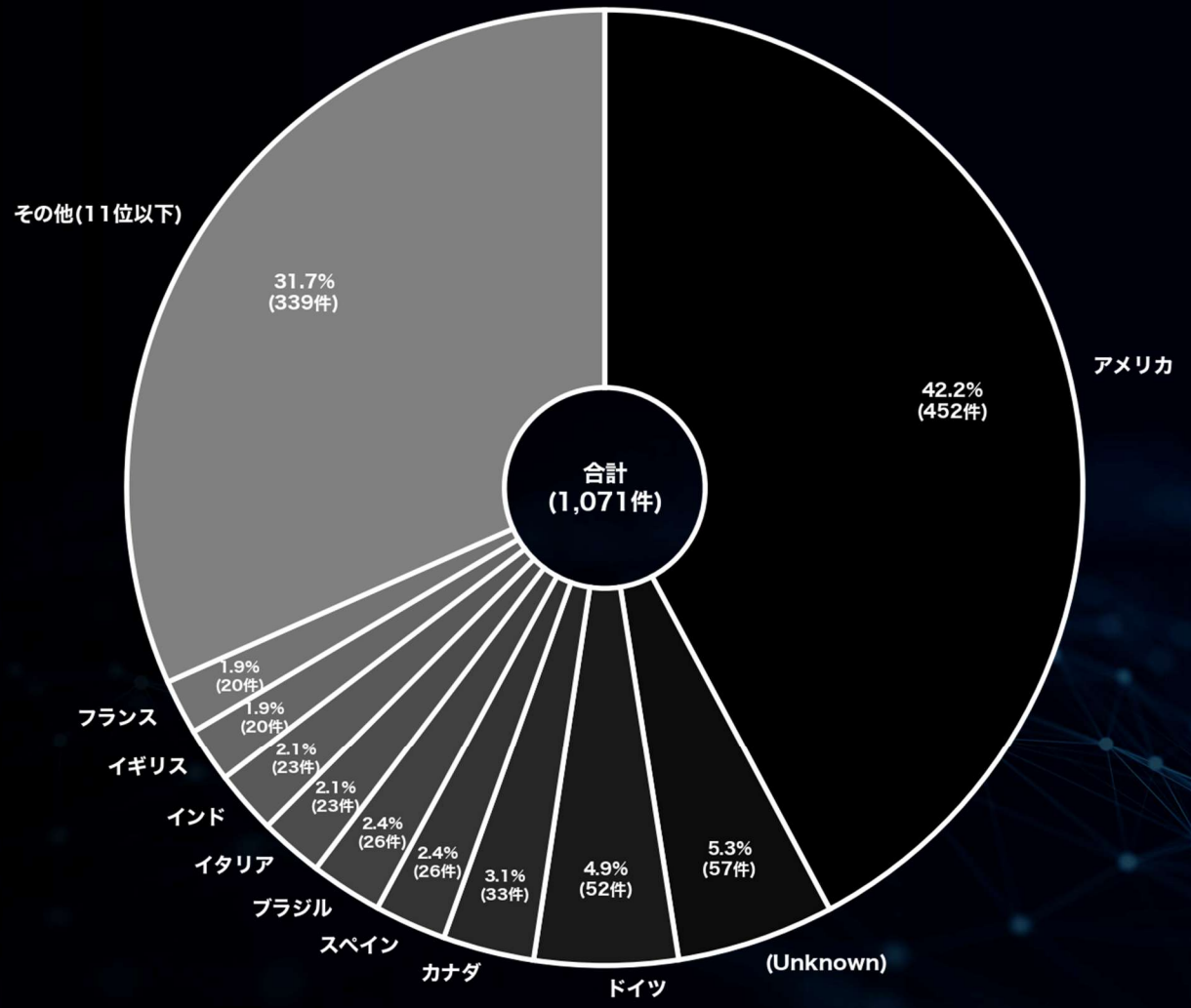
月別内訳 被害国TOP10（全世界）

（2026年 10 月）

※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	452	42.2	+ 108
(Unknown)	57	5.3	+ 17
ドイツ	52	4.9	+ 28
カナダ	33	3.1	± 0
スペイン	26	2.4	± 0
ブラジル	26	2.4	+ 3
イタリア	23	2.1	+ 1
インド	23	2.1	- 4
イギリス	20	1.9	± 0
フランス	20	1.9	- 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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

被害国 月別統計
（アジア）　（過去3ヶ月分）

2026
10

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

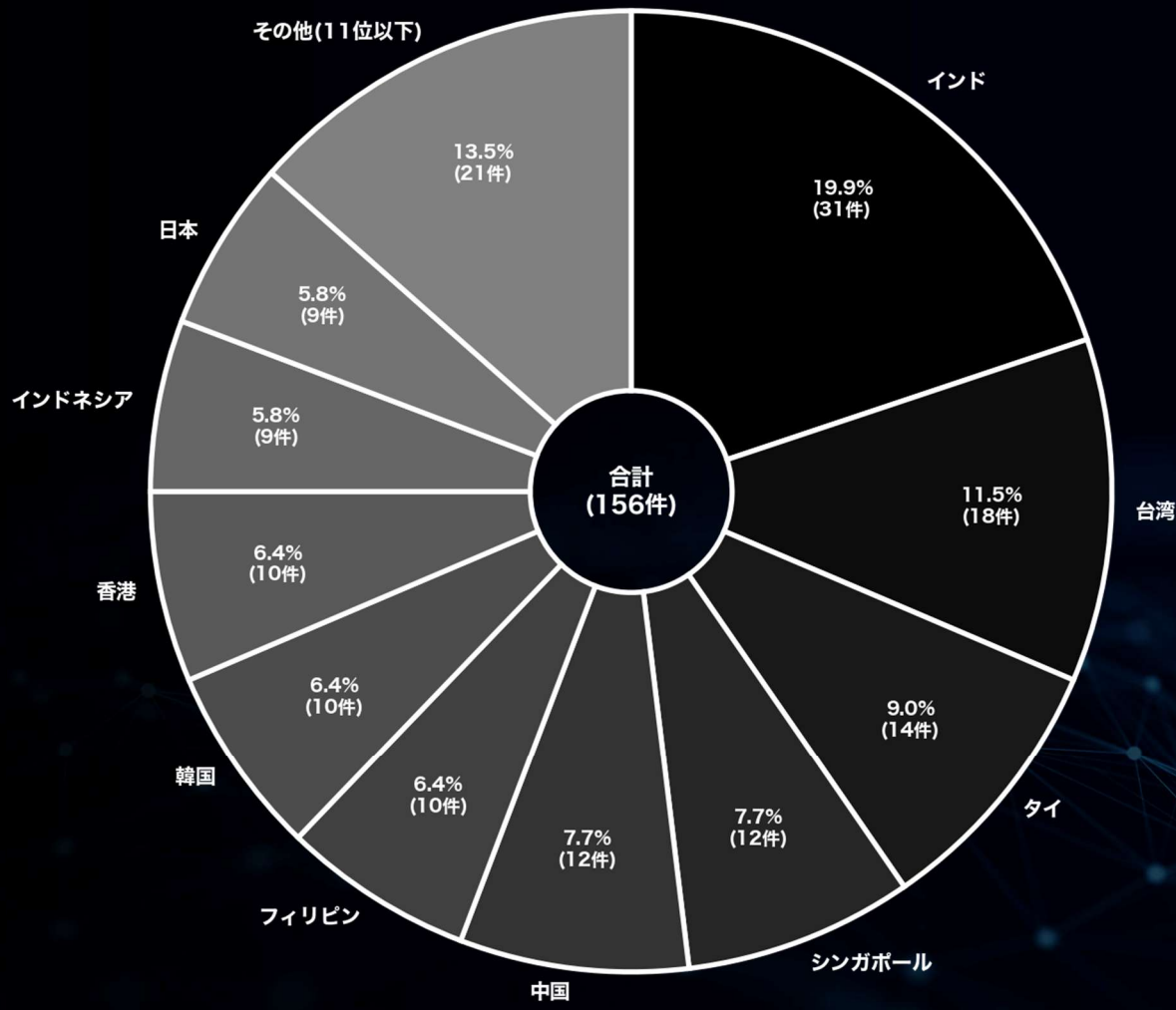
月別内訳 被害国TOP10（アジア）

（2026年 8 月）

※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	31	19.9	- 1
台湾	18	11.5	+ 8
タイ	14	9.0	+ 6
シンガポール	12	7.7	± 0
中国	12	7.7	+ 3
フィリピン	10	6.4	+ 4
韓国	10	6.4	+ 9
香港	10	6.4	+ 3
インドネシア	9	5.8	+ 3
日本	9	5.8	+ 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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

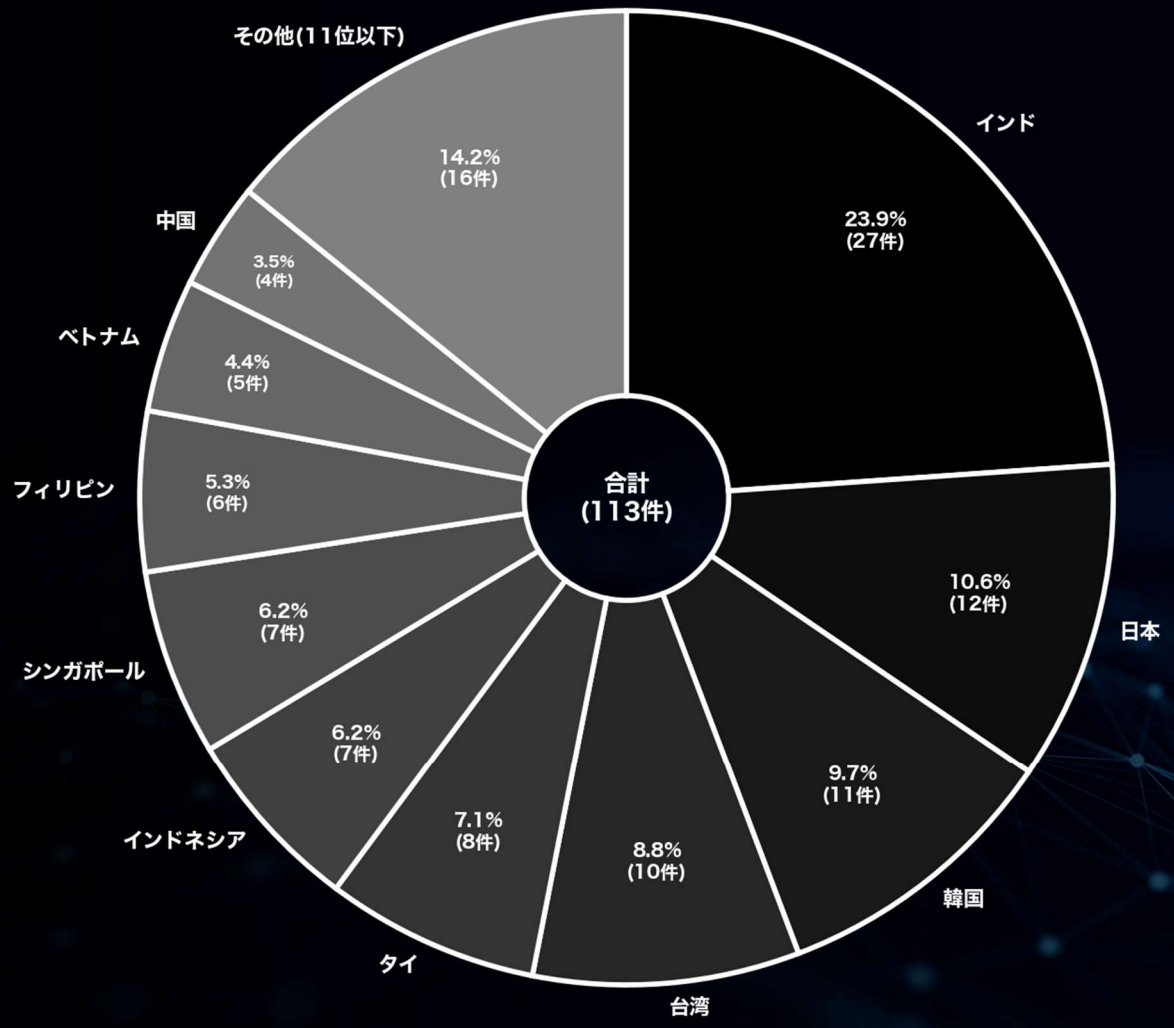
月別内訳 被害国TOP10（アジア）

（2026年 9 月）

※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	27	23.9	- 4
日本	12	10.6	+ 3
韓国	11	9.7	+ 1
台湾	10	8.8	- 8
タイ	8	7.1	- 6
インドネシア	7	6.2	- 2
シンガポール	7	6.2	- 5
フィリピン	6	5.3	- 4
ベトナム	5	4.4	- 1
中国	4	3.5	- 8

▼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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

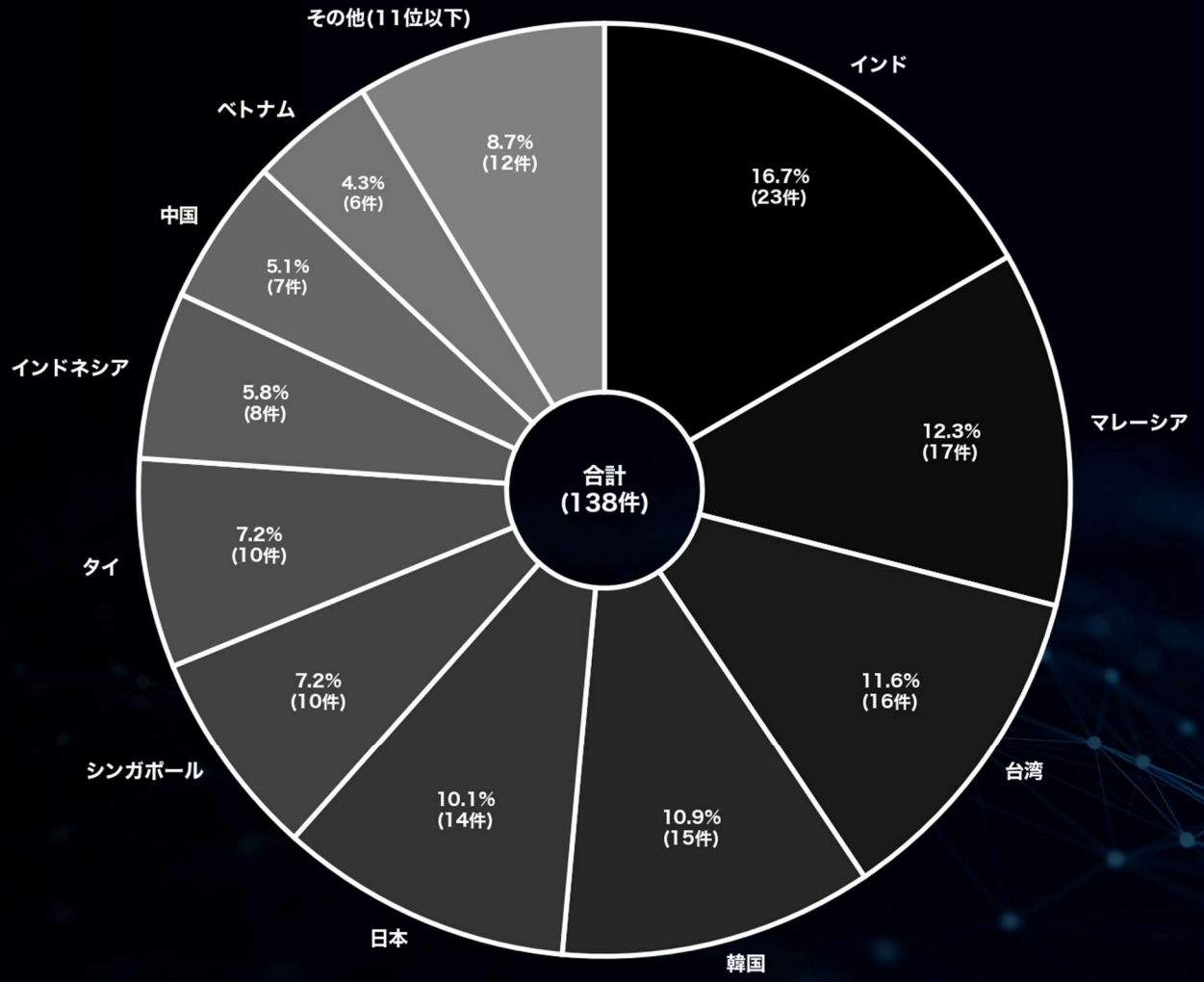
月別内訳 被害国TOP10（アジア）

（2026年 10 月）

※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	16.7	- 4
マレーシア	17	12.3	+ 15
台湾	16	11.6	+ 6
韓国	15	10.9	+ 4
日本	14	10.1	+ 2
シンガポール	10	7.2	+ 3
タイ	10	7.2	+ 2
インドネシア	8	5.8	+ 1
中国	7	5.1	+ 3
ベトナム	6	4.3	+ 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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

業種 月別統計
（全世界）　（過去3ヶ月分）

2026
10

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

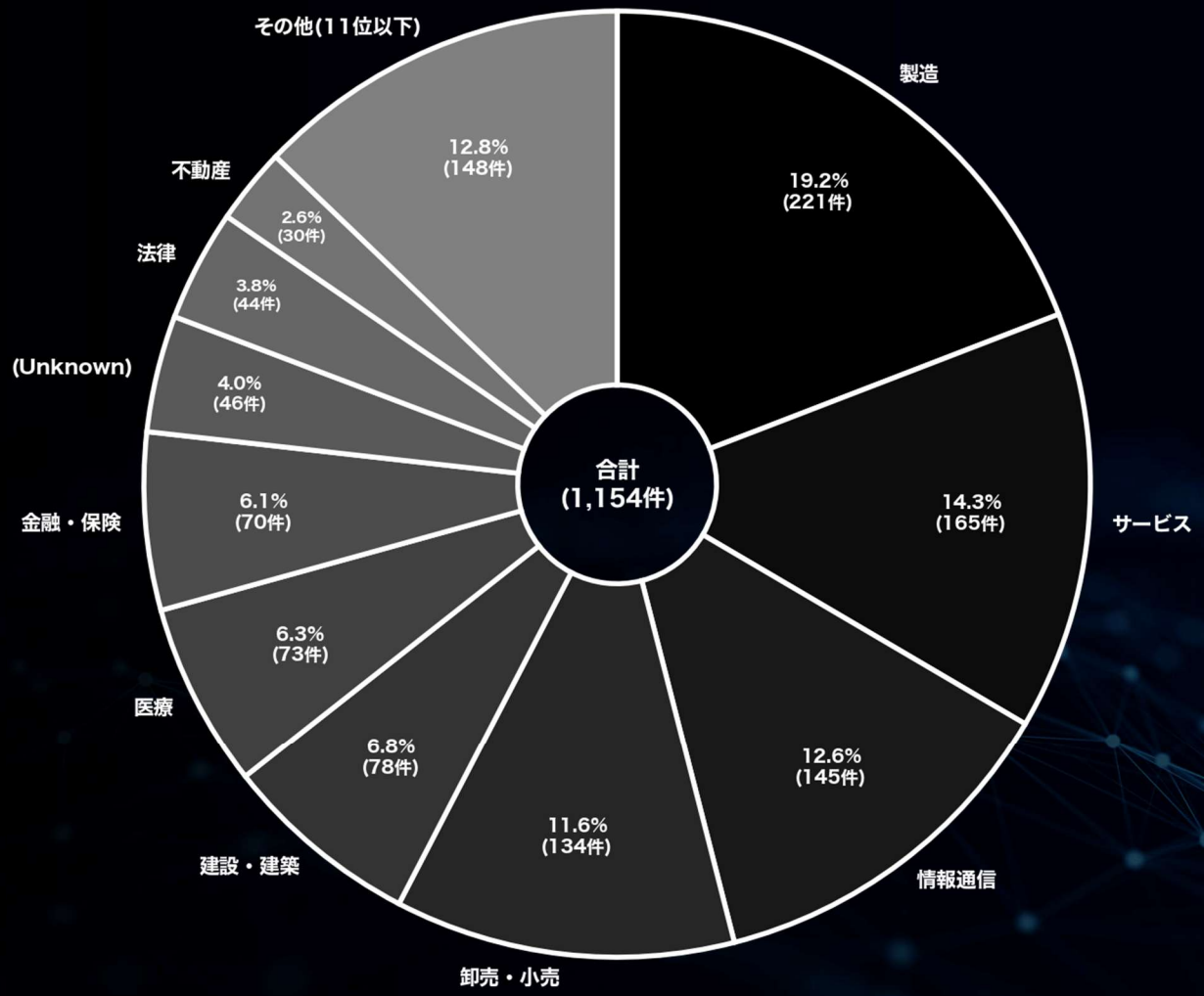
月別内訳 業種 TOP10（全世界）

（2026年 8 月）

※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	221	19.2	+ 19
サービス	165	14.3	+ 40
情報通信	145	12.6	+ 43
卸売・小売	134	11.6	+ 30
建設・建築	78	6.8	+ 8
医療	73	6.3	+ 9
金融・保険	70	6.1	+ 27
(Unknown)	46	4.0	+ 20
法律	44	3.8	+ 15
不動産	30	2.6	+ 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）



※ 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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

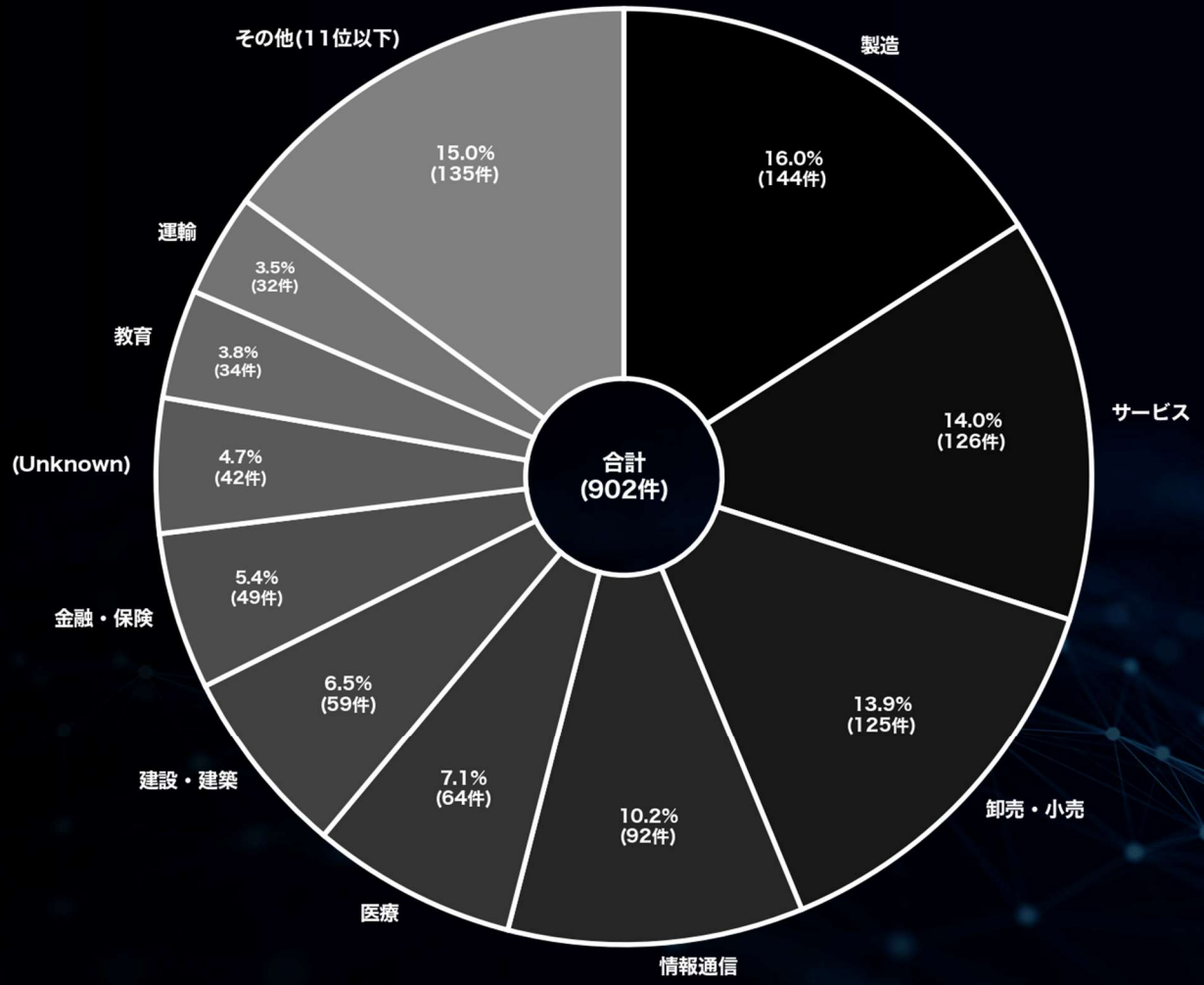
月別内訳 業種 TOP10（全世界）

（2026年 9 月）

※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	144	16.0	- 77
サービス	126	14.0	- 39
卸売・小売	125	13.9	- 9
情報通信	92	10.2	- 53
医療	64	7.1	- 9
建設・建築	59	6.5	- 19
金融・保険	49	5.4	- 21
(Unknown)	42	4.7	- 4
教育	34	3.8	+ 6
運輸	32	3.5	+ 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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

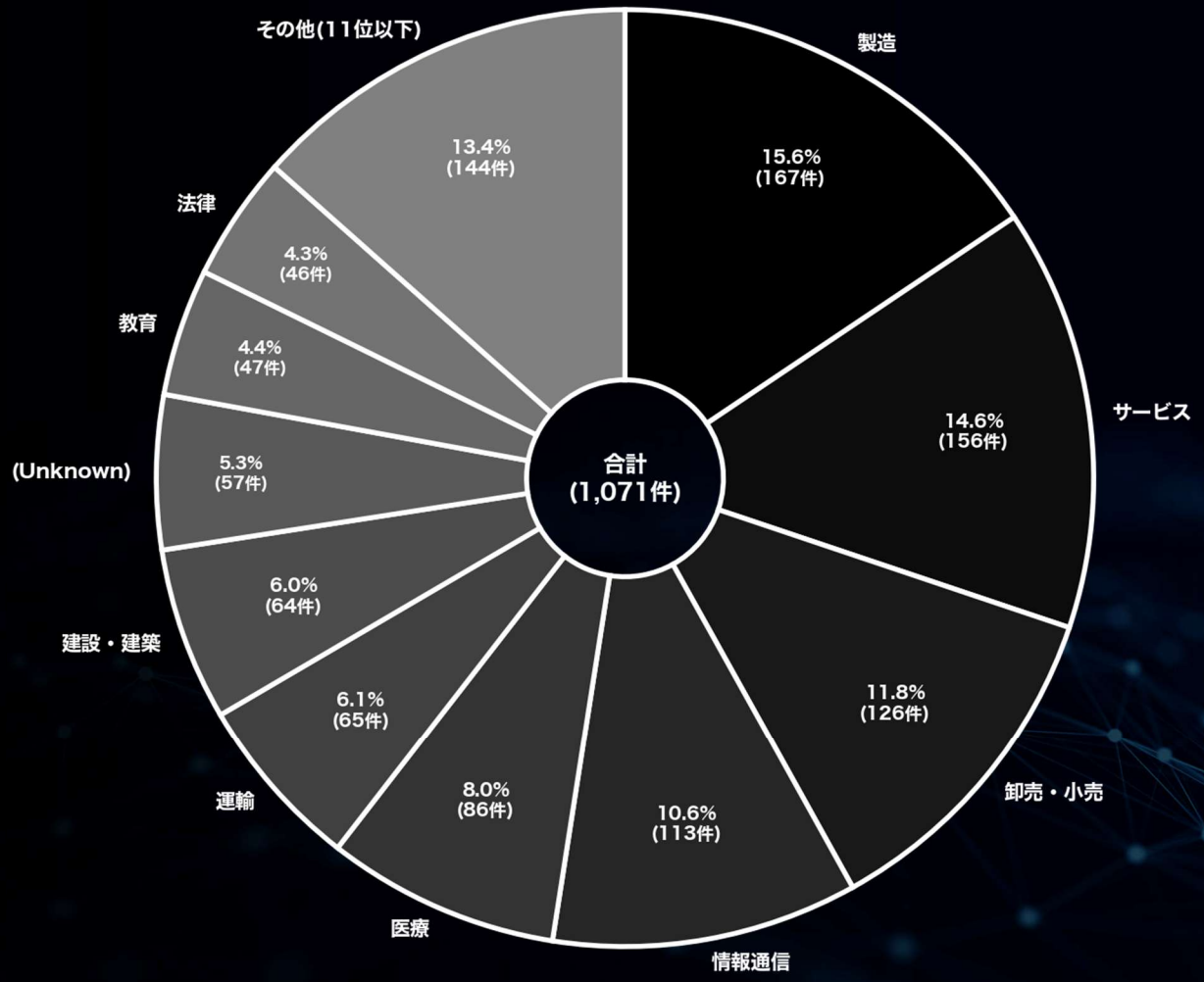
月別内訳 業種 TOP10（全世界）

（2026年 10 月）

※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	167	15.6	+ 23
サービス	156	14.6	+ 30
卸売・小売	126	11.8	+ 1
情報通信	113	10.6	+ 21
医療	86	8.0	+ 22
運輸	65	6.1	+ 33
建設・建築	64	6.0	+ 5
(Unknown)	57	5.3	+ 15
教育	47	4.4	+ 13
法律	46	4.3	+ 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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

2026

10

被害数の推移に関する統計
（全世界及び国内）

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

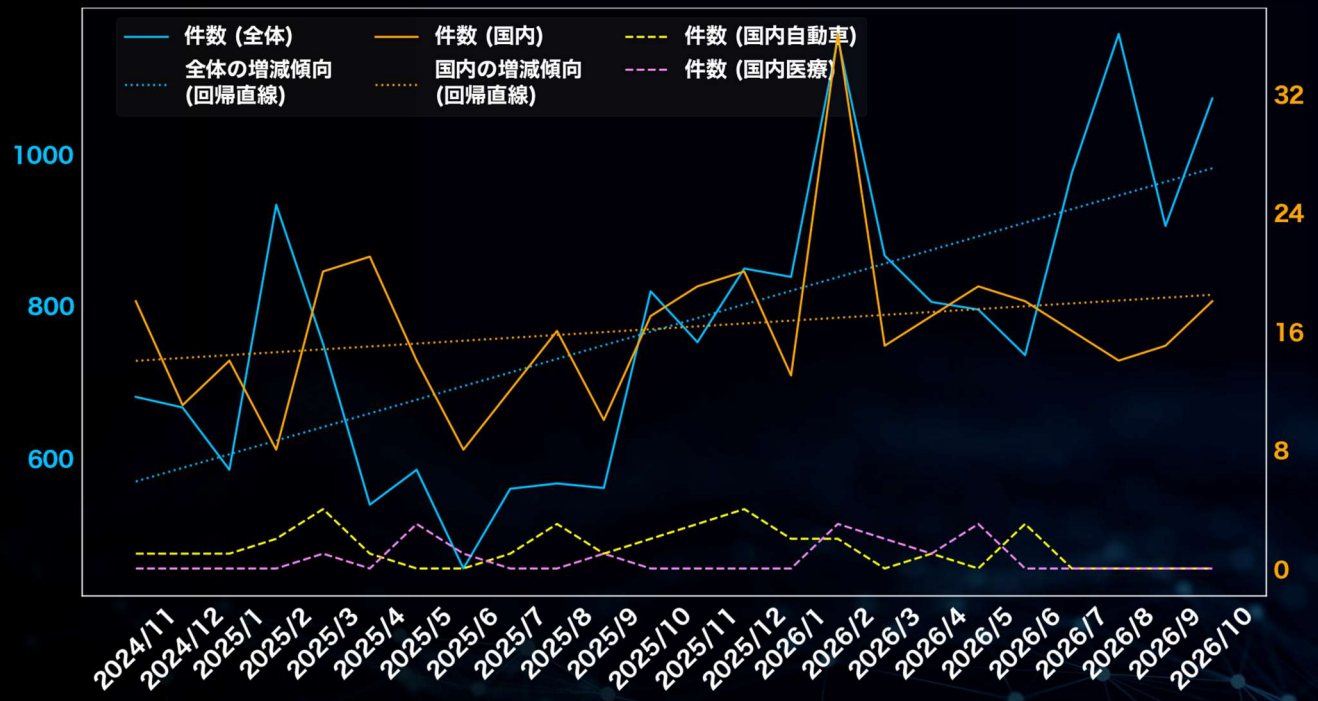
被害数の推移（全世界及び国内）
（過去2年間／2024年11月～2026年10月）

※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…	件数 (国内医療)
2024/11	680	18	1	0
2024/12	666	11	1	0
2025/1	584	14	1	0
2025/2	933	8	2	0
2025/3	750	20	4	1
2025/4	538	21	1	0
2025/5	584	14	0	3
2025/6	454	8	0	1
2025/7	559	12	1	0
2025/8	566	16	3	0
2025/9	560	10	1	1
2025/10	819	17	2	0
2025/11	752	19	3	0
2025/12	849	20	4	0
2026/1	838	13	2	0
2026/2	1152	36	2	3
2026/3	866	15	0	2
2026/4	805	17	1	1
2026/5	795	19	0	3
2026/6	735	18	3	0
2026/7	975	16	0	0
2026/8	1158	14	0	0
2026/9	905	15	0	0
2026/10	1073	18	0	0
合計	18596	389	32	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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

資本金別の統計
（国内）

2026

10

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

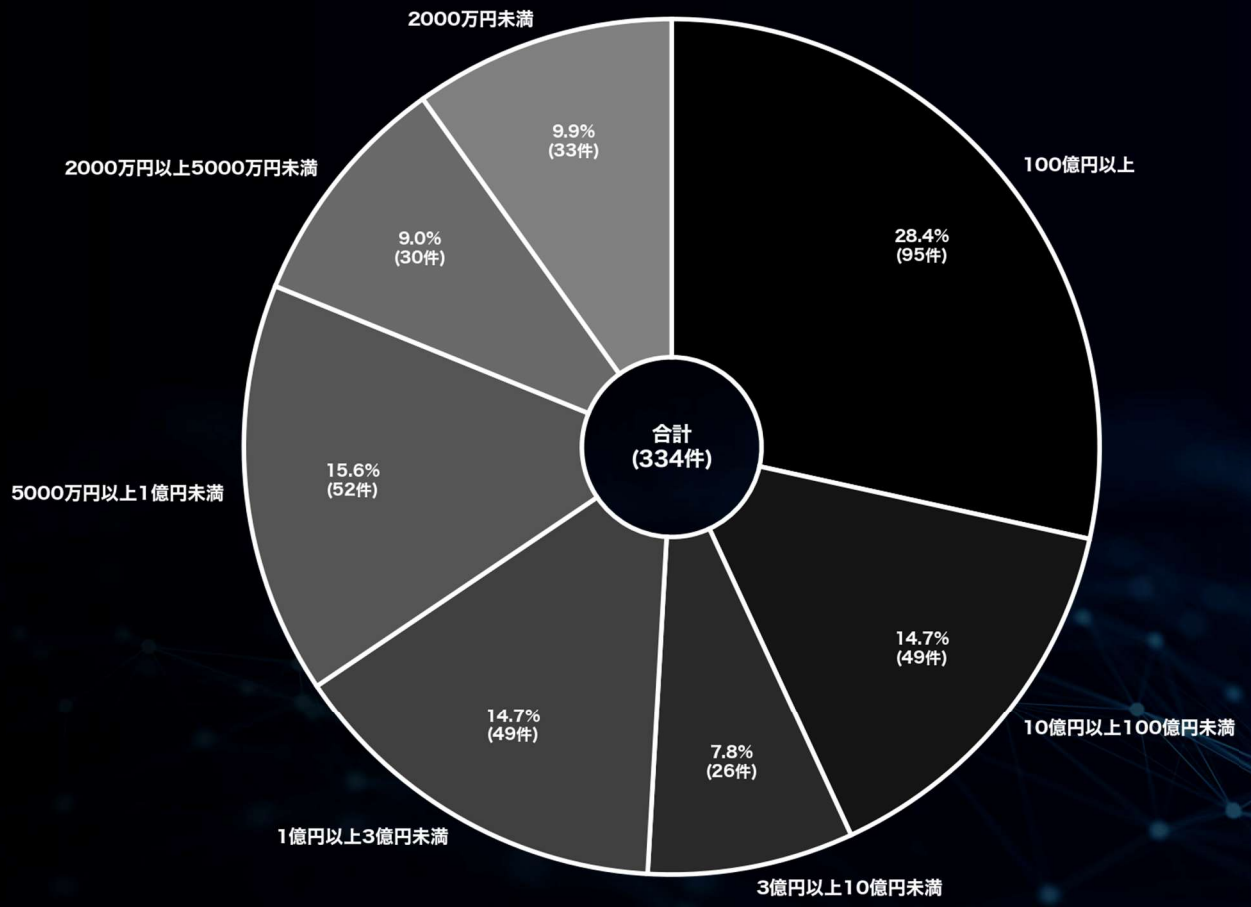
資本金別（国内）
（過去2年間／2024年11月～2026年10月）

※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	95	28.4
10億円以上100億円未満	49	14.7
3億円以上10億円未満	26	7.8
1億円以上3億円未満	49	14.7
5000万円以上1億円未満	52	15.6
2000万円以上5000万円未満	30	9.0
2000万円未満	33	9.9

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

▼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）



（※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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

公表と暴露に関する統計
（国内）

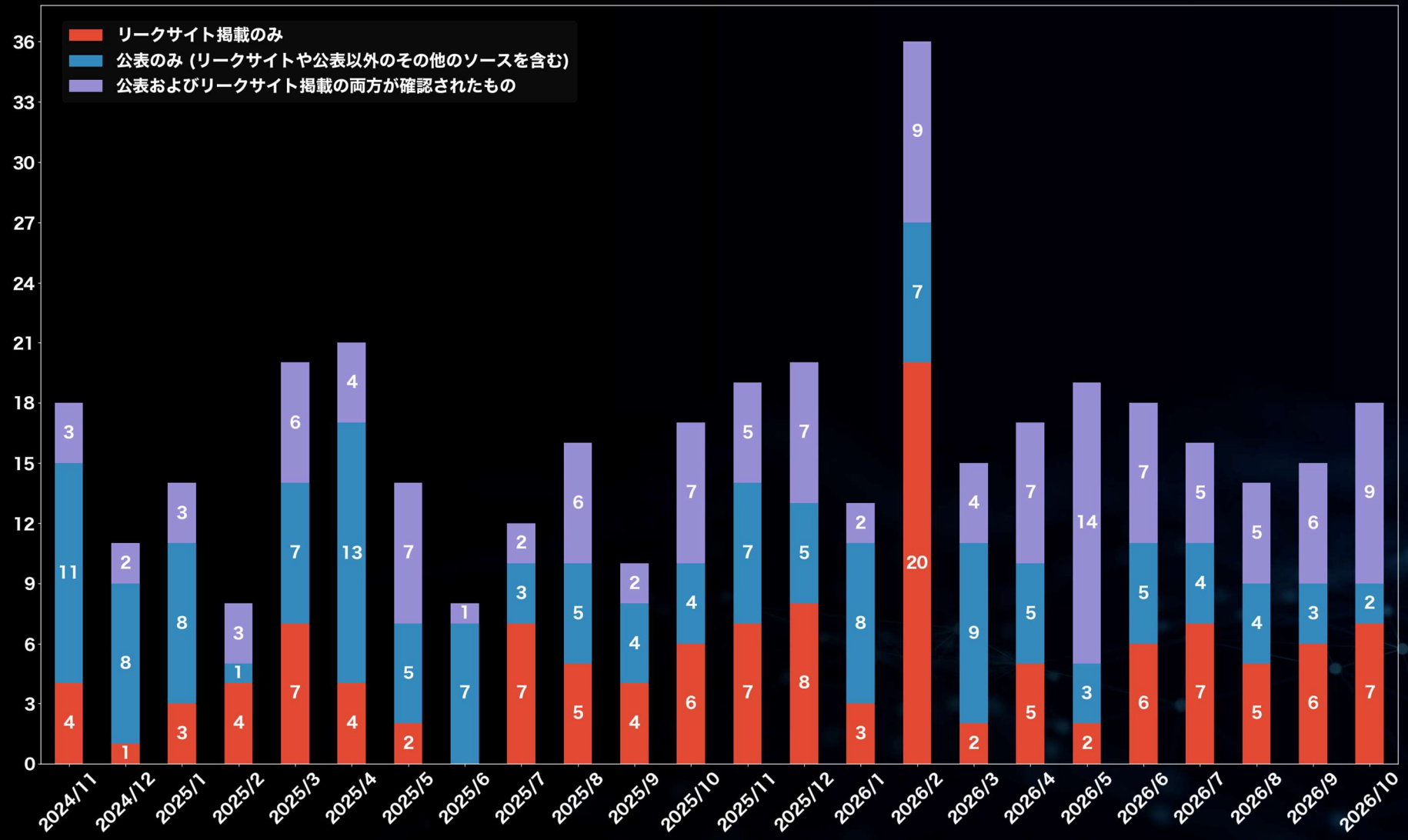
2026

10

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

公表割合 月別内訳（国内）
（過去2年間／2024年11月～2026年10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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

公となった国内被害組織 概要一覧

2026

10

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

公となった国内被害組織概要一覧（国内）
（過去1年間／2025年11月～2026年10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
2025/11	(Unknown)	私立大学
2025/11	WORLD LEAKS	プラスチック製品製造業
2025/11	Warlock	サスペンションメーカー
2025/11	Qilin (Agenda)	弁理士法人
2025/11	(Unknown)	システムインテグレーター
2025/11	Qilin (Agenda)	通信機器メーカー
2025/11	(Unknown)	雑貨・アパレル小売
2025/11	CRYPTO24	電子部品メーカー
2025/11	CL0P (CLOP)	ラベル印刷機器メーカー
2025/11	INC Ransom	自動車部品メーカー(海外拠点)
2025/11	(Unknown)	教育委員会
2025/11	(Unknown)	私立学校
2025/11	CL0P (CLOP)	大手精密機器メーカー(海外拠点)
2025/11	CL0P (CLOP)	大手自動車メーカー
2025/11	CL0P (CLOP)	大手総合化学メーカー
2025/11	Sinobi	警報装置メーカー
2025/11	Qilin (Agenda)	大手建設会社(海外拠点)
2025/11	(Unknown)	精密部品製造
2025/11	(Unknown)	国際総合検定機関
2025/12	(Unknown)	エレクトロニクス専門商社(海外拠点)
2025/12	(Unknown)	教育系ITサービス提供
2025/12	AKIRA	食用油脂メーカー(海外拠点)
2025/12	Payouts King	プラスチック精密工業部品メーカー(海外拠点)
2025/12	COINBASE CARTEL	大手半導体メーカー
2025/12	INC Ransom	ワイヤーハーネスメーカー
2025/12	Lynx	総合デベロッパー
2025/12	Qilin (Agenda)	空調・衛生設備工事(海外拠点)
2025/12	(Unknown)	総合色材・機能性化学メーカー(海外拠点)
2025/12	root	金融商品取引所
2025/12	Qilin (Agenda)	大手テクノロジー企業(海外拠点)
2025/12	Rhysida	私立学校
2025/12	Qilin (Agenda)	電気機械部品メーカー(海外拠点)
2025/12	DragonForce	自動車部品メーカー(海外拠点)
2025/12	(Unknown)	公立大学
2025/12	(Unknown)	私立大学
2025/12	Lynx	映像制作
2025/12	SAFEPAY	ECサイト運営
2025/12	Qilin (Agenda)	ソフトウェア開発
2025/12	Qilin (Agenda)	精密部品メーカー(海外拠点)
2026/1	Qilin (Agenda)	工業用計測機器メーカー
2026/1	(Unknown)	印刷サービス
2026/1	(Unknown)	ソフトウェア開発
2026/1	(Unknown)	図書整備支援
2026/1	(Unknown)	総合化学商社
2026/1	(Unknown)	生産用機械器具製造業(海外拠点)
2026/1	Everest	大手自動車メーカー
2026/1	(Unknown)	不動産管理
2026/1	Orion Leaks	タイヤメーカー(海外拠点)
2026/1	(Unknown)	飲料メーカー
2026/1	(Unknown)	スポーツ教室
2026/1	The Gentlemen	産業廃棄物処理
2026/1	Brain Cipher	システムインテグレーター
2026/2	Qilin (Agenda)	特殊金属材料・製造
2026/2	Everest	機械器具製造
2026/2	Everest	金属加工メーカー
2026/2	(Unknown)	大手化学素材メーカー(海外拠点)
2026/2	0APT	大手電気機器メーカー
2026/2	0APT	大手テクノロジー企業
2026/2	0APT	自動制御機器製品メーカー
2026/2	(Unknown)	ペット関連用品製造
2026/2	0APT	医療機器メーカー
2026/2	0APT	医療機器メーカー
2026/2	(Unknown)	スキー場運営
2026/2	INC Ransom	国際貨物運送取扱業
2026/2	The Gentlemen	伝熱管メーカー
2026/2	0APT	タイヤメーカー
2026/2	0APT	総合電機メーカー
2026/2	0APT	大手自動車メーカー
2026/2	0APT	建設機械メーカー
2026/2	0APT	総合電機メーカー
2026/2	(Unknown)	ソフトウェア開発
2026/2	Qilin (Agenda)	総合デベロッパー
2026/2	(Unknown)	ホテル業・飲食店業
2026/2	0APT	鉄道会社
2026/2	0APT	地方自治体
2026/2	0APT	電力会社
2026/2	0APT	地方自治体
2026/2	Qilin (Agenda)	種苗メーカー兼商社(海外拠点)
2026/2	NightSpire	繊維・衣料関連卸売業
2026/2	(Unknown)	半導体試験装置メーカー
2026/2	NetRunner	総合病院
2026/2	LockBit	機械・工具メーカー(海外拠点)
2026/2	BLACKSHRANTAC	紳士服・婦人服販売
2026/2	NightSpire	モータースポーツチーム運営
2026/2	(Unknown)	印刷会社
2026/2	INC Ransom	石油製品・LPガス販売
2026/2	The Gentlemen	材料加工装置メーカー
2026/2	Everest	商用車メーカー
2026/3	(Unknown)	市場調査・コンサルティング
2026/3	NetRunner	療養型病院
2026/3	(Unknown)	FAX通信・BPOサービス
2026/3	(Unknown)	工業用ゴム・樹脂・配管資材商社
2026/3	(Unknown)	住宅・商業施設向けリペア
2026/3	(Unknown)	美容クリニック
2026/3	(Unknown)	シティホテル運営
2026/3	The Gentlemen	医療・看護専門出版社
2026/3	Space Bears	介護・カラオケ・飲食事業
2026/3	(Unknown)	光半導体デバイスメーカー(海外拠点)
2026/3	WORLD LEAKS	広告・制作
2026/3	The Gentlemen	繊維加工・食品加工メーカー
2026/3	(Unknown)	設備工事
2026/3	(Unknown)	美容室向け化粧品メーカー
2026/3	ALP-001	国立研究開発法人
2026/4	AKIRA	流体システム製品メーカー
2026/4	(Unknown)	非鉄金属・資源開発(海外拠点)
2026/4	(Unknown)	システムインテグレーター
2026/4	KRYBIT	酒類製造業
2026/4	LockBit	水処理・環境設備
2026/4	DragonForce	オフィス家具メーカー(海外拠点)
2026/4	(Unknown)	診療予約システム開発
2026/4	Qilin (Agenda)	舗装・土木工事

（※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）

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

公となった国内被害組織概要一覧（国内）
（過去1年間／2025年11月～2026年10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
2026/4	The Gentlemen	電気機器メーカー
2026/4	Qilin (Agenda)	建設資材・福祉用具のレンタル・販売
2026/4	(Unknown)	生活協同組合
2026/4	COINBASE CARTEL	大学研究会
2026/4	Ransom EXX	ソフトウェア開発
2026/4	LockBit	電子部品(コネクタ)製造(海外拠点)
2026/4	(Unknown)	二輪用品専門チェーン
2026/4	The Gentlemen	ソフトウェア開発
2026/4	Qilin (Agenda)	大手自動車部品メーカー(海外拠点)
2026/5	(Unknown)	百貨店業・不動産賃貸業
2026/5	FulcrumSec	移植医療支援
2026/5	KILLSEC	オンライン処方箋サービス
2026/5	(Unknown)	教育サービス・学習教材
2026/5	AiLock	半導体製造装置・精密機器メーカー(海外拠点)
2026/5	The Gentlemen	医薬品卸売業
2026/5	The Gentlemen	商業施設運営サービス
2026/5	SAFEPAY	産業資材商社
2026/5	AKIRA	家電メーカー(海外拠点)
2026/5	Lynx	水処理装置メーカー(海外拠点)
2026/5	Lynx	蓄電池・電源システム(海外拠点)
2026/5	Metaencryptor	空調メーカー
2026/5	The Gentlemen	ジュエリー輸入・企画販売
2026/5	Payload	空調設備施工
2026/5	The Gentlemen	ガラス容器メーカー
2026/5	NightSpire	医薬品・食品関連製造(海外拠点)
2026/5	(Unknown)	国立大学法人
2026/5	SAFEPAY	紙器製造
2026/5	SAFEPAY	建材リペア・再生工事
2026/6	SAFEPAY	楽器メーカー(海外拠点)
2026/6	(Unknown)	サポーター・健康用品製造販売
2026/6	(Unknown)	化粧品・健康食品製造販売、エステ運営
2026/6	STORMOUS	化学系専門商社(海外拠点)
2026/6	(Unknown)	米穀・飼料・食品卸売等
2026/6	(Unknown)	ローカルキャラクターの活動支援
2026/6	SAFEPAY	音楽系書籍販売
2026/6	(Unknown)	シェアモビリティ、駐車場運営
2026/6	Qilin (Agenda)	トラック・バス等の製造販売(海外拠点)

被害月	攻撃グループ	業種概要
2026/6	CMD ORGANIZATION	ロボットシステムインテグレーター
2026/6	SHADOWBYT3$	大手ゲーム機・ゲームソフトメーカー(海外拠点)
2026/6	AUR0RA	非鉄金属・自動車部品メーカー(海外拠点)
2026/6	SAFEPAY	建設コンサルタント
2026/6	LockBit	自動車部品・合成樹脂製品メーカー(海外拠点)
2026/6	BlackField	自動車部品メーカー(海外拠点)
2026/6	DragonForce	特殊弁メーカー
2026/6	Qilin (Agenda)	私立大学
2026/6	The Gentlemen	化粧品・健康食品製造販売
2026/7	(Unknown)	私立中学・高等学校
2026/7	(Unknown)	引越し・配送会社
2026/7	(Unknown)	総合アパレル業
2026/7	(Unknown)	穀物乾燥機メーカー
2026/7	AiLock	大手タクシー会社
2026/7	AiLock	業務用ソフトウェア開発会社
2026/7	COINBASE CARTEL	航空機向け電子機器メーカー(海外拠点)
2026/7	CHAOS (2025)	大手酒類・食品持株会社(海外拠点)
2026/7	The Gentlemen	排水処理設備メーカー
2026/7	The Gentlemen	ソフトウェア開発会社
2026/7	INC Ransom	特装車メーカー
2026/7	INC Ransom	大手酒類・食品持株会社(海外拠点)
2026/7	RansomHouse	大手冷凍食品メーカー
2026/7	Morpheus	めっき・樹脂成形メーカー(海外拠点)
2026/7	GLOBAL SECRET GROUP	オンラインゲーム会社
2026/7	Everest	ITサービス会社
2026/8	SAFEPAY	不動産コンサルティング・資産管理
2026/8	OROVA	複合機・OA機器・オフィス家具販売・保守
2026/8	(Unknown)	システムインテグレーター
2026/8	AiLock	温室・農業資材メーカー
2026/8	AiLock	食品スーパーマーケット
2026/8	COINBASE CARTEL	精密機器メーカー
2026/8	The Gentlemen	総合建設業
2026/8	MEDUZALOCKER	産業廃棄物収集運搬・処分業者
2026/8	(Unknown)	システムインテグレーター
2026/8	SETTRA	賃貸管理・サブリース
2026/8	The Gentlemen	産業用機械・生産設備メーカー

被害月	攻撃グループ	業種概要
2026/8	(Unknown)	総合建築事業・総合人材サービス業
2026/8	KRYBIT	建設資材メーカー(海外拠点)
2026/8	(Unknown)	印刷用インキ・合成樹脂メーカー
2026/9	RansomHouse	リユース・エンタメ小売(WonderGOO等)の持株…
2026/9	(Unknown)	システムインテグレーター
2026/9	(Unknown)	地方自治体
2026/9	Qilin (Agenda)	樹脂専門商社
2026/9	AUDIT	不明
2026/9	Metaencryptor	鉄鋼メーカー
2026/9	The Gentlemen	アパレル副資材・RFIDタグメーカー
2026/9	(Unknown)	時計修理
2026/9	SAFEPAY	ソフトウェア開発
2026/9	VEXY	事務機器・OA機器販売
2026/9	Qilin (Agenda)	放送機器メーカー
2026/9	Metaencryptor	自動車部品メーカー
2026/9	Everest	ソフトウェア開発
2026/9	Qilin (Agenda)	配電盤・制御盤・監視システムメーカー
2026/9	Qilin (Agenda)	倉庫・物流業
2026/10	ECLIPSE	英字新聞社
2026/10	(Unknown)	公立大学
2026/10	Qilin (Agenda)	生コンクリート製造販売
2026/10	(Unknown)	クラウドサービス・データセンター事業者
2026/10	EXITIM	切断機・溶接機材・産業用ガスメーカー
2026/10	N0N	外航旅客・貨物船運航
2026/10	N0N	外航海運
2026/10	N0N	国際総合物流(海外拠点)
2026/10	ECLIPSE	医薬品・食品関連製造(海外拠点)
2026/10	Qilin (Agenda)	鉄道事業者
2026/10	The Gentlemen	国立大学法人
2026/10	Everest	麺類製造販売・商社
2026/10	Everest	伸縮継手・ダンパメーカー
2026/10	VEXY	政策情報プラットフォーム開発・提供
2026/10	Qilin (Agenda)	不動産投資・アセットマネジメント
2026/10	BLACKX	医療情報提供サービス
2026/10	SAFEPAY	私立大学
2026/10	Qilin (Agenda)	高機能材料メーカー

（※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
© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

公となった国内被害組織における拠点割合（国内）

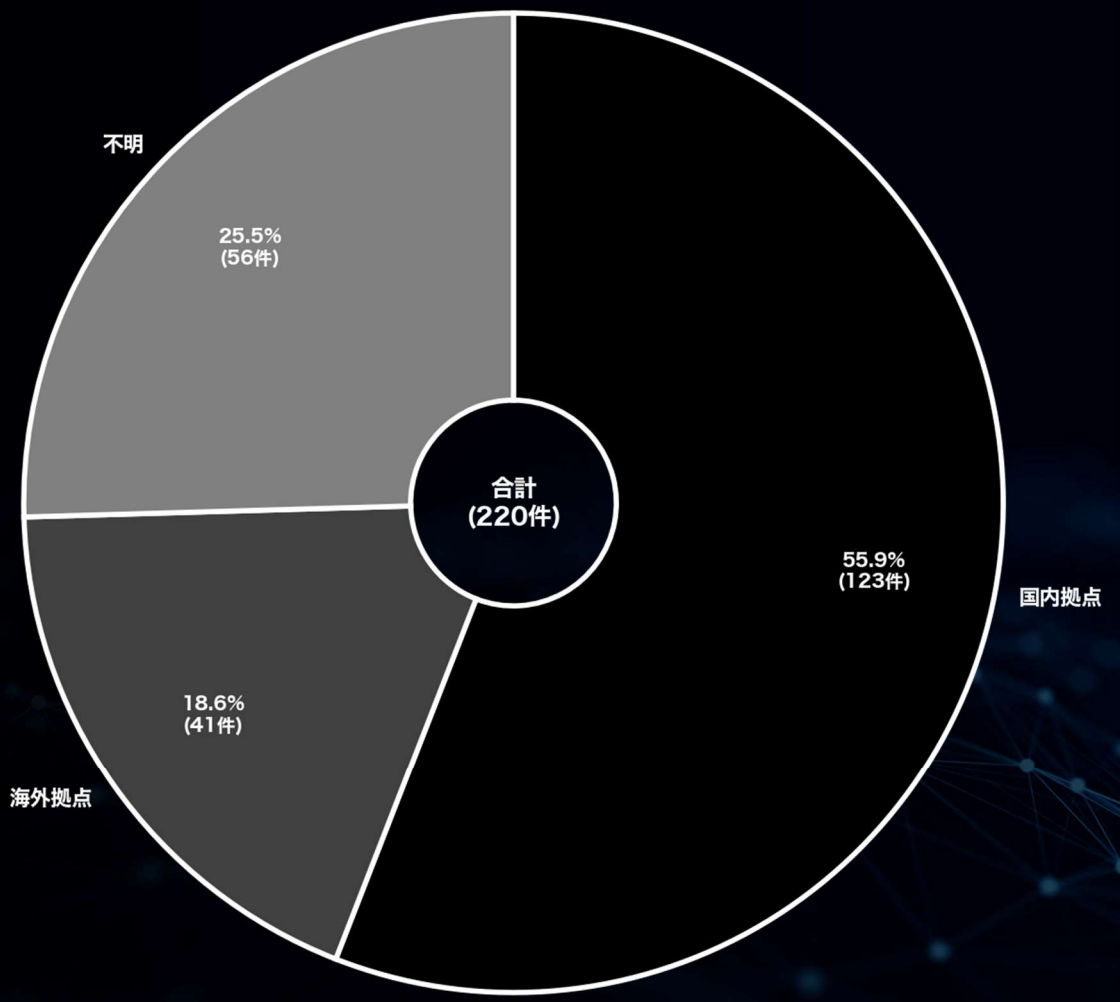
（過去1年間／2025年11月～2026年10月）

（※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	123	55.9
海外拠点	41	18.6
不明	56	25.5

▼ランサムウェア攻撃を受けた日本関連組織の拠点別割合



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

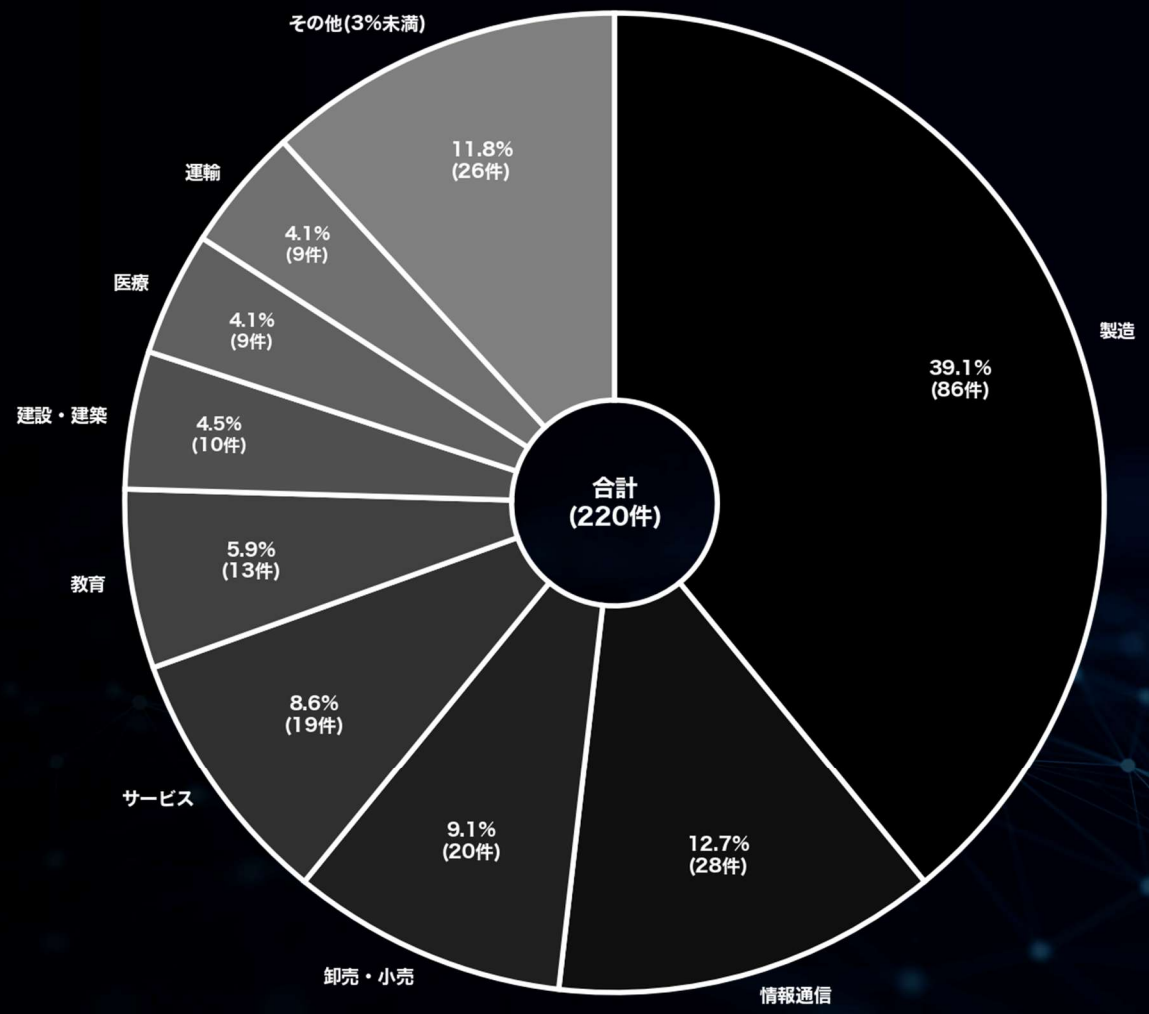
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

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／2025年11月～2026年10月）

業種	件数	割合(%)
製造	86	39.1
情報通信	28	12.7
卸売・小売	20	9.1
サービス	19	8.6
教育	13	5.9
建設・建築	10	4.5
医療	9	4.1
運輸	9	4.1
その他(3%未満)	26	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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

2026

10

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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

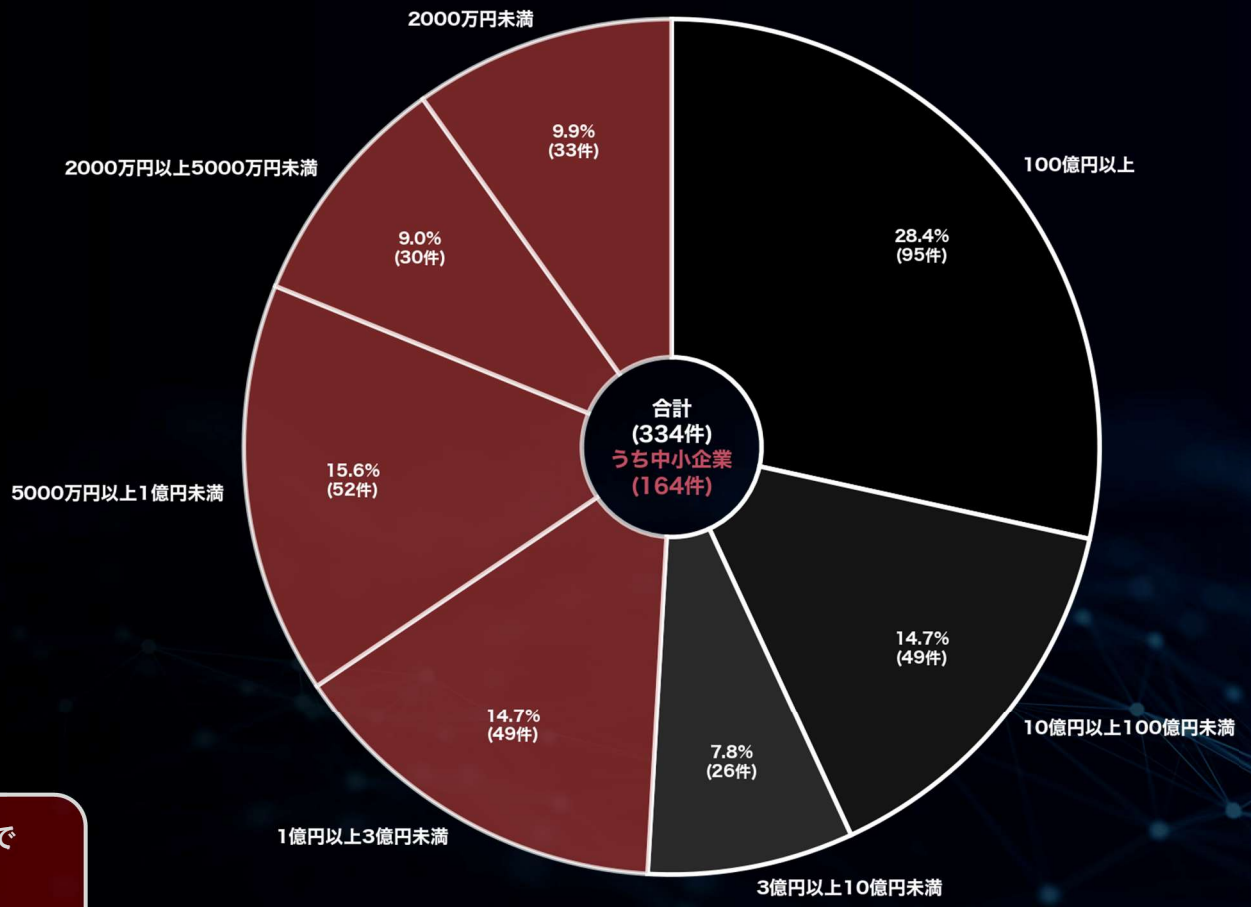
資本金別（国内-中小企業）
（過去2年間／2024年11月～2026年10月）

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	95	28.4
10億円以上100億円未満	49	14.7
3億円以上10億円未満	26	7.8
1億円以上3億円未満	49	14.7
5000万円以上1億円未満	52	15.6
2000万円以上5000万円未満	30	9.0
2000万円未満	33	9.9

▼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）



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164件にのぼり、全体の49.1%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

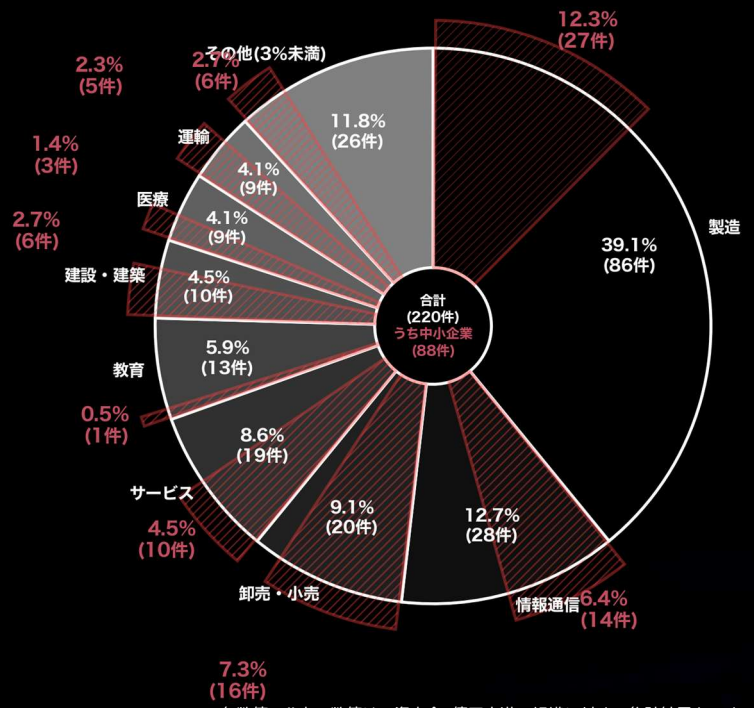
© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

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／2025年11月～2026年10月）

赤色は中小企業を示す

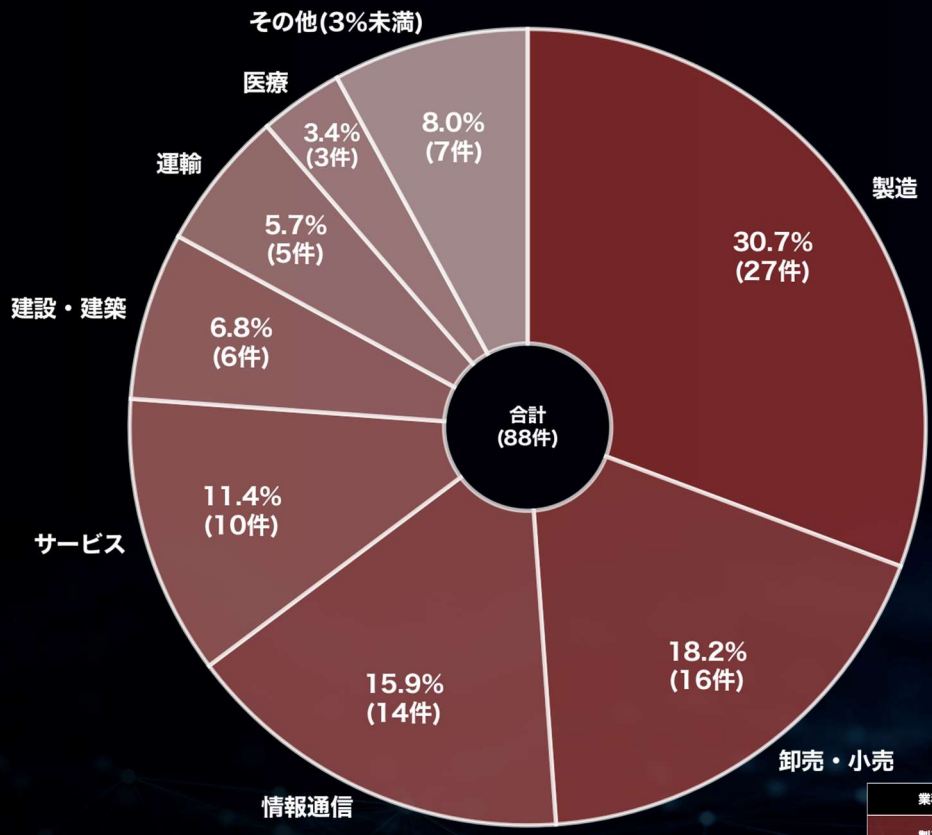
▼全体割合



※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	86 (27)	39.1 (12.3)
情報通信	28 (14)	12.7 (6.4)
卸売・小売	20 (16)	9.1 (7.3)
サービス	19 (10)	8.6 (4.5)
教育	13 (1)	5.9 (0.5)
建設・建築	10 (6)	4.5 (2.7)
医療	9 (3)	4.1 (1.4)
運輸	9 (5)	4.1 (2.3)
その他(3%未満)	26 (6)	11.8 (2.7)

▼中小企業のみの割合



業種	件数	割合(%)
製造	27	30.7
卸売・小売	16	18.2
情報通信	14	15.9
サービス	10	11.4
建設・建築	6	6.8
運輸	5	5.7
医療	3	3.4
その他(3%未満)	7	8.0

過去1年間の業種別分析においては、中小企業のみに限定すると、被害件数の割合は業種を問わず、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

（※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

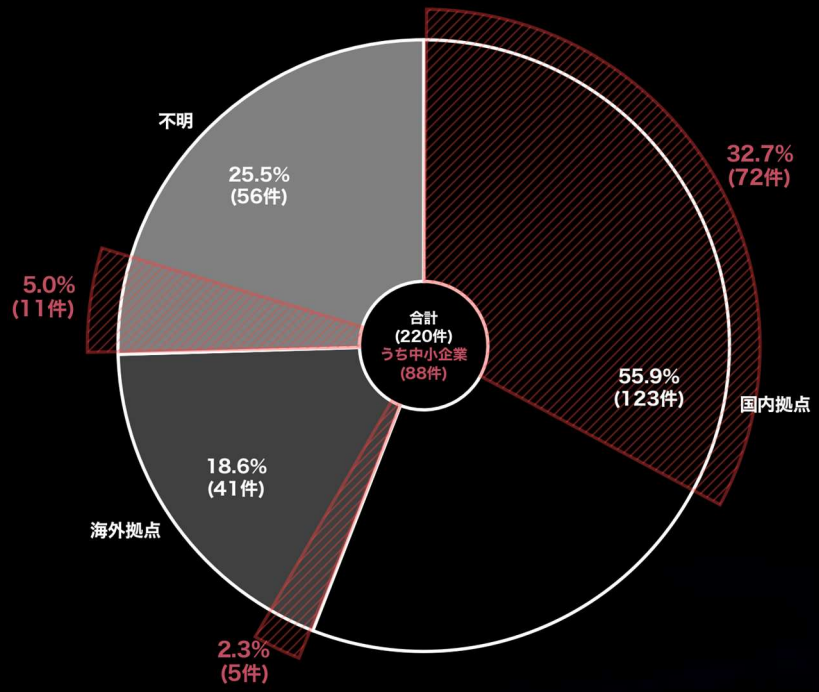
© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

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）

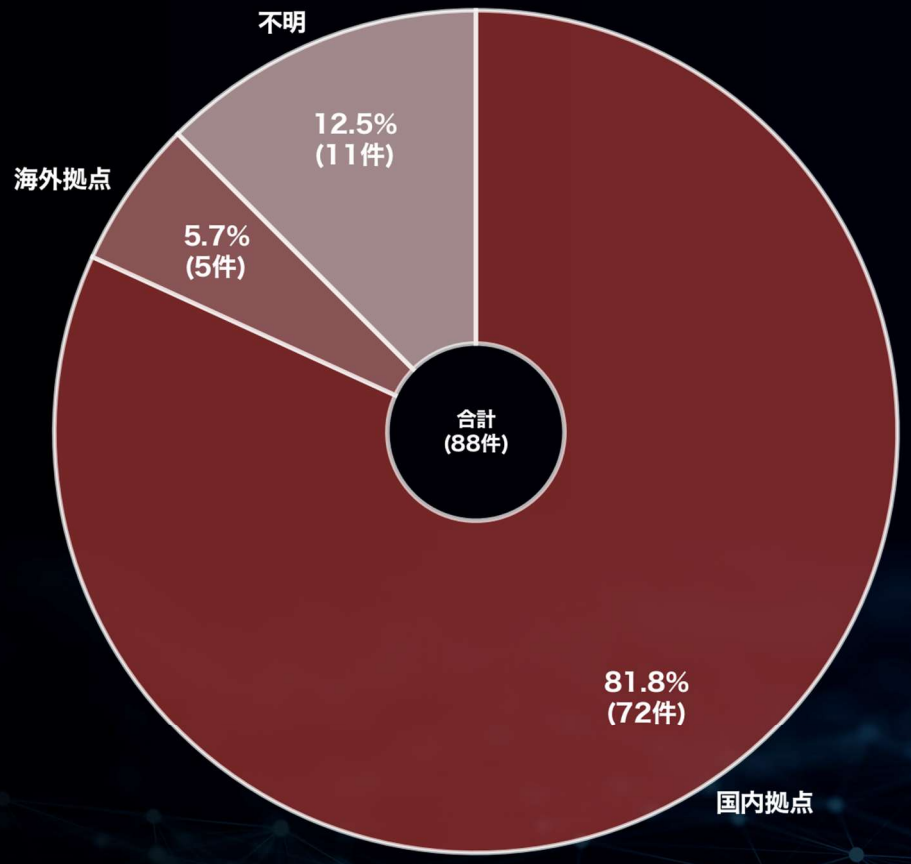
（過去1年間／2025年11月～2026年10月）

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3億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	123 (72)	55.9 (32.7)
海外拠点	41 (5)	18.6 (2.3)
不明	56 (11)	25.5 (5.0)
合計	220 (88)	100 (40.0)

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	72	81.8
海外拠点	5	5.7
不明	11	12.5

（※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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

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／2025年11月～2026年10月）

赤色は中小企業を示す

被害月	攻撃グループ	業種概要
2025/11	(Unknown)	私立大学
2025/11	WORLD LEAKS	プラスチック製品製造業
2025/11	Warlock	サスペンションメーカー
2025/11	Qilin (Agenda)	弁理士法人
2025/11	(Unknown)	システムインテグレーター
2025/11	Qilin (Agenda)	通信機器メーカー
2025/11	(Unknown)	雑貨・アパレル小売
2025/11	CRYPTO24	電子部品メーカー
2025/11	CL0P (CLOP)	ラベル印刷機器メーカー
2025/11	INC Ransom	自動車部品メーカー(海外拠点)
2025/11	(Unknown)	教育委員会
2025/11	(Unknown)	私立学校
2025/11	CL0P (CLOP)	大手精密機器メーカー(海外拠点)
2025/11	CL0P (CLOP)	大手自動車メーカー
2025/11	CL0P (CLOP)	大手総合化学メーカー
2025/11	Sinobi	警報装置メーカー
2025/11	Qilin (Agenda)	大手建設会社(海外拠点)
2025/11	(Unknown)	精密部品製造
2025/11	(Unknown)	国際総合検定機関
2025/12	(Unknown)	エレクトロニクス専門商社(海外拠点)
2025/12	(Unknown)	教育系ITサービス提供
2025/12	AKIRA	食用油脂メーカー(海外拠点)
2025/12	Payouts King	プラスチック精密工業部品メーカー(海外拠点)
2025/12	COINBASE CARTEL	大手半導体メーカー
2025/12	INC Ransom	ワイヤーハーネスメーカー
2025/12	Lynx	総合デベロッパー
2025/12	Qilin (Agenda)	空調・衛生設備工事(海外拠点)
2025/12	(Unknown)	総合色材・機能性化学メーカー(海外拠点)
2025/12	root	金融商品取引所
2025/12	Qilin (Agenda)	大手テクノロジー企業(海外拠点)
2025/12	Rhysida	私立学校
2025/12	Qilin (Agenda)	電気機械部品メーカー(海外拠点)
2025/12	DragonForce	自動車部品メーカー(海外拠点)
2025/12	(Unknown)	公立大学
2025/12	(Unknown)	私立大学
2025/12	Lynx	映像制作
2025/12	SAFEPAY	ECサイト運営

被害月	攻撃グループ	業種概要
2025/12	Qilin (Agenda)	ソフトウェア開発
2025/12	Qilin (Agenda)	精密部品メーカー(海外拠点)
2026/1	Qilin (Agenda)	工業用計測機器メーカー
2026/1	(Unknown)	印刷サービス
2026/1	(Unknown)	ソフトウェア開発
2026/1	(Unknown)	図書整備支援
2026/1	(Unknown)	総合化学商社
2026/1	(Unknown)	生産用機械器具製造業(海外拠点)
2026/1	Everest	大手自動車メーカー
2026/1	(Unknown)	不動産管理
2026/1	Orion Leaks	タイヤメーカー(海外拠点)
2026/1	(Unknown)	飲料メーカー
2026/1	(Unknown)	スポーツ教室
2026/1	The Gentlemen	産業廃棄物処理
2026/1	Brain Cipher	システムインテグレーター
2026/2	Qilin (Agenda)	特殊金属材料・製造
2026/2	Everest	機械器具製造
2026/2	Everest	金属加工メーカー
2026/2	(Unknown)	大手化学素材メーカー(海外拠点)
2026/2	0APT	大手電気機器メーカー
2026/2	0APT	大手テクノロジー企業
2026/2	0APT	自動制御機器製品メーカー
2026/2	(Unknown)	ペット関連用品製造
2026/2	0APT	医療機器メーカー
2026/2	0APT	医療機器メーカー
2026/2	(Unknown)	スキー場運営
2026/2	INC Ransom	国際貨物運送取扱業
2026/2	The Gentlemen	伝熱管メーカー
2026/2	0APT	タイヤメーカー
2026/2	0APT	総合電機メーカー
2026/2	0APT	大手自動車メーカー
2026/2	0APT	建設機械メーカー
2026/2	0APT	総合電機メーカー
2026/2	(Unknown)	ソフトウェア開発
2026/2	Qilin (Agenda)	総合デベロッパー
2026/2	(Unknown)	ホテル業・飲食店業
2026/2	0APT	鉄道会社

被害月	攻撃グループ	業種概要
2026/2	0APT	地方自治体
2026/2	0APT	電力会社
2026/2	0APT	地方自治体
2026/2	Qilin (Agenda)	種苗メーカー兼商社(海外拠点)
2026/2	NightSpire	繊維・衣料関連卸売業
2026/2	(Unknown)	半導体試験装置メーカー
2026/2	NetRunner	総合病院
2026/2	LockBit	機械・工具メーカー(海外拠点)
2026/2	BLACKSHRANTAC	紳士服・婦人服販売
2026/2	NightSpire	モータースポーツチーム運営
2026/2	(Unknown)	印刷会社
2026/2	INC Ransom	石油製品・LPガス販売
2026/2	The Gentlemen	材料加工装置メーカー
2026/2	Everest	商用車メーカー
2026/3	(Unknown)	市場調査・コンサルティング
2026/3	NetRunner	療養型病院
2026/3	(Unknown)	FAX通信・BPOサービス
2026/3	(Unknown)	工業用ゴム・樹脂・配管資材商社
2026/3	(Unknown)	住宅・商業施設向けリペア
2026/3	(Unknown)	美容クリニック
2026/3	(Unknown)	シティホテル運営
2026/3	The Gentlemen	医療・看護専門出版社
2026/3	Space Bears	介護・カラオケ・飲食事業
2026/3	(Unknown)	光半導体デバイスメーカー(海外拠点)
2026/3	WORLD LEAKS	広告・制作
2026/3	The Gentlemen	繊維加工・食品加工メーカー
2026/3	(Unknown)	設備工事
2026/3	(Unknown)	美容室向け化粧品メーカー
2026/3	ALP-001	国立研究開発法人
2026/4	AKIRA	流体システム製品メーカー
2026/4	(Unknown)	非鉄金属・資源開発(海外拠点)
2026/4	(Unknown)	システムインテグレーター
2026/4	KRYBIT	酒類製造業
2026/4	LockBit	水処理・環境設備
2026/4	DragonForce	オフィス家具メーカー(海外拠点)
2026/4	(Unknown)	診療予約システム開発
2026/4	Qilin (Agenda)	舗装・土木工事

※ (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。
※ 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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

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／2025年11月～2026年10月）

赤色は中小企業を示す

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ことが分かる。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

被害月	攻撃グループ	業種概要
2026/4	The Gentlemen	電気機器メーカー
2026/4	Qilin (Agenda)	建設資材・福祉用具のレンタル・販売
2026/4	(Unknown)	生活協同組合
2026/4	COINBASE CARTEL	大学研究会
2026/4	Ransom EXX	ソフトウェア開発
2026/4	LockBit	電子部品(コネクタ)製造(海外拠点)
2026/4	(Unknown)	二輪用品専門チェーン
2026/4	The Gentlemen	ソフトウェア開発
2026/4	Qilin (Agenda)	大手自動車部品メーカー(海外拠点)
2026/5	(Unknown)	百貨店業・不動産賃貸業
2026/5	FulcrumSec	移植医療支援
2026/5	KILLSEC	オンライン処方箋サービス
2026/5	(Unknown)	教育サービス・学習教材
2026/5	AiLock	半導体製造装置・精密機器メーカー(海外拠点)
2026/5	The Gentlemen	医薬品卸売業
2026/5	The Gentlemen	商業施設運営サービス
2026/5	SAFEPAY	産業資材商社
2026/5	AKIRA	家電メーカー(海外拠点)
2026/5	Lynx	水処理装置メーカー(海外拠点)
2026/5	Lynx	蓄電池・電源システム(海外拠点)
2026/5	Metaencryptor	空調メーカー
2026/5	The Gentlemen	ジュエリー輸入・企画販売
2026/5	Payload	空調設備施工
2026/5	The Gentlemen	ガラス容器メーカー
2026/5	NightSpire	医薬品・食品関連製造(海外拠点)
2026/5	(Unknown)	国立大学法人
2026/5	SAFEPAY	紙器製造
2026/5	SAFEPAY	建材リペア・再生工事
2026/6	SAFEPAY	楽器メーカー(海外拠点)
2026/6	(Unknown)	サポーター・健康用品製造販売
2026/6	(Unknown)	化粧品・健康食品製造販売、エステ運営
2026/6	STORMOUS	化学系専門商社(海外拠点)
2026/6	(Unknown)	米穀・飼料・食品卸売等
2026/6	(Unknown)	ローカルキャラクターの活動支援
2026/6	SAFEPAY	音楽系書籍販売
2026/6	(Unknown)	シェアモビリティ、駐車場運営
2026/6	Qilin (Agenda)	トラック・バス等の製造販売(海外拠点)
2026/6	CMD ORGANIZATION	ロボットシステムインテグレーター
2026/6	SHADOWBYT3$	大手ゲーム機・ゲームソフトメーカー(海外拠点)
2026/6	AUR0RA	非鉄金属・自動車部品メーカー(海外拠点)
2026/6	SAFEPAY	建設コンサルタント
2026/6	LockBit	自動車部品・合成樹脂製品メーカー(海外拠点)
2026/6	BlackField	自動車部品メーカー(海外拠点)
2026/6	DragonForce	特殊井メーカー
2026/6	Qilin (Agenda)	私立大学
2026/6	The Gentlemen	化粧品・健康食品製造販売
2026/7	(Unknown)	私立中学・高等学校
2026/7	(Unknown)	引越し・配送会社
2026/7	(Unknown)	総合アパレル業
2026/7	(Unknown)	穀物乾燥機メーカー
2026/7	AiLock	大手タクシー会社
2026/7	AiLock	業務用ソフトウェア開発会社
2026/7	COINBASE CARTEL	航空機向け電子機器メーカー(海外拠点)
2026/7	CHAOS (2025)	大手酒類・食品持株会社(海外拠点)
2026/7	The Gentlemen	排水処理設備メーカー
2026/7	The Gentlemen	ソフトウェア開発会社
2026/7	INC Ransom	特装車メーカー
2026/7	INC Ransom	大手酒類・食品持株会社(海外拠点)
2026/7	RansomHouse	大手冷凍食品メーカー
2026/7	Morpheus	めっき・樹脂成形メーカー(海外拠点)
2026/7	GLOBAL SECRET GROUP	オンラインゲーム会社
2026/7	Everest	ITサービス会社
2026/8	SAFEPAY	不動産コンサルティング・資産管理
2026/8	OROVA	複合機・OA機器・オフィス家具販売・保守
2026/8	(Unknown)	システムインテグレーター
2026/8	AiLock	温室・農業資材メーカー
2026/8	AiLock	食品スーパーマーケット
2026/8	COINBASE CARTEL	精密機器メーカー
2026/8	The Gentlemen	総合建設業
2026/8	MEDUZALOCKER	産業廃棄物収集運搬・処分業者
2026/8	(Unknown)	システムインテグレーター
2026/8	SETTRA	賃貸管理・サブリース
2026/8	The Gentlemen	産業用機械・生産設備メーカー
2026/8	(Unknown)	総合建築事業・総合人材サービス業
2026/8	KRYBIT	建設資材メーカー(海外拠点)
2026/8	(Unknown)	印刷用インキ・合成樹脂メーカー
2026/9	RansomHouse	リユース・エンタメ小売(WonderGOO等)の持株…
2026/9	(Unknown)	システムインテグレーター
2026/9	(Unknown)	地方自治体
2026/9	Qilin (Agenda)	樹脂専門商社
2026/9	AUDIT	不明
2026/9	Metaencryptor	鉄鋼メーカー
2026/9	The Gentlemen	アパレル副資材・RFIDタグメーカー
2026/9	(Unknown)	時計修理
2026/9	SAFEPAY	ソフトウェア開発
2026/9	VEXY	事務機器・OA機器販売
2026/9	Qilin (Agenda)	放送機器メーカー
2026/9	Metaencryptor	自動車部品メーカー
2026/9	Everest	ソフトウェア開発
2026/9	Qilin (Agenda)	配電盤・制御盤・監視システムメーカー
2026/9	Qilin (Agenda)	倉庫・物流業
2026/10	ECLIPSE	英字新聞社
2026/10	(Unknown)	公立大学
2026/10	Qilin (Agenda)	生コンクリート製造販売
2026/10	(Unknown)	クラウドサービス・データセンター事業者
2026/10	EXITIM	切断機・溶接機材・産業用ガスメーカー
2026/10	N0N	外航旅客・貨物船運航
2026/10	N0N	外航海運
2026/10	N0N	国際総合物流(海外拠点)
2026/10	ECLIPSE	医薬品・食品関連製造(海外拠点)
2026/10	Qilin (Agenda)	鉄道事業者
2026/10	The Gentlemen	国立大学法人
2026/10	Everest	麺類製造販売・商社
2026/10	Everest	伸縮継手・ダンパメーカー
2026/10	VEXY	政策情報プラットフォーム開発・提供
2026/10	Qilin (Agenda)	不動産投資・アセットマネジメント
2026/10	BLACKX	医療情報提供サービス
2026/10	SAFEPAY	私立大学
2026/10	Qilin (Agenda)	高機能材料メーカー

※（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。
※ 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
© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

2026

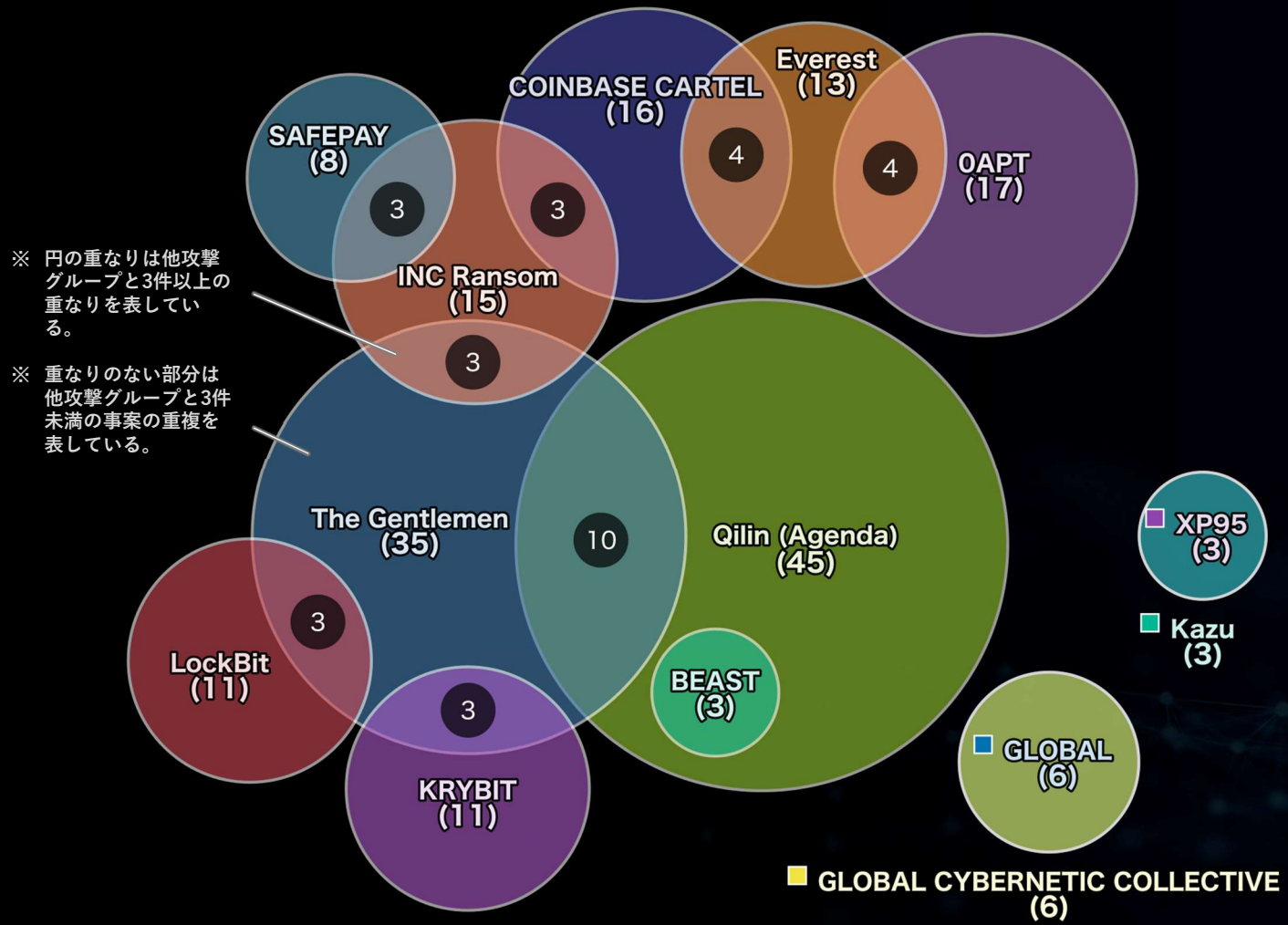
10

多重被害に関する分析

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

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）

（過去1年間／2025年11月～2026年10月）（累計189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。

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

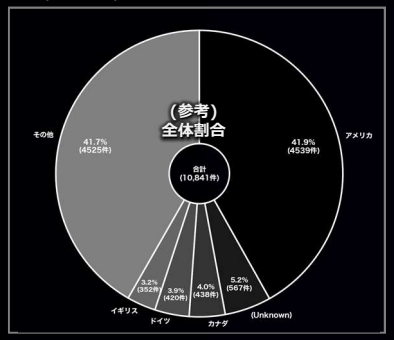
© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

多重被害に遭った被害組織の傾向と分析（全世界）

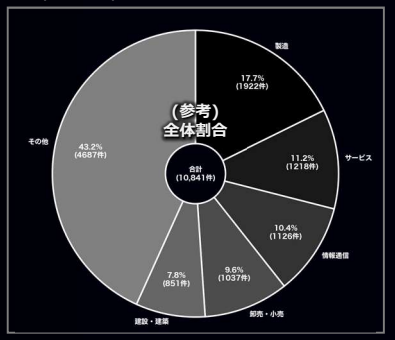
（過去1年間／2025年11月～2026年10月）

※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

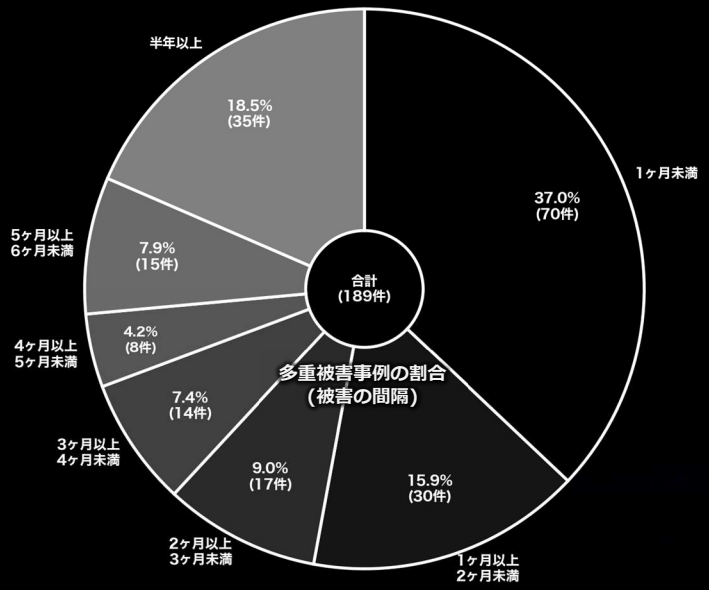


(参考比較) 同期間の全データにおける割合

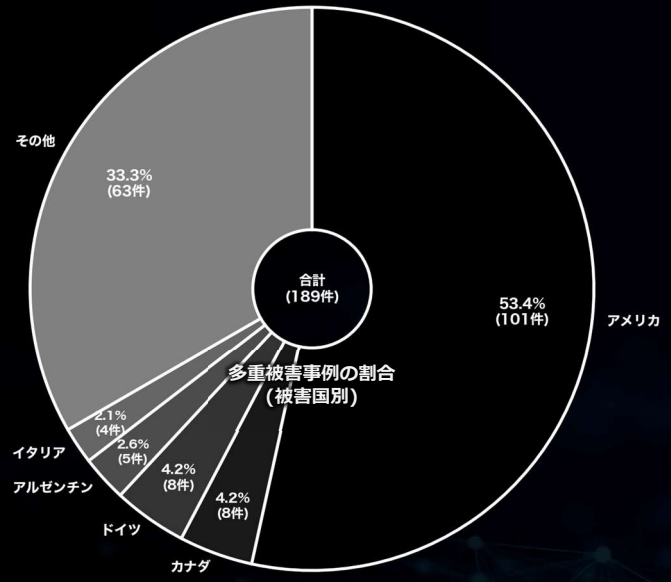


▼被害の間隔

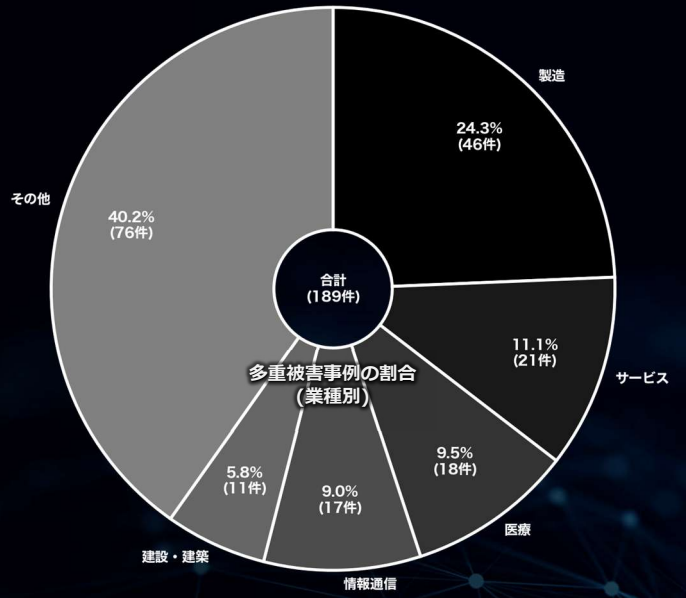
（一度目の被害から二度目の被害までの間隔）



▼被害国別



▼業種別



▶多重被害に遭った組織数の累計：189件（全体10841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全体割合とおおむね同様の傾向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、実に半数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。

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

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）

2026

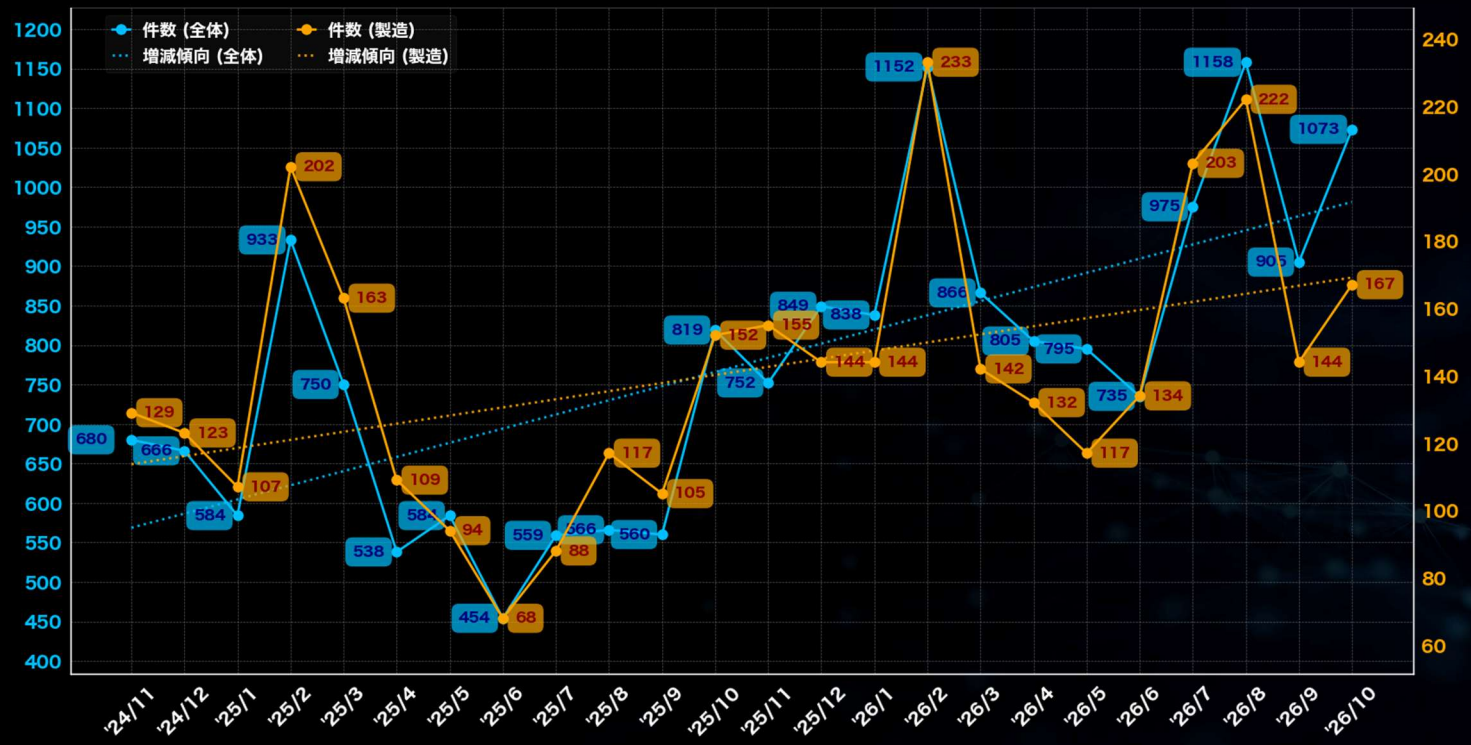
10

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

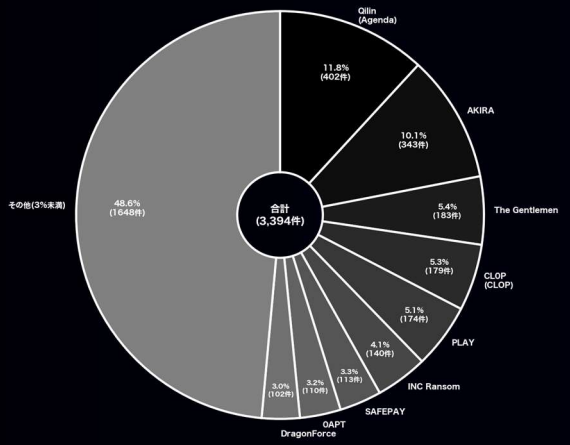
業種に関する分析（全世界）
（過去2年間／2024年11月～2026年10月）

製造

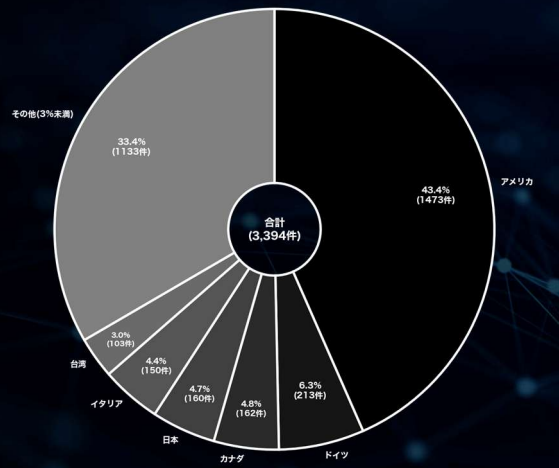
「製造」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年2月で、233件の掲載があった。一方、最も少なかった月は2025年6月で、68件であった。被害組織の所在国の割合では、アメリカが約43%と最も多く、次いでドイツとカナダがそれぞれ約6%と約5%である。攻撃グループについては、少なくとも180のグループが関与しており、特に「Qilin (Agenda)」が402件のリークサイト掲載を実施している。次いで「AKIRA」と「The Gentlemen」がそれぞれ343件と183件の掲載を行っている。製造関連の件数は全体件数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、長期にわた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）

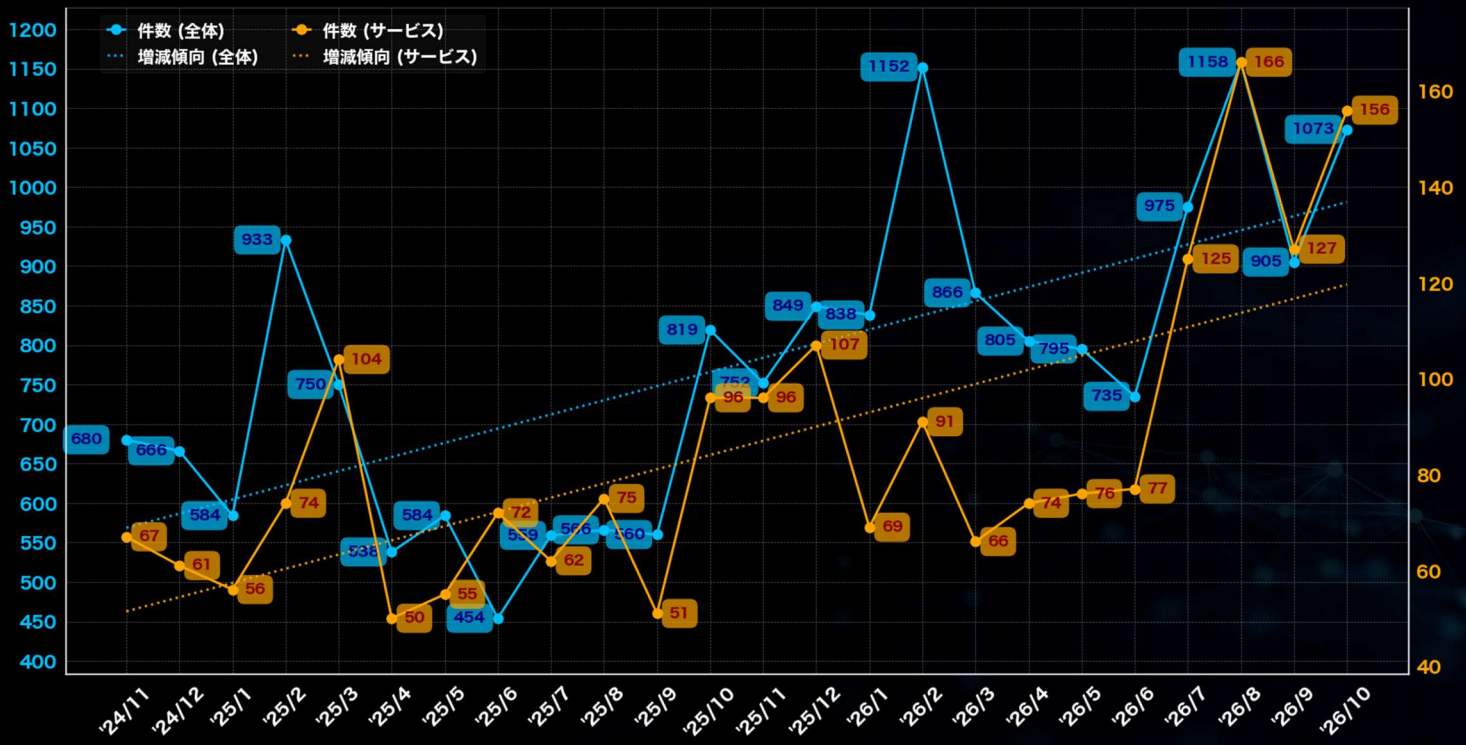
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

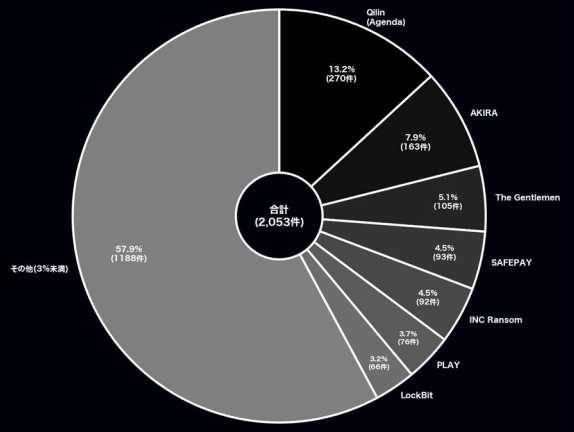
業種に関する分析（全世界）
（過去2年間／2024年11月～2026年10月）

サービス

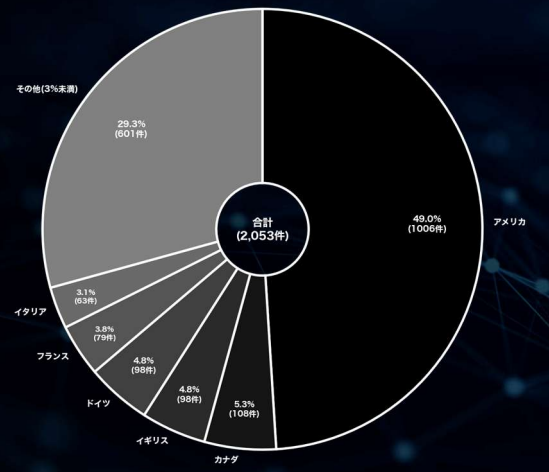
「サービス」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年8月で、166件の掲載があった。一方、最も少なかった月は2025年4月で、50件であった。被害組織の所在国の割合では、アメリカが約49%と最も多く、次いでカナダとイギリスがそれぞれ約5%である。攻撃グループについては、少なくとも166のグループが関与しており、特に「Qilin (Agenda)」が270件のリークサイト掲載を実施している。次いで「AKIRA」と「The Gentlemen」がそれぞれ163件と105件の掲載を行っている。サービス関連の件数は製造関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）

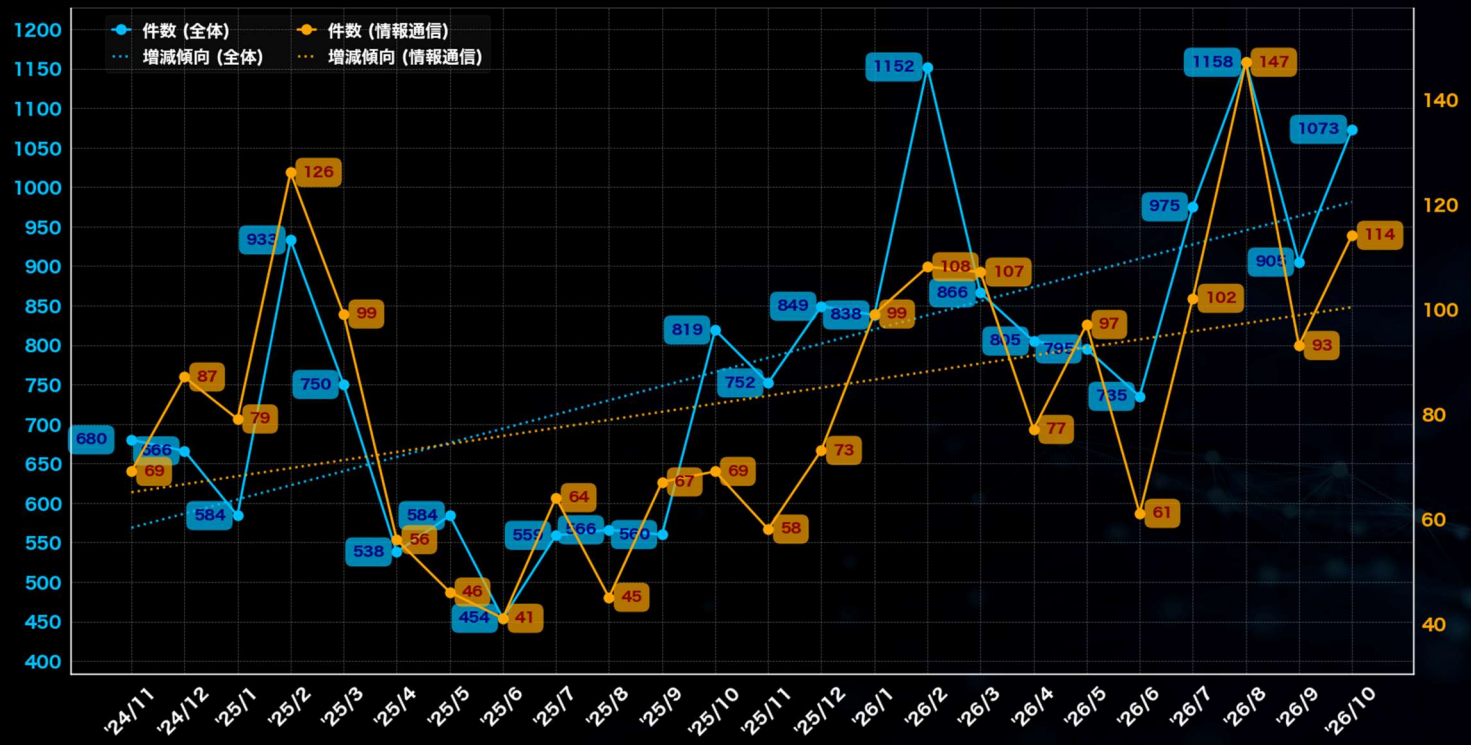
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

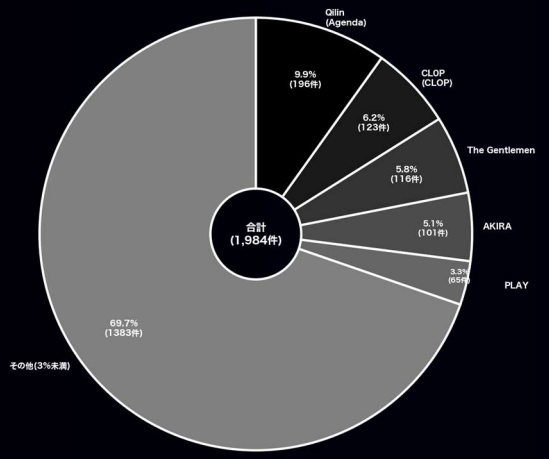
業種に関する分析（全世界）
（過去2年間／2024年11月～2026年10月）

情報通信

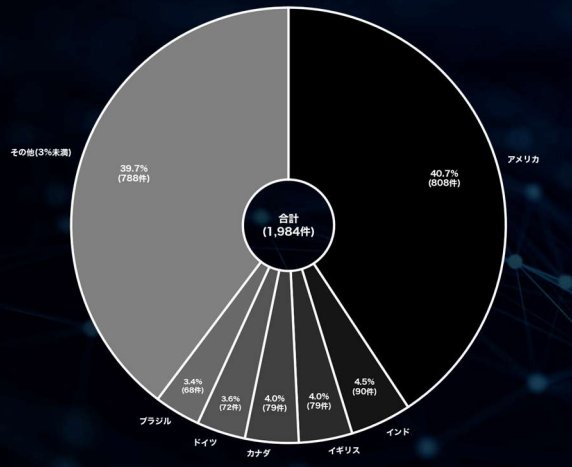
「情報通信」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年8月で、147件の掲載があった。一方、最も少なかった月は2025年6月で、41件であった。被害組織の所在国の割合では、アメリカが約41%と最も多く、次いでインドとイギリスがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも179のグループが関与しており、特に「Qilin (Agenda)」が196件のリークサイト掲載を実施している。次いで「CL0P (CLOP)」と「The Gentlemen」がそれぞれ123件と116件の掲載を行っている。情報通信業界は技術情報や顧客データを多く保有することから、引き続きランサムウェア攻撃の主要な標的となっており、関与グループ数も製造業と並ぶ規模となっている。



▼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）

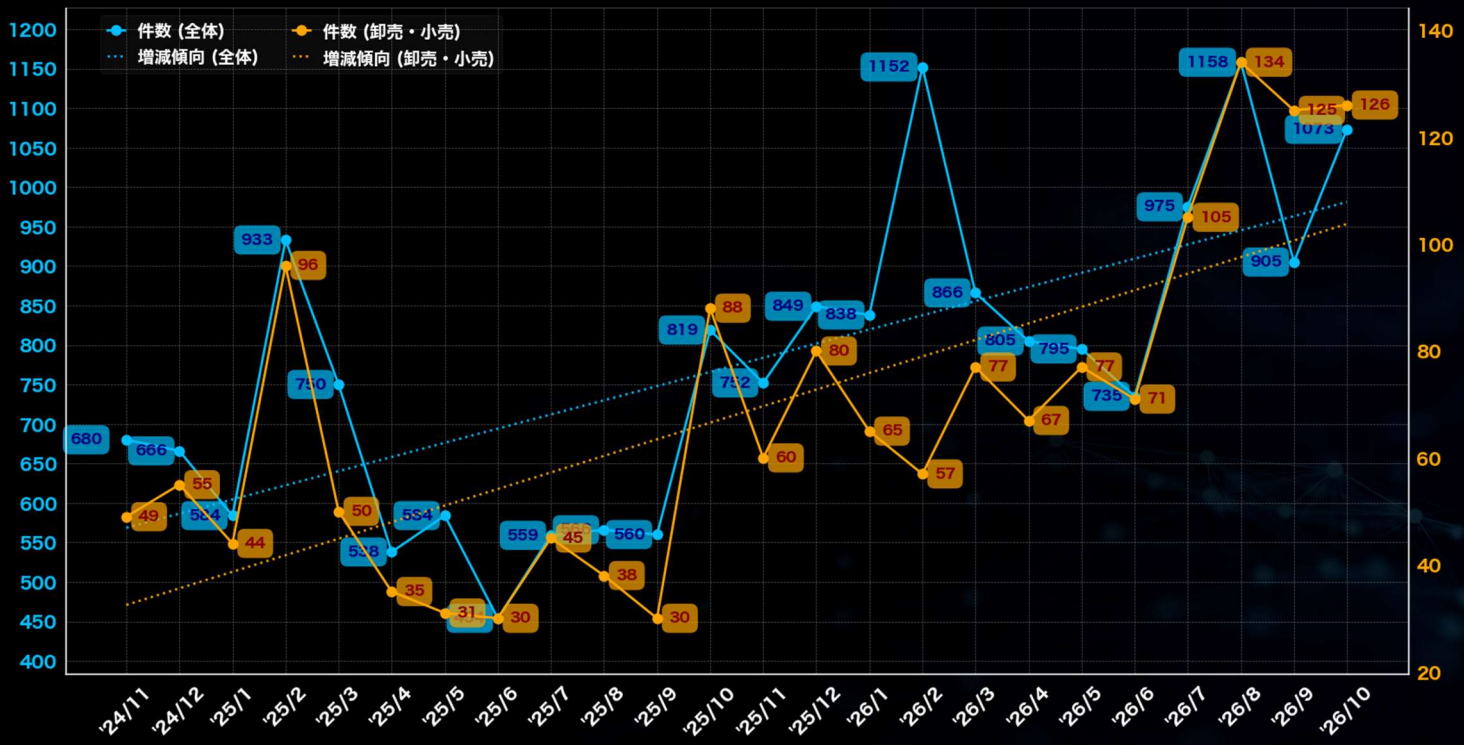
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

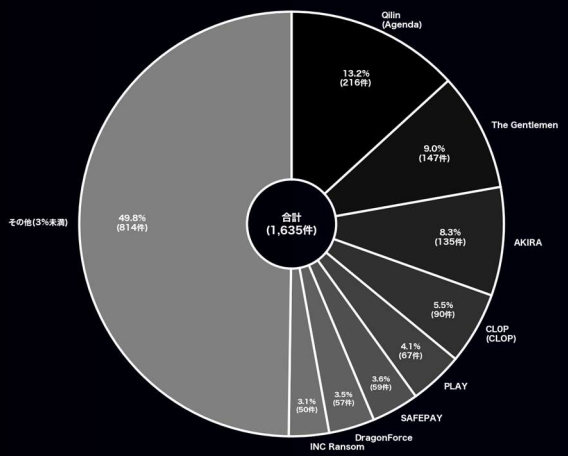
業種に関する分析（全世界）
（過去2年間／2024年11月～2026年10月）

卸売・小売

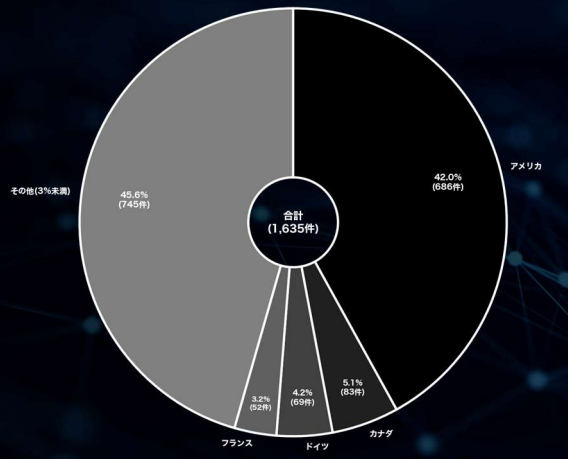
「卸売・小売」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年8月で、134件の掲載があった。一方、最も少なかった月は2025年6月と2025年9月で、いずれも30件であった。被害組織の所在国の割合では、アメリカが約42%と最も多く、次いでカナダとドイツがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも148のグループが関与しており、特に「Qilin (Agenda)」が216件のリークサイト掲載を実施している。次いで「The Gentlemen」と「AKIRA」がそれぞれ147件と135件の掲載を行っている。卸売・小売業界は最大月と最小月の差が大きく月次変動の激しい業種でありながら、全体としては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）

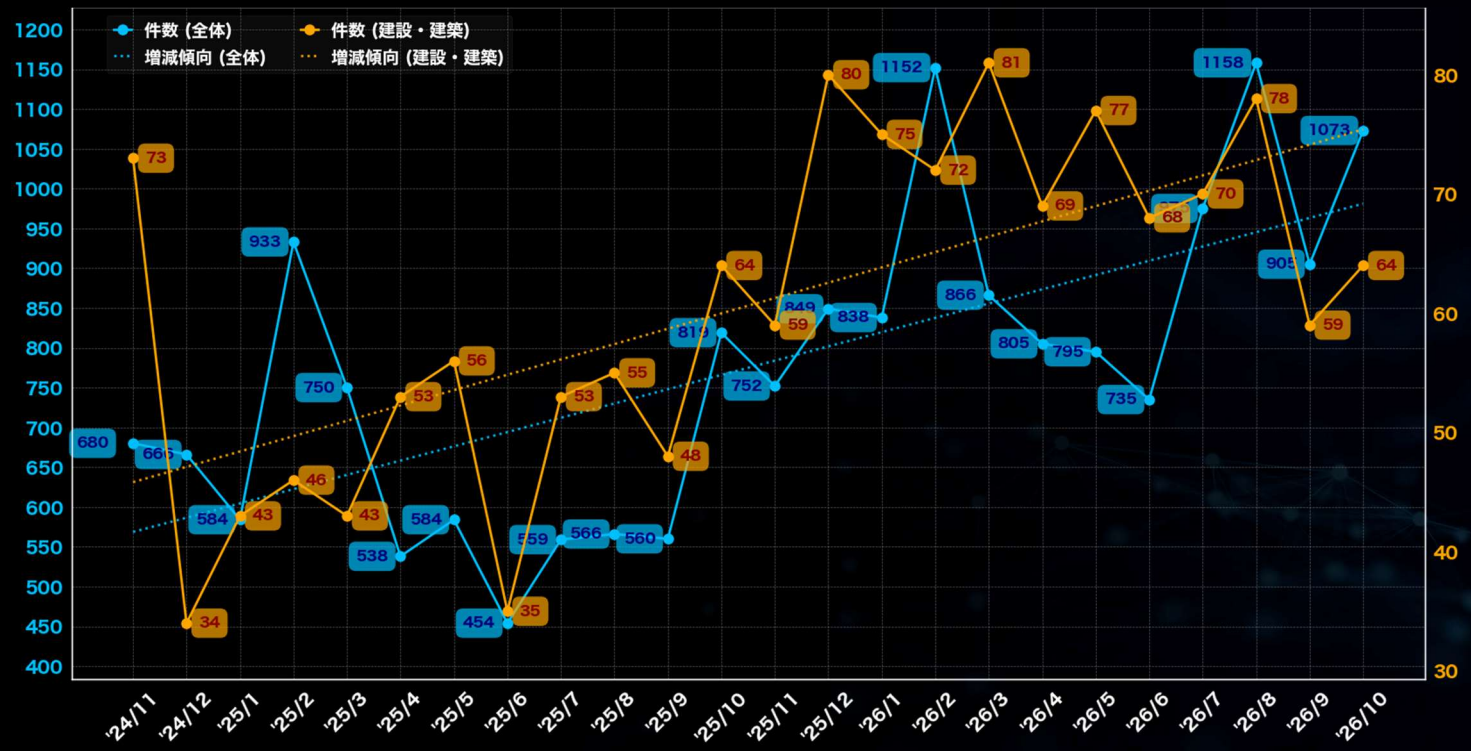
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

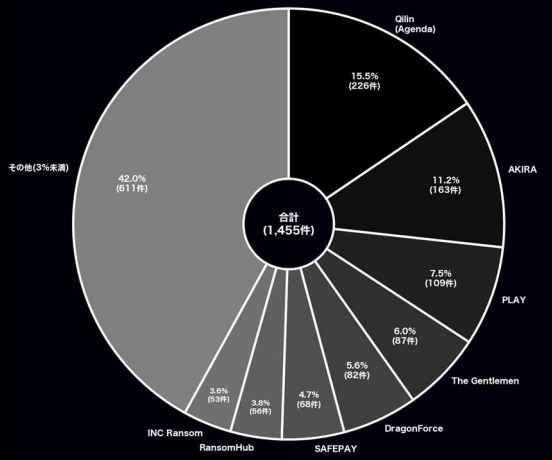
業種に関する分析（全世界）
（過去2年間／2024年11月～2026年10月）

建設・建築

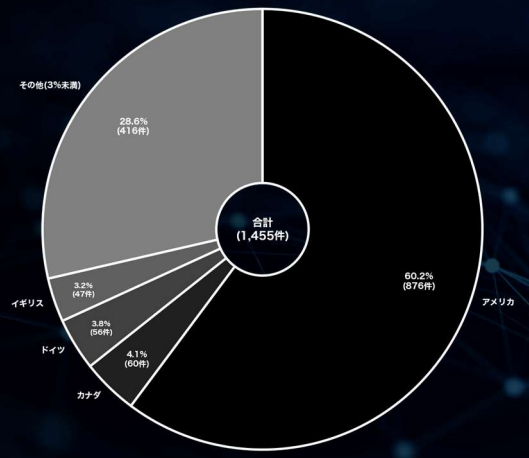
「建設・建築」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年3月で、81件の掲載があった。一方、最も少なかった月は2024年12月で、34件であった。被害組織の所在国の割合では、アメリカが約60%と最も多く、次いでカナダとドイツがそれぞれ約4%である。攻撃グループについては、少なくとも131のグループが関与しており、特に「Qilin (Agenda)」が226件のリークサイト掲載を実施している。次いで「AKIRA」と「PLAY」がそれぞれ163件と109件の掲載を行っている。建設・建築業界はアメリカに被害が集中しており、攻撃対象としての偏りが顕著に表れている。



▼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）

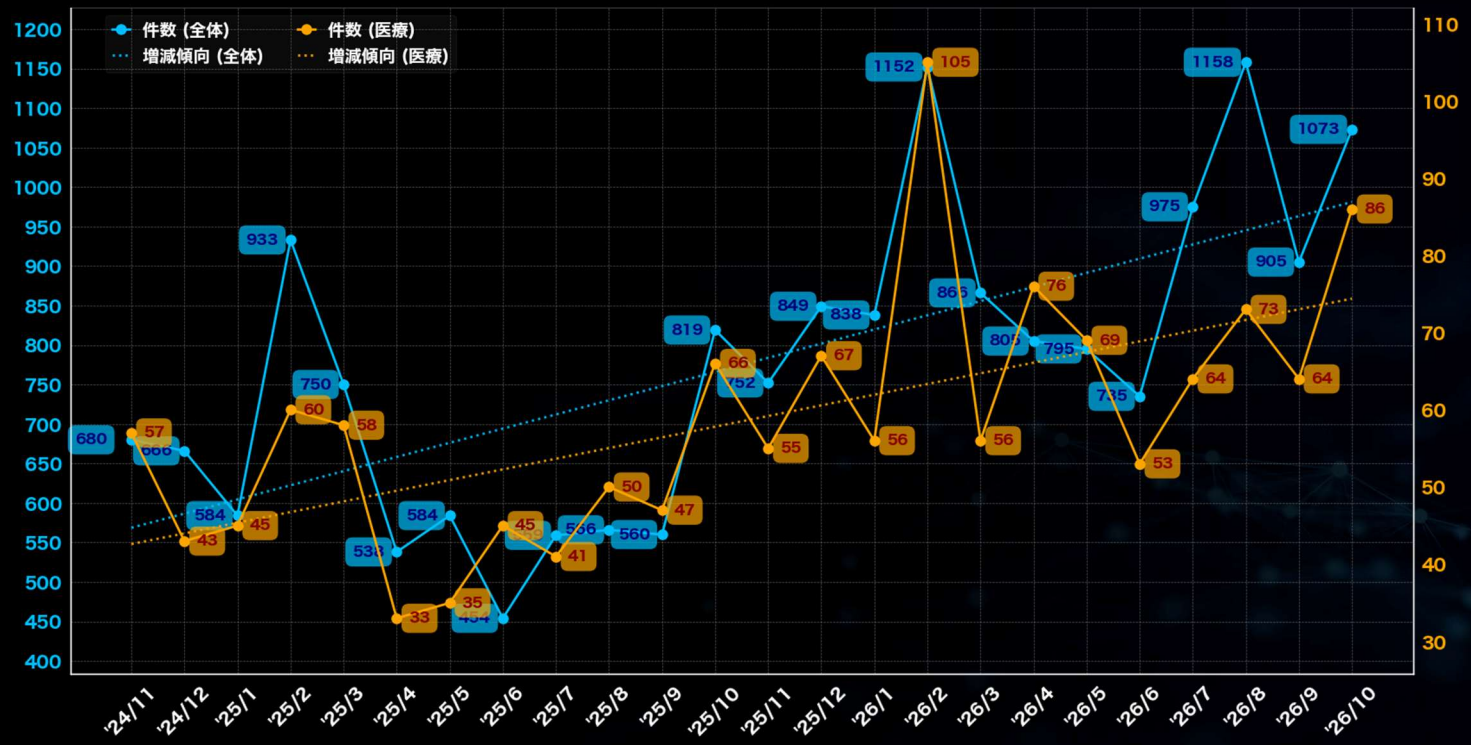
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

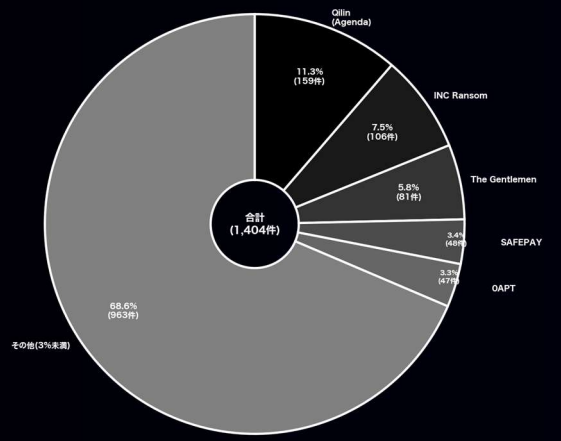
業種に関する分析（全世界）
（過去2年間／2024年11月～2026年10月）

医療

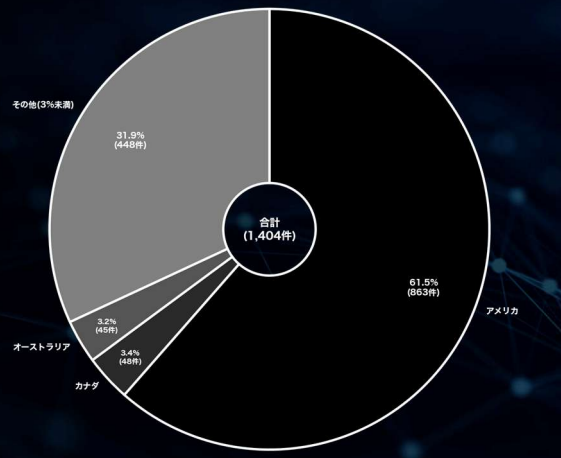
「医療」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年2月で、105件の掲載があった。一方、最も少なかった月は2025年4月で、33件であった。被害組織の所在国の割合では、アメリカが約62%と最も多く、次いでカナダとオーストラリアがそれぞれ約3%である。攻撃グループについては、少なくとも145のグループが関与しており、特に「Qilin (Agenda)」が159件のリークサイト掲載を実施している。次いで「INC Ransom」と「The Gentlemen」がそれぞれ106件と81件の掲載を行っている。医療業界は患者情報など機微なデータを保有することから、依然として攻撃者の標的となっている。



▼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）

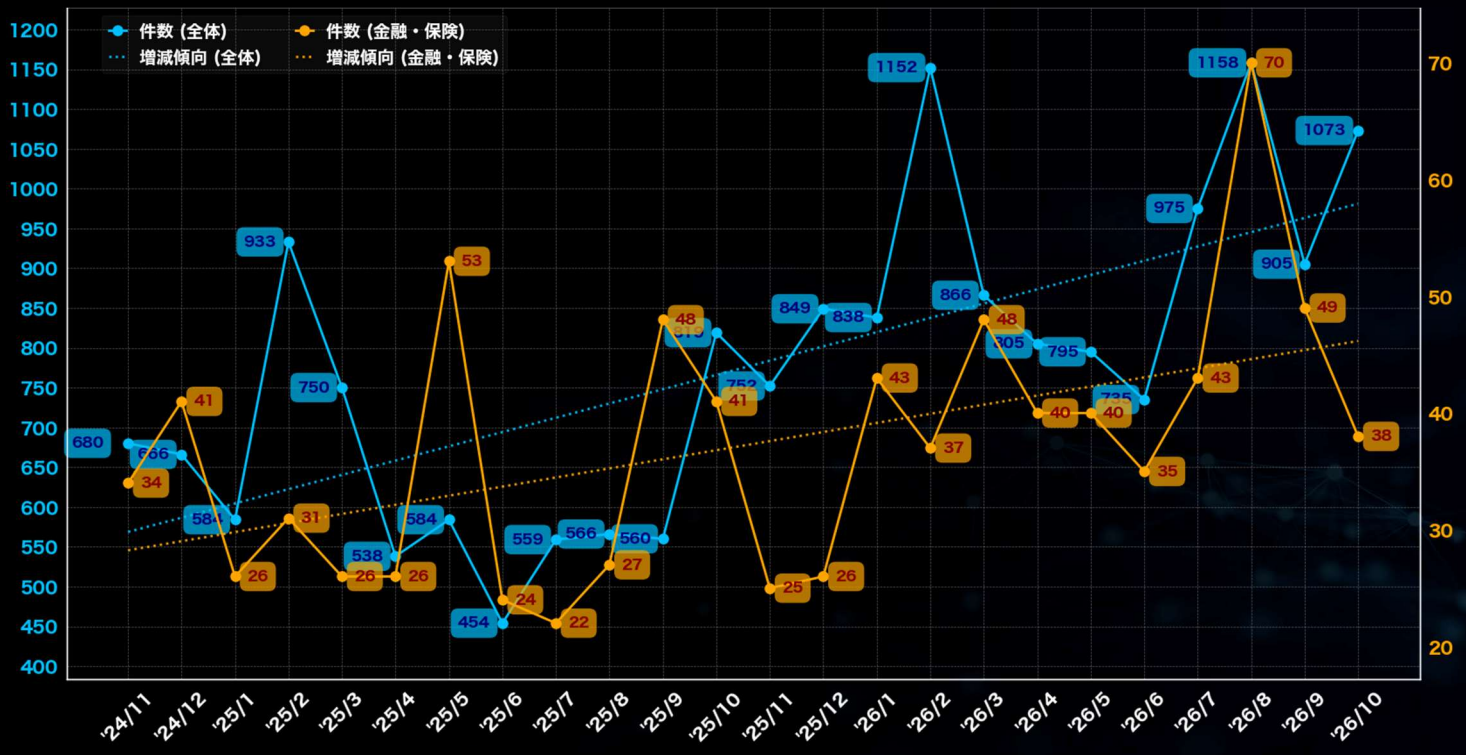
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

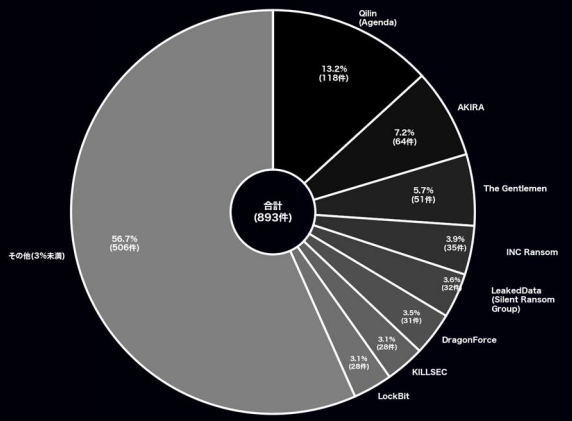
業種に関する分析（全世界）
（過去2年間／2024年11月～2026年10月）

金融・保険

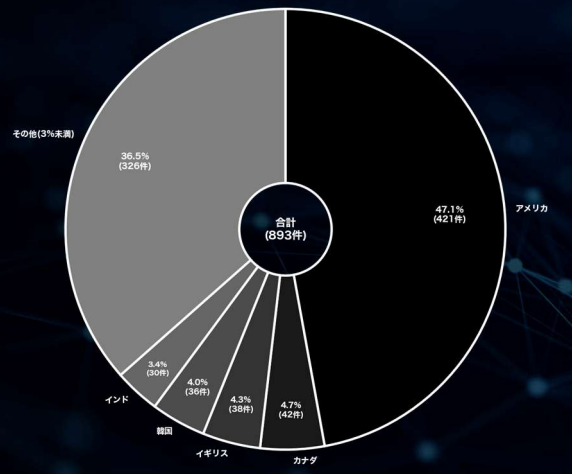
「金融・保険」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年8月で、70件の掲載があった。一方、最も少なかった月は2025年7月で、22件であった。被害組織の所在国の割合では、アメリカが約47%と最も多く、次いでカナダとイギリスがそれぞれ約5%と約4%である。攻撃グループについては、少なくとも139のグループが関与しており、特に「Qilin (Agenda)」が118件のリークサイト掲載を実施している。次いで「AKIRA」と「The Gentlemen」がそれぞれ64件と51件の掲載を行っている。金融・保険業界は被害件数こそ他業界に比べ少ないものの、関与する攻撃グループは139と多岐にわたっており、引き続き警戒が必要である。



▼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）

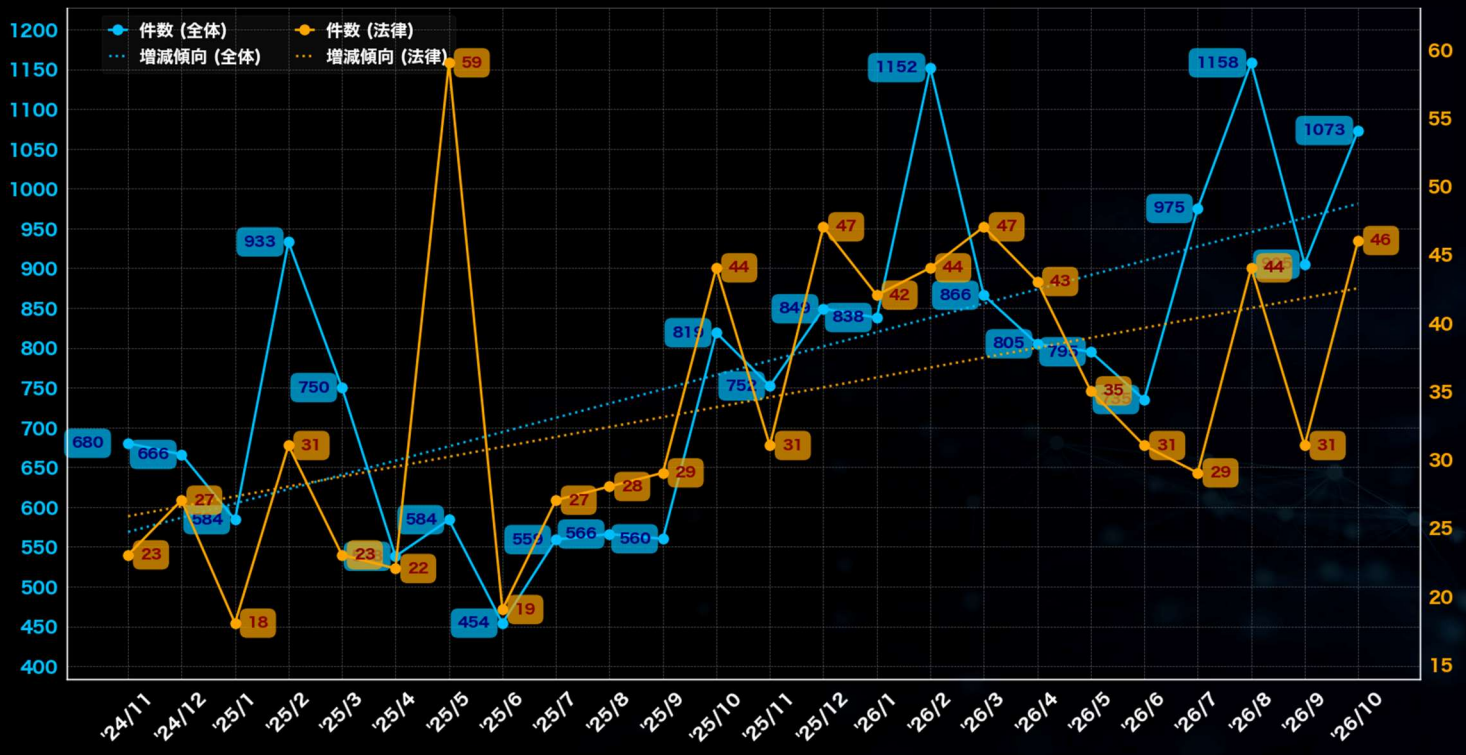
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

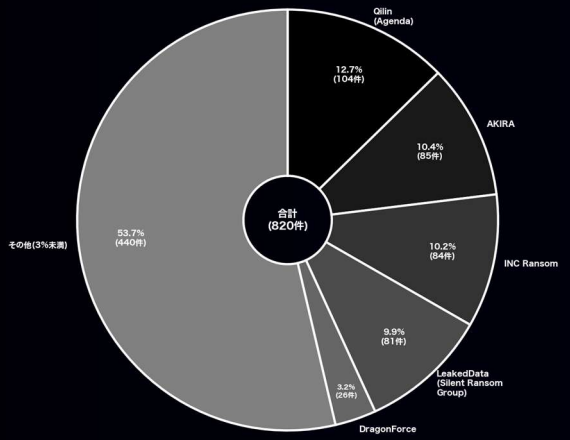
業種に関する分析（全世界）
（過去2年間／2024年11月～2026年10月）

法律

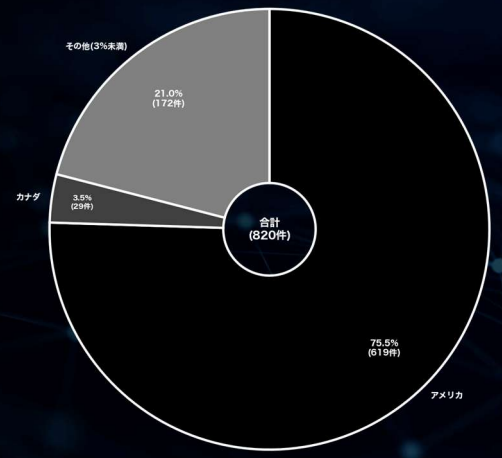
「法律」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年5月で、59件の掲載があった。一方、最も少なかった月は2025年1月で、18件であった。被害組織の所在国の割合では、アメリカが約76%と最も多く、次いでカナダとイギリスがそれぞれ約4%と約3%である。攻撃グループについては、少なくとも102のグループが関与しており、特に「Qilin (Agenda)」が104件のリークサイト掲載を実施している。次いで「AKIRA」と「INC Ransom」がそれぞれ85件と84件の掲載を行っている。法律業界はアメリカの被害が極端に集中している点も特徴である。



▼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）

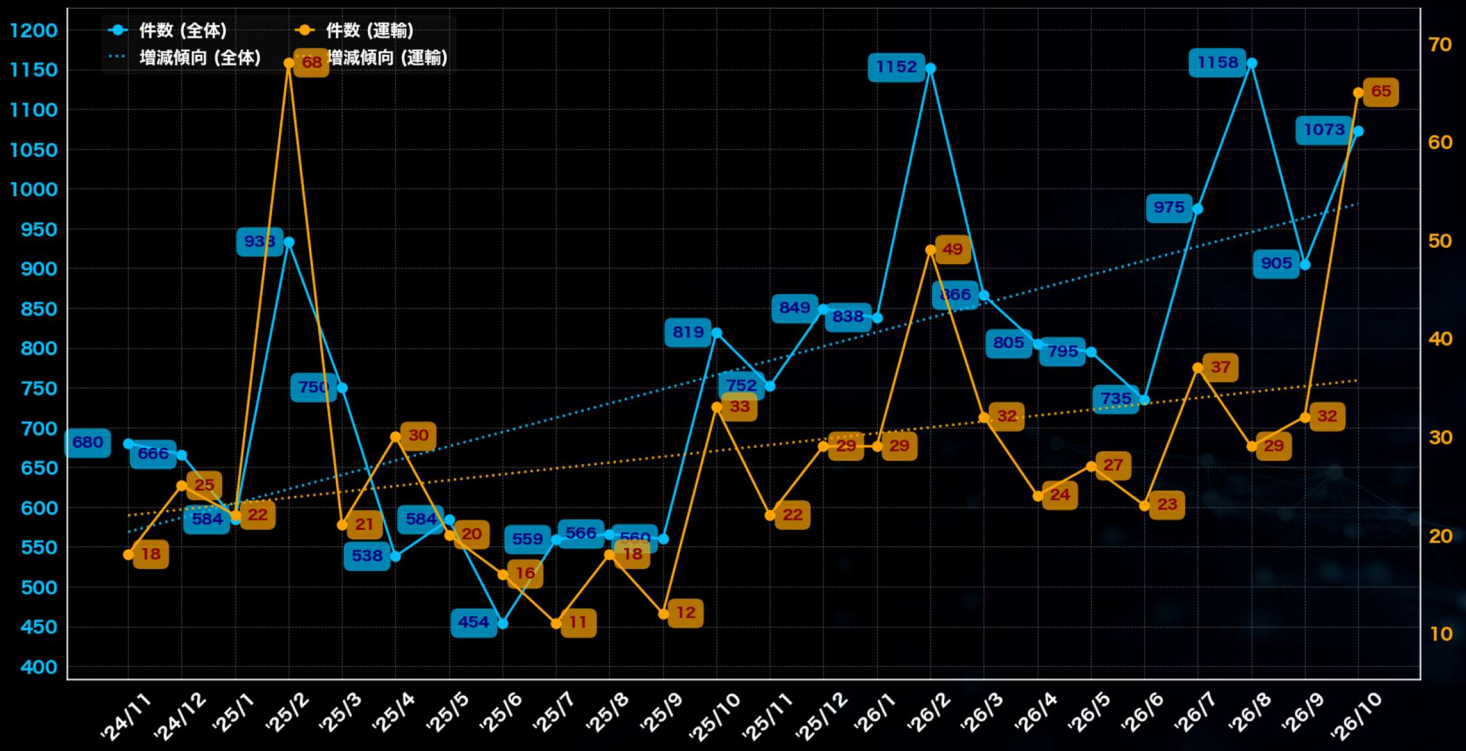
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

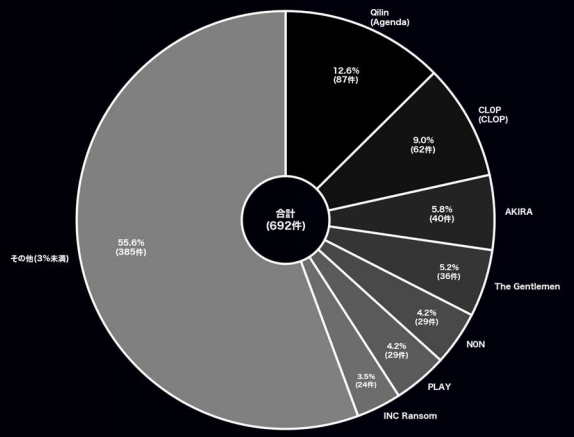
業種に関する分析（全世界）
（過去2年間／2024年11月～2026年10月）

運輸

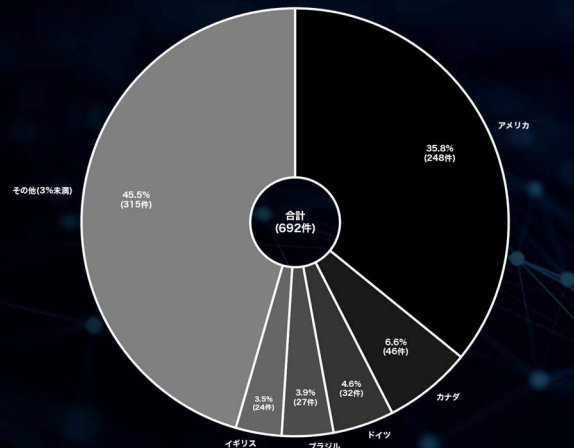
「運輸」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2025年2月で、68件の掲載があった。一方、最も少なかった月は2025年7月で、11件であった。被害組織の所在国の割合では、アメリカが約36%と最も多く、次いでカナダとドイツがそれぞれ約7%と約5%である。攻撃グループについては、少なくとも122のグループが関与しており、特に「Qilin (Agenda)」が87件のリークサイト掲載を実施している。次いで「CL0P (CLOP)」と「AKIRA」がそれぞれ62件と40件の掲載を行っている。運輸関係は全体件数に対する割合こそ低いものの、サプライチェーンへの影響を考慮すると引き続き注視が必要である。



▼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）

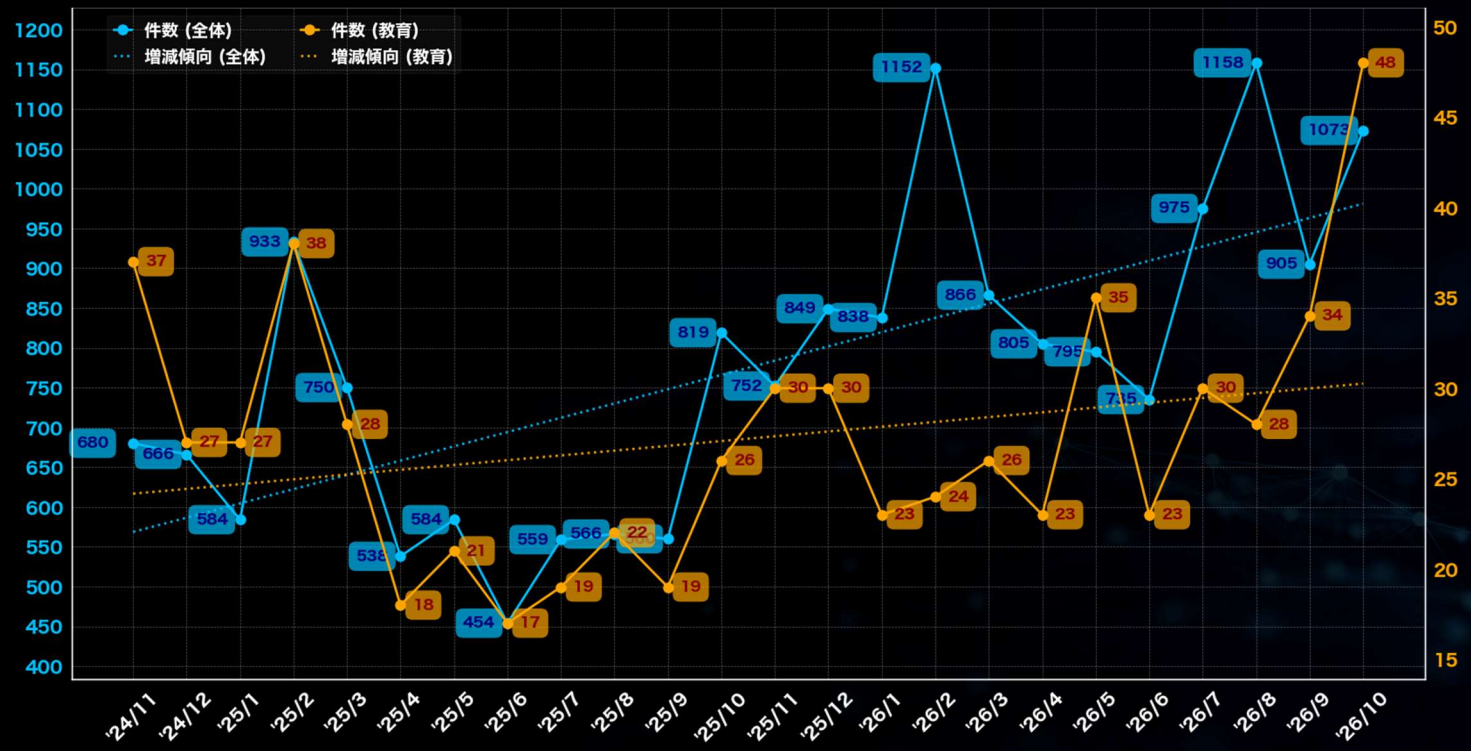
※ 各集計や分析に関する留意事項は末尾の「本資料に関する留意事項及び二次利用について」の項を参照

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

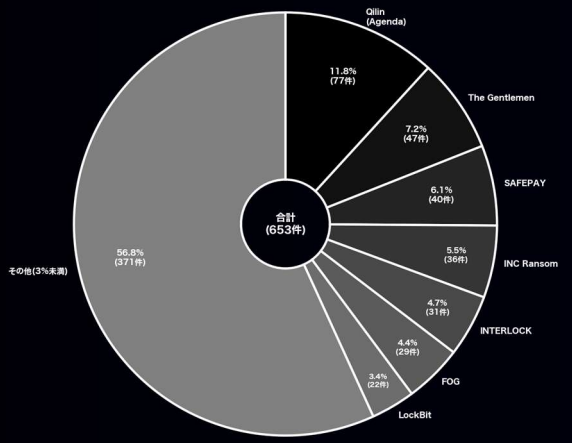
業種に関する分析（全世界）
（過去2年間／2024年11月～2026年10月）

教育

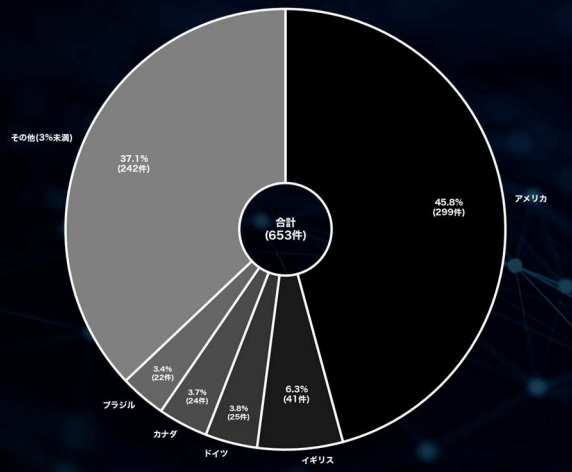
「教育」業界に対するランサムウェア攻撃のリークサイト掲載件数は、過去2年間で様々な変動が確認されている。最も多かった月は2026年10月で、48件の掲載があった。一方、最も少なかった月は2025年6月で、17件であった。被害組織の所在国の割合では、アメリカが約46%と最も多く、次いでイギリスとドイツがそれぞれ約6%と約4%である。攻撃グループについては、少なくとも114のグループが関与しており、特に「Qilin (Agenda)」が77件のリークサイト掲載を実施している。次いで「The Gentlemen」と「SAFEPAY」がそれぞれ47件と40件の掲載を行っている。教育業界は他業界に比べ被害件数は限定的であるものの、関与する攻撃グループは114と多く、依然として注意が必要である。



▼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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

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。

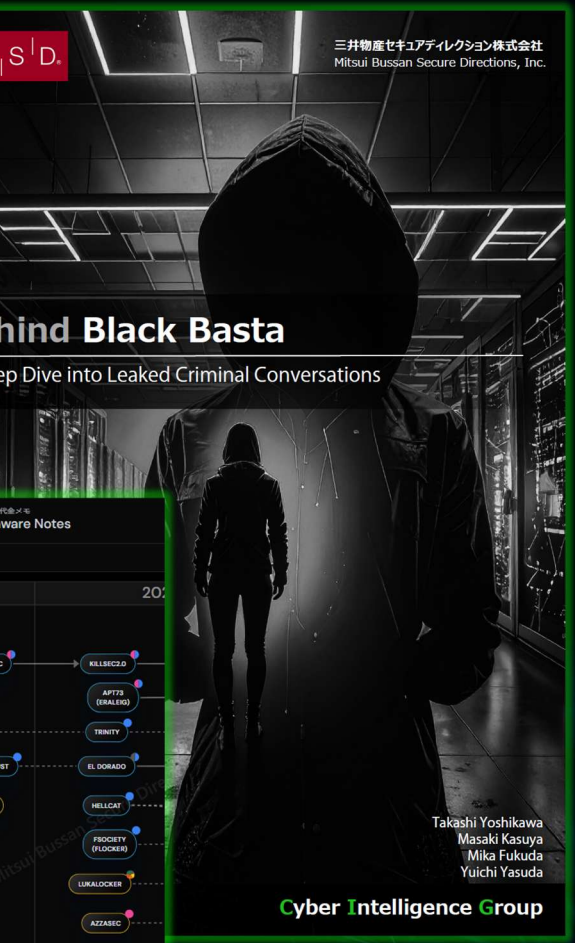
● CIG Ransomware Information Portal (WEBアプリケーション)：
https://www.mbsd.jp/cig-ransomware-portal/

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

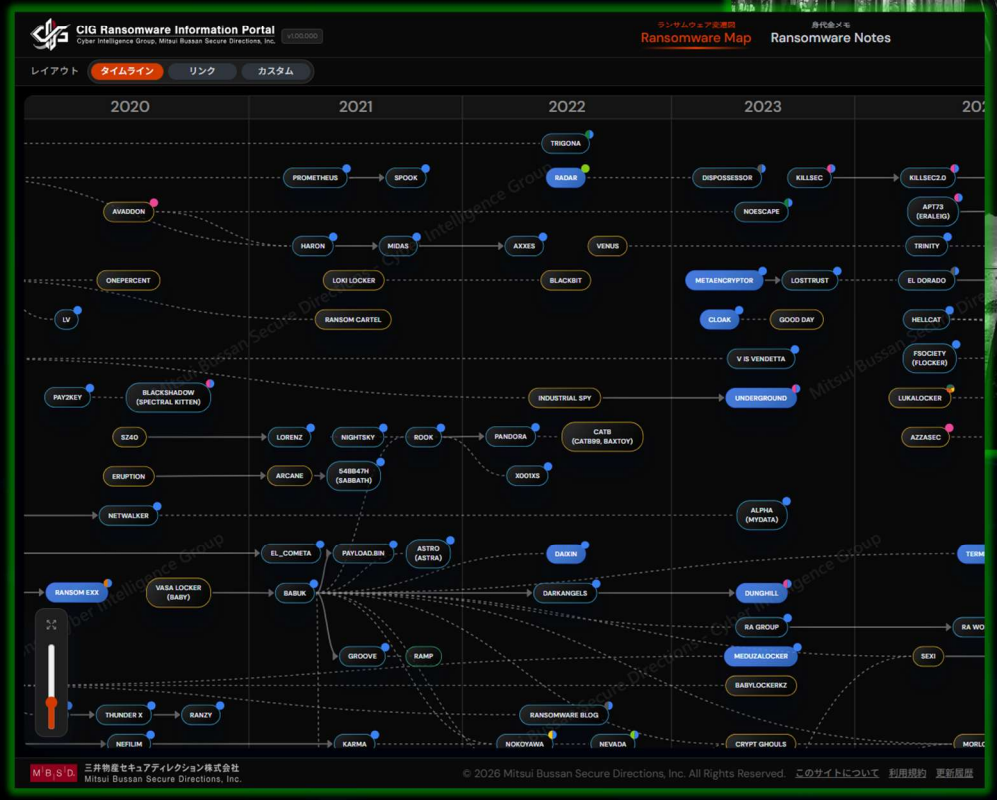
● 技術ブログ：
https://www.mbsd.jp/research/cig/
https://www.mbsd.jp/research/t.yoshikawa/
https://www.mbsd.jp/research/m.kasuya/
https://www.mbsd.jp/research/s.urata/

● 分析レポート：
https://www.mbsd.jp/report

Black Basta 内部チャット分析レポート



CIG Ransomware Information Portal



※ 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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.

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

本レポートはご自由に二次利用いただけます。様々な用途にぜひご活用ください。
ご利用・転載・引用の際には、出典として「MBSD Cyber Intelligence Group (CIG)」と明記くださいますようお願いいたします。
(※本レポートそのものの販売など直接的な営利目的でのご利用はご遠慮ください。有料セミナーや出版物、メディア記事など、利用者側の収益が発生する活動においても、参考情報として一部を引用・掲載いただくことに問題はありません。その際は大変お手数ですが、状況把握のため、ご利用前に下記連絡先まで簡単にご一報いただけますと幸いです)

お問い合わせ窓口：https://www.mbsd.jp/contact-list/

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.



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

© 2026 Mitsui Bussan Secure Directions, Inc. All Rights Reserved.