Network Detection and Response

Report

PSI新宿① 8ec79c06-70e4-87cc-564e-d41411adf4d7 日次レポート (2026-08-30)

日次レポート

PSI新宿① 8ec79c06-70e4-87cc-564e-d41411adf4d7

レポート期間: 2026-08-30 00:00 ～ 2026-08-30 23:59

脅威 — High 0件を含む計17件の脅威を検出 / 影響アセット1件以上 要確認

リスク件数	セッション	トラフィック	影響対象アセット
17件	386,707 前日比 ▼ 86,988	2.1 GB 前日比 ▼ 764.3 MB	1件以上 前日比 ▲ 0

本日の脅威分布（17件）

前日 15件 → 本日 17件

High 0件 (0%) — Medium 17件 (100%) — Low 0件 (0%)

上位脅威 TOP 5

MEDIUM 192.168[redacted] 08月30日 23:53

[AI脅威検出] 内部の単一ホストが複数の外部NetBIOSサーバーをスキャンするネットワーク異常兆候検知

NetBIOS（Network Basic Input/Output System）は、Windows環境でシステム間の名前解決、ファイル共有、プリンタ共有などの機能を提供するプロトコルで、主に内部ネットワークで使用されます。UDP 137、UDP 138、TCP 139ポートを使用し、SMB（Server Message Block）プロトコルと連携してファイル共有やネットワークサービスに重要な役割を果たします。しかし、内部の単一ホストが多くの外部NetBIOSサーバーを対象にポートスキャンを実行する行為は、異常なネットワーク活動として認識される可能性が高く、内部システムがマルウェアに感染しているか、攻撃者がリモート制御を行っている可能性が示唆されます。 攻撃者はNetBIOSスキャンを利用して、外部ネットワークのSMB脆弱性を探索したり、匿名アクセス（Anonymous Access）、アカウント情報収集、セッションハイジャック（Session Hijacking）、リモートコード実行（Remote Code Execution, RCE）などの追加攻撃を試みる可能性があります。特に、内部システムがマルウェアに感染している場合、ボットネット（Botnet）活動の一環として外部ネットワークをターゲットにした自動化されたSMB攻撃が行われる可能性があります。そのため、内部で大量のNetBIOSポートスキャンが検出された場合、これは未承認のリモート接続試行、内部システムの悪質な活動の兆候、または外部ネットワークへの攻撃の拡散を意味する可能性があります。 NetBIOSポートスキャンが検出された場合、スキャンを実行している内部ホストの行動分析、特定の外部サーバーを対象に繰り返しスキャンを行っているか、一定の時間間隔で自動化されたスキャンが発生しているかなどを確認する必要があります。必要に応じて、疑わしい内部システムのネットワーク隔離、SMBトラフィックの制限、NetBIOS関連ポートのブロック、セキュリティパッチの適用および認証ポリシーの強化などの対策を実施し、追加のセキュリティリスクを防ぐことが重要です。

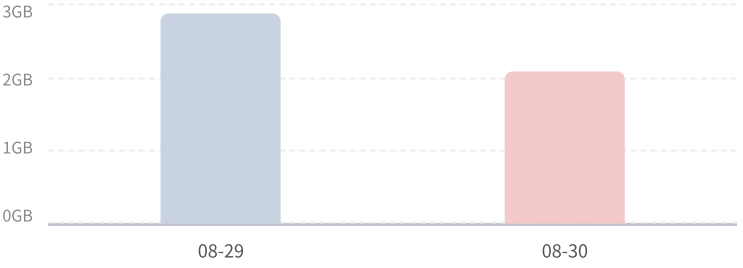
Scan NetBIOS

脅威アセット現況 TOP 5

IPアドレス	リスクレベル	比率	総件数
192.168[redacted]	Medium 17		17件

トラフィック前日比較

2026-08-29 トラフィック	2026-08-30 トラフィック
2.9 GB	2.1 GB
セッション 473,695	セッション 386,707



CTX 脅威インテリジェンス

Feed 総計	High
134,587 ▼ 2,030	3,672 ▼ 1,034

収集された国 TOP 5

1	アメリカ合衆国	35,986
2	中国	11,825
3	ドイツ	7,667
4	オランダ	7,003
5	ロシア	5,257

ネットワーク分析

プロトコル TOP 10

#	Protocol	比率	セッション件数
1	TCP		136,756
2	UDP		135,190
3	DNS		72,770
4	SSL		29,353
5	NETBIOS		4,451
6	QUIC		2,249
7	SSDP		1,395
8	HTTP		1,042
9	LINK-LOCAL MULTICAST NAME RESOLUTION		959
10	SIP		704

アプリケーション TOP 10

#	Application	比率	セッション件数
1	unclassified		9,893
2	Microsoft Services		2,443
3	Google APIs		1,862
4	Microsoft 365		582
5	Microsoft Teams		430
6	Google Play		374
7	ATT Services		345
8	Mozilla Services		328
9	GStatic		326
10	Google Meet		325

Threat Insight

AI 脅威検出 自動分類・High 0件

合計脅威件数	送信元IP (SRC)	宛先IP (DST)	検出時間帯
0件 High のみ	1件以上	0件以上	-

発生元 IP 別脅威タイムライン

High

00:00 03:00 06:00 09:00 12:00 15:00 18:00 21:00

発生元 IP グループ別詳細

192.168.[redacted]　合計 17 件

Ticket	発生時間	プレイブック名	リスクレベル	宛先IP
39792	2026-08-30 03:23:20	[AI脅威検出] 内部の単一ホストが複数の外部NetBIOSサーバーをスキャンするネットワーク異常兆候検知 NetBIOS（Network Basic Input/Output System）は、Windows環境でシステム間の名前解決、ファイル共有、プリンタ共有などの機能を提供するプロトコルで、主に内部ネットワークで使用されます。UDP 137、UDP 138、TCP 139ポートを使用し、SMB（Server Message Block）プロトコルと連携してファイル共有やネットワークサービスに重要な役割を果たします。しかし、内部の単一ホストが多くの外部NetBIOSサーバーを対象にポートスキャンを実行する行為は、異常なネットワーク活動として認識される可能性が高く、内部システムがマルウェアに感染しているか、攻撃者がリモート制御を行っている可能性が示唆されます。 攻撃者はNetBIOSスキャンを利用して、外部ネットワークのSMB脆弱性を探索したり、匿名アクセス（Anonymous Access）、アカウント情報収集、セッションハイジャック（Session Hijacking）、リモートコード実行（Remote Code Execution, RCE）などの追加攻撃を試みる可能性があります。特に、内部システムがマルウェアに感染している場合、ボットネット（Botnet）活動の一環として外部ネットワークをターゲットにした自動化されたSMB攻撃が行われる可能性があります。そのため、内部で大量のNetBIOSポートスキャンが検出された場合、これは未承認のリモート接続試行、内部システムの悪質な活動の兆候、または外部ネットワークへの攻撃の拡散を意味する可能性があります。 NetBIOSポートスキャンが検出された場合、スキャンを実行している内部ホストの行動分析、特定の外部サーバーを対象に繰り返しスキャンを行っているか、一定の時間間隔で自動化されたスキャンが発生しているかなどを確認する必要があります。必要に応じて、疑わしい内部システムのネットワーク隔離、SMBトラフィックの制限、NetBIOS関連ポートのブロック、セキュリティパッチの適用および認証ポリシーの強化などの対策を実施し、追加のセキュリティリスクを防ぐことが重要です。	MEDIUM	192.168.[redacted]

Ticket	発生時間	プレイブック名	リスクレベル	宛先IP
39795	2026-08-30 04:23:20	[AI脅威検出] 内部の単一ホストが複数の外部NetBIOSサーバーをスキャンするネットワーク異常兆候検知 NetBIOS（Network Basic Input/Output System）は、Windows環境でシステム間の名前解決、ファイル共有、プリンタ共有などの機能を提供するプロトコルで、主に内部ネットワークで使用されます。UDP 137、UDP 138、TCP 139ポートを使用し、SMB（Server Message Block）プロトコルと連携してファイル共有やネットワークサービスに重要な役割を果たします。しかし、内部の単一ホストが多くの外部NetBIOSサーバーを対象にポートスキャンを実行する行為は、異常なネットワーク活動として認識される可能性が高く、内部システムがマルウェアに感染しているか、攻撃者がリモート制御を行っている可能性が示唆されます。 攻撃者はNetBIOSスキャンを利用して、外部ネットワークのSMB脆弱性を探索したり、匿名アクセス（Anonymous Access）、アカウント情報収集、セッションハイジャック（Session Hijacking）、リモートコード実行（Remote Code Execution, RCE）などの追加攻撃を試みる可能性があります。特に、内部システムがマルウェアに感染している場合、ボットネット（Botnet）活動の一環として外部ネットワークをターゲットにした自動化されたSMB攻撃が行われる可能性があります。そのため、内部で大量のNetBIOSポートスキャンが検出された場合、これは未承認のリモート接続試行、内部システムの悪質な活動の兆候、または外部ネットワークへの攻撃の拡散を意味する可能性があります。 NetBIOSポートスキャンが検出された場合、スキャンを実行している内部ホストの行動分析、特定の外部サーバーを対象に繰り返しスキャンを行っているか、一定の時間間隔で自動化されたスキャンが発生しているかなどを確認する必要があります。必要に応じて、疑わしい内部システムのネットワーク隔離、SMBトラフィックの制限、NetBIOS関連ポートのブロック、セキュリティパッチの適用および認証ポリシーの強化などの対策を実施し、追加のセキュリティリスクを防ぐことが重要です。	MEDIUM	192.168[redacted]
39799	2026-08-30 05:53:20	[AI脅威検出] 内部の単一ホストが複数の外部NetBIOSサーバーをスキャンするネットワーク異常兆候検知 NetBIOS（Network Basic Input/Output System）は、Windows環境でシステム間の名前解決、ファイル共有、プリンタ共有などの機能を提供するプロトコルで、主に内部ネットワークで使用されます。UDP 137、UDP 138、TCP 139ポートを使用し、SMB（Server Message Block）プロトコルと連携してファイル共有やネットワークサービスに重要な役割を果たします。しかし、内部の単一ホストが多くの外部NetBIOSサーバーを対象にポートスキャンを実行する行為は、異常なネットワーク活動として認識される可能性が高く、内部システムがマルウェアに感染しているか、攻撃者がリモート制御を行っている可能性が示唆されます。 攻撃者はNetBIOSスキャンを利用して、外部ネットワークのSMB脆弱性を探索したり、匿名アクセス（Anonymous Access）、アカウント情報収集、セッションハイジャック（Session Hijacking）、リモートコード実行（Remote Code Execution, RCE）などの追加攻撃を試みる可能性があります。特に、内部システムがマルウェアに感染している場合、ボットネット（Botnet）活動の一環として外部ネットワークをターゲットにした自動化されたSMB攻撃が行われる可能性があります。そのため、内部で大量のNetBIOSポートスキャンが検出された場合、これは未承認のリモート接続試行、内部システムの悪質な活動の兆候、または外部ネットワークへの攻撃の拡散を意味する可能性があります。 NetBIOSポートスキャンが検出された場合、スキャンを実行している内部ホストの行動分析、特定の外部サーバーを対象に繰り返しスキャンを行っているか、一定の時間間隔で自動化されたスキャンが発生しているかなどを確認する必要があります。必要に応じて、疑わしい内部システムのネットワーク隔離、SMBトラフィックの制限、NetBIOS関連ポートのブロック、セキュリティパッチの適用および認証ポリシーの強化などの対策を実施し、追加のセキュリティリスクを防ぐことが重要です。	MEDIUM	192.168[redacted]

Ticket	発生時間	プレイブック名	リスクレベル	宛先IP
39804	2026-08-30 07:23:20	[AI脅威検出] 内部の単一ホストが複数の外部NetBIOSサーバーをスキャンするネットワーク異常兆候検知 NetBIOS（Network Basic Input/Output System）は、Windows環境でシステム間の名前解決、ファイル共有、プリンタ共有などの機能を提供するプロトコルで、主に内部ネットワークで使用されます。UDP 137、UDP 138、TCP 139ポートを使用し、SMB（Server Message Block）プロトコルと連携してファイル共有やネットワークサービスに重要な役割を果たします。しかし、内部の単一ホストが多くの外部NetBIOSサーバーを対象にポートスキャンを実行する行為は、異常なネットワーク活動として認識される可能性が高く、内部システムがマルウェアに感染しているか、攻撃者がリモート制御を行っている可能性が示唆されます。 攻撃者はNetBIOSスキャンを利用して、外部ネットワークのSMB脆弱性を探索したり、匿名アクセス（Anonymous Access）、アカウント情報収集、セッションハイジャック（Session Hijacking）、リモートコード実行（Remote Code Execution, RCE）などの追加攻撃を試みる可能性があります。特に、内部システムがマルウェアに感染している場合、ボットネット（Botnet）活動の一環として外部ネットワークをターゲットにした自動化されたSMB攻撃が行われる可能性があります。そのため、内部で大量のNetBIOSポートスキャンが検出された場合、これは未承認のリモート接続試行、内部システムの悪質な活動の兆候、または外部ネットワークへの攻撃の拡散を意味する可能性があります。 NetBIOSポートスキャンが検出された場合、スキャンを実行している内部ホストの行動分析、特定の外部サーバーを対象に繰り返しスキャンを行っているか、一定の時間間隔で自動化されたスキャンが発生しているかなどを確認する必要があります。必要に応じて、疑わしい内部システムのネットワーク隔離、SMBトラフィックの制限、NetBIOS関連ポートのブロック、セキュリティパッチの適用および認証ポリシーの強化などの対策を実施し、追加のセキュリティリスクを防ぐことが重要です。	MEDIUM	192.168.1.77
39808	2026-08-30 08:53:20	[AI脅威検出] 内部の単一ホストが複数の外部NetBIOSサーバーをスキャンするネットワーク異常兆候検知 NetBIOS（Network Basic Input/Output System）は、Windows環境でシステム間の名前解決、ファイル共有、プリンタ共有などの機能を提供するプロトコルで、主に内部ネットワークで使用されます。UDP 137、UDP 138、TCP 139ポートを使用し、SMB（Server Message Block）プロトコルと連携してファイル共有やネットワークサービスに重要な役割を果たします。しかし、内部の単一ホストが多くの外部NetBIOSサーバーを対象にポートスキャンを実行する行為は、異常なネットワーク活動として認識される可能性が高く、内部システムがマルウェアに感染しているか、攻撃者がリモート制御を行っている可能性が示唆されます。 攻撃者はNetBIOSスキャンを利用して、外部ネットワークのSMB脆弱性を探索したり、匿名アクセス（Anonymous Access）、アカウント情報収集、セッションハイジャック（Session Hijacking）、リモートコード実行（Remote Code Execution, RCE）などの追加攻撃を試みる可能性があります。特に、内部システムがマルウェアに感染している場合、ボットネット（Botnet）活動の一環として外部ネットワークをターゲットにした自動化されたSMB攻撃が行われる可能性があります。そのため、内部で大量のNetBIOSポートスキャンが検出された場合、これは未承認のリモート接続試行、内部システムの悪質な活動の兆候、または外部ネットワークへの攻撃の拡散を意味する可能性があります。 NetBIOSポートスキャンが検出された場合、スキャンを実行している内部ホストの行動分析、特定の外部サーバーを対象に繰り返しスキャンを行っているか、一定の時間間隔で自動化されたスキャンが発生しているかなどを確認する必要があります。必要に応じて、疑わしい内部システムのネットワーク隔離、SMBトラフィックの制限、NetBIOS関連ポートのブロック、セキュリティパッチの適用および認証ポリシーの強化などの対策を実施し、追加のセキュリティリスクを防ぐことが重要です。	MEDIUM	192.168.1.77