

脅威アクター動向ダイジェスト（2026-09-24）

対象：直近 7 日間に収集した情報（09/17 14:31～09/24 14:31 JST）

注：アクターへの帰属（アトリビューション）はベンダー・当局の見解であり確定事実ではありません。リークサイト掲載は犯行グループ側の主張であり、被害の事実確認は別途必要です。

1. 日本関連

リークサイト新規掲載（日本）：11 件

グループ	掲載組織	業種	攻撃日(主張)	検知日
auditteam	ki***jp	Not Found	2026-09-09	2026-09-10
auditteam	kit-e.jp	Technology	2026-09-09	2026-09-18
vexy ransomware	Hashimoto Jimuki	Manufacturing	2026-09-15	2026-09-15
metaencryptor	Astemo, Ltd.	Manufacturing	2026-09-21	2026-09-21
metaencryptor	Nippon Steel Corporation	Manufacturing	2026-09-15	2026-09-15
Qilin	IKEGAMI TSUSHINKI COMPANY LIMITED	Manufacturing	2026-09-21	2026-09-21
Qilin	Mitsuwa Trading Co., Ltd	Retail & E- Commerce	2026-09-09	2026-09-09
RansomHouse	REXT Holdings Co., Ltd.	Other	2026-09-01	2026-09-01
SafePay	ryomo.co.jp	Not Found	2026-09-15	2026-09-15
The Gentlemen	Tentac	Technology	2026-09-14	2026-09-15
The Gentlemen	Wada Farms	Agriculture and Food Production	2026-09-14	2026-09-15

日本関連記事：19 件

- 美容医療プラットフォーム「Unni（カンナムオンニ）」への不正アクセスについてまとめた
piyolog・2026-09-24
- 旭化成の元従業員による営業秘密の持ち出しについてまとめた
piyolog・2026-09-24

- [21st September – Threat Intelligence Report](#)
Check Point Research • 2026-09-22
- [理工学部教職員がフィッシング被害、不審メールが送信 - 日大](#)
Security NEXT • 2026-09-18
- [TSUBAME Report Overflow \(Apr-Jun 2026\)](#)
JPCERT/CC Eyes (英) • 2026-09-18
- [xxx.soumu.go.jp などのサブドメインも拒否に ～ 総務省を装うフィッシングメール対策強化](#)
ScanNetSecurity • 2026-09-18
- [Mitsubishi Electric GX Works3 and Motion Control Settings](#)
CISA Advisories • 2026-09-17
- [Ransomware incidents in Japan in the first half of 2026: Investigation of The Gentlemen’s infrastructure and evidence of Qilin’s AI use](#)
Cisco Talos • 2026-09-17 ／ 関連：Qilin, The Gentlemen
- [NTT ドコモによる Amazon への顧客情報の無断提供についてまとめた](#)
piyolog • 2026-09-17
- [Weekly Report: 警察庁が「令和 8 年上半期におけるサイバー空間をめぐる脅威の情勢等について」を公開](#)
JPCERT/CC 注意喚起等 • 2026-09-16
- [Weekly Report: 独立行政法人情報処理推進機構（IPA）が「ランサムウェア被害から学ぶ教訓集 経営者のためのランサムウェア対策ハンドブック」を公開](#)
JPCERT/CC 注意喚起等 • 2026-09-16
- [4 件目も見つかった Anthropic の評価中 AI モデルによる不正アクセス事案についてまとめた](#)
piyolog • 2026-09-15
- [沖縄県知事選挙をめぐる偽情報や誹謗中傷の拡散についてまとめた](#)
piyolog • 2026-09-15
- [日本大学理工学部教職員のアカウントに対し巧妙に偽装されたフィッシングメール、多数の不審メールを送信](#)
ScanNetSecurity • 2026-09-15
- [MAMAMOO JAPAN OFFICIAL FANCLUB「MOOMOO JAPAN」に不正アクセス](#)
ScanNetSecurity • 2026-09-15
- [日本企業はセキュリティの「意思決定」を外部委託 ～ MM 総研調査](#)
ScanNetSecurity • 2026-09-15
- [デジタル庁のガバメントソリューションサービス\(GSS\)への不正アクセスについてまとめた](#)
piyolog • 2026-09-11
- [Project Glasswing と日本国内の状況についてまとめた](#)
piyolog • 2026-09-08

- [ランサムウェアグループによる Cursor の悪用についてまとめた](#)
piyolog • 2026-09-02

2. ランサムウェア：リークサイト掲載状況

新規掲載 合計 619 件（74 グループ）

グループ	件数	うち日本
The Gentlemen	60	2
Qilin	59	2
Akira	32	0
Krybit	31	0
auditteam	29	2
storm	23	0
settra	22	0
INC Ransom	20	0
SafePay	20	1
direwolf	17	0
emperador	16	0
panzer	15	0
Luna Moth	15	0
vexy ransomware	15	1
metaencryptor	15	2
LockBit	14	0
n0n	13	0
medusalocker	9	0
Play	9	0
Rhysida	9	0

3. ランサムウェア：関連記事

payload

- [Group Policy hijacked: PAYLOAD ransomware weaponizes Active Directory GPO](#)
Securelist • 2026-09-21 / 検出表記：PAYLOAD
- [PuzzleMask: Abusing Plain Prose as a Covert AI Attack Vector](#)
Check Point Research • 2026-09-10 / 検出表記：payload
- [Untracked Nightmares: The Threats Hiding Behind Commodity Infrastructure](#)
Unit 42 • 2026-09-09 / 検出表記：payload

- [ClearFake WebDAV infection chain delivers Amatera stealer, ZigCryptoStealer, and NetSupport Manager](#)
Cisco Talos • 2026-09-08 / 検出表記：payload
- [ValleyRAT masquerading as adware](#)
Securelist • 2026-08-31 / 検出表記：payload

ShinyHunters — G1057

- [FBI investigating alleged ShinyHunters breach of its jobs site](#)
The Record • 2026-09-23 / 検出表記：ShinyHunters
- [ShinyHunters claims FBI hack, data theft in PeopleSoft zero-day breach](#)
BleepingComputer • 2026-09-23 / 検出表記：ShinyHunters
- [実在するセキュリティ担当者を装った電話がかかってくる攻撃についてまとめてみた](#)
piyolog • 2026-08-26 / 検出表記：ShinyHunters

global

- [The New Rules of Machine Speed Defense](#)
Recorded Future • 2026-09-17 / 検出表記：global
- [GTIG AI Threat Tracker: From Prompting to Autonomy – The Evolution of Adversarial AI](#)
Google Threat Intel • 2026-09-08 / 検出表記：global
- [7th September – Threat Intelligence Report](#)
Check Point Research • 2026-09-07 / 検出表記：global

eclipse

- [New Windows Defender zero-day blocks Microsoft antivirus updates](#)
BleepingComputer • 2026-09-22 / 検出表記：Eclipse

underground

- [AI Threat Landscape Digest: July–August 2026](#)
Check Point Research • 2026-09-17 / 検出表記：underground

Qilin (キリン)

- [Ransomware incidents in Japan in the first half of 2026: Investigation of The Gentlemen's infrastructure and evidence of Qilin's AI use](#)
Cisco Talos • 2026-09-17 / 検出表記：Qilin

The Gentlemen

- [Ransomware incidents in Japan in the first half of 2026: Investigation of The Gentlemen's infrastructure and evidence of Qilin's AI use](#)
Cisco Talos • 2026-09-17 / 検出表記：The Gentlemen

entropy

- [Siemens Reyrolle 7SR5](#)
CISA Advisories • 2026-09-15 / 検出表記：Entropy

4. 北朝鮮系：関連記事

TraderTraitor（トレーダートレイター） — 上位: Lazarus Group

- [Don't Call Us, We'll Call Your APIs | TraderTraitor Backdoors Resurface on Victim With No Crypto Ties](#)
SentinelLabs • 2026-09-19 / 検出表記：TraderTraitor

5. 中国系：関連記事

Salt Typhoon — G1045

- [Beware the SparroWock: The backdoor that bites, the commands that catch](#)
ESET WeLiveSecurity • 2026-09-17 / 検出表記：FamousSparrow

Earth Berberoka

- [Gaming the system: how a Chinese-speaking actor turned Brazilian government sites into an SEO weapon](#)
Check Point Research • 2026-09-02 / 検出表記：Earth Berberoka

6. ロシア系：関連記事

APT28 — G0007

- [BlueDelta Targets Defense and Diplomacy with HOOKEDGE](#)
Recorded Future • 2026-08-27 / 検出表記：BlueDelta

7. イラン系：関連記事

(該当なし)

8. イスラエル系：関連記事

(該当なし)

9. 金銭目的犯罪（ランサム関連含む）：関連記事

TeamPCP — G1056

- [GTIG AI Threat Tracker: From Prompting to Autonomy – The Evolution of Adversarial AI](#)
Google Threat Intel • 2026-09-08 / 検出表記：UNC6780