株式会社サンプルレポート様 御中

Catoクラウド運用サービス
月次報告書 別紙
(2023年12月度)

SCSK株式会社

2024年1月2日

1. トラフィック分析

1.1. サイト一覧

表 1. サイト一覧 (2024年1月1日時点)

サイト名	接続タイプ	接続状態	帯域 (Mbps)	PoP	HA状態	転送量 (Upstream)	転送量 (Downstream)
本社サイト	Socket X1500	接続	25	Osaka	-	3.5 GB	9.1 GB
PoCサイト	Socket X1500	切断	-	Osaka_DC2	-	-	-

1.2. サイト : 本社サイト

1.2.1. 最大スループット(Upstream)

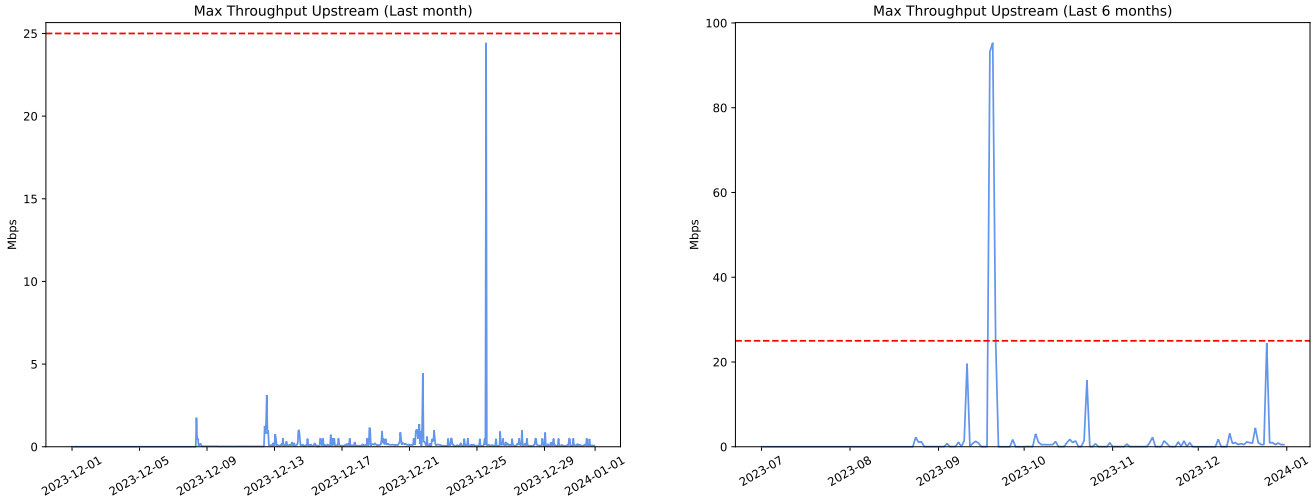

図 1. 最大スループット(Upstream)

1.2.2. 最大スループット(Downstream)

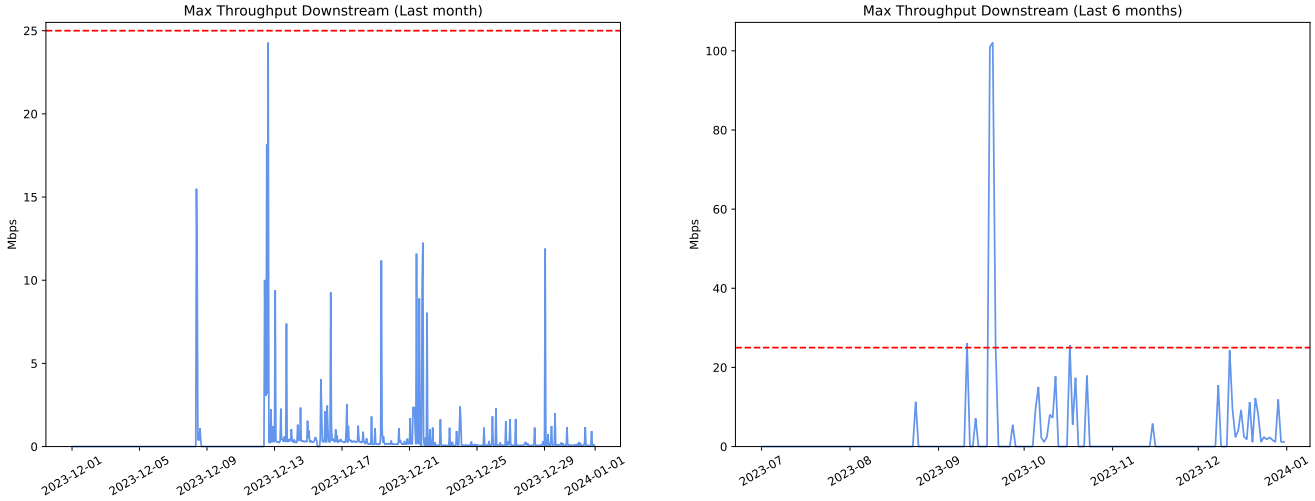

図 2. 最大スループット(Downstream)

1.2.3. 平均スループット(Upstream)

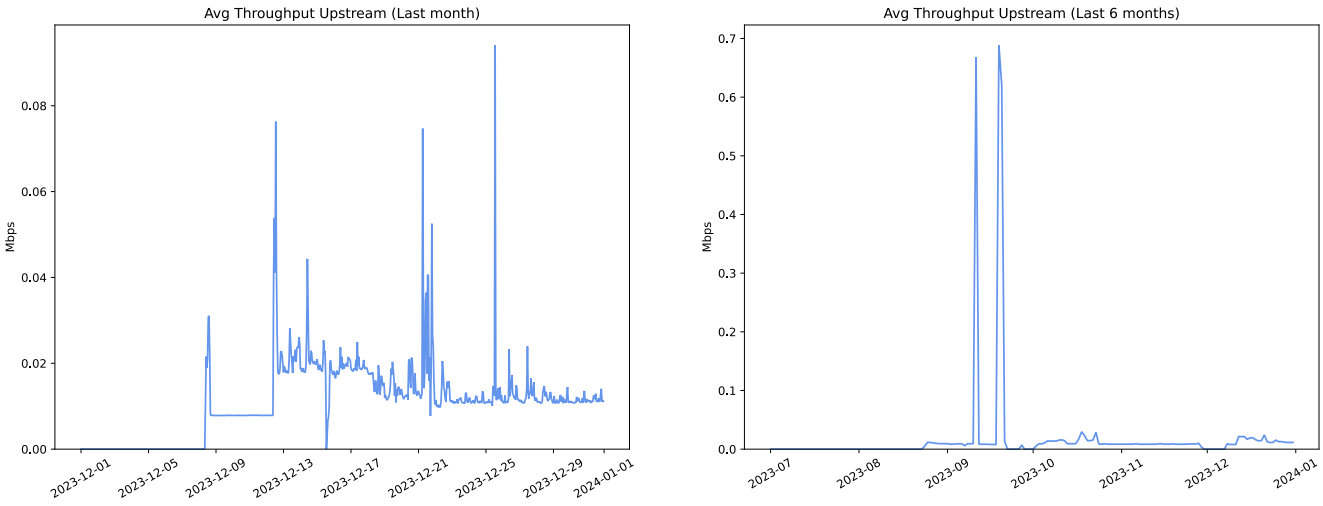

図 3. 平均スループット(Upstream)

1.2.4. 平均スループット(Downstream)

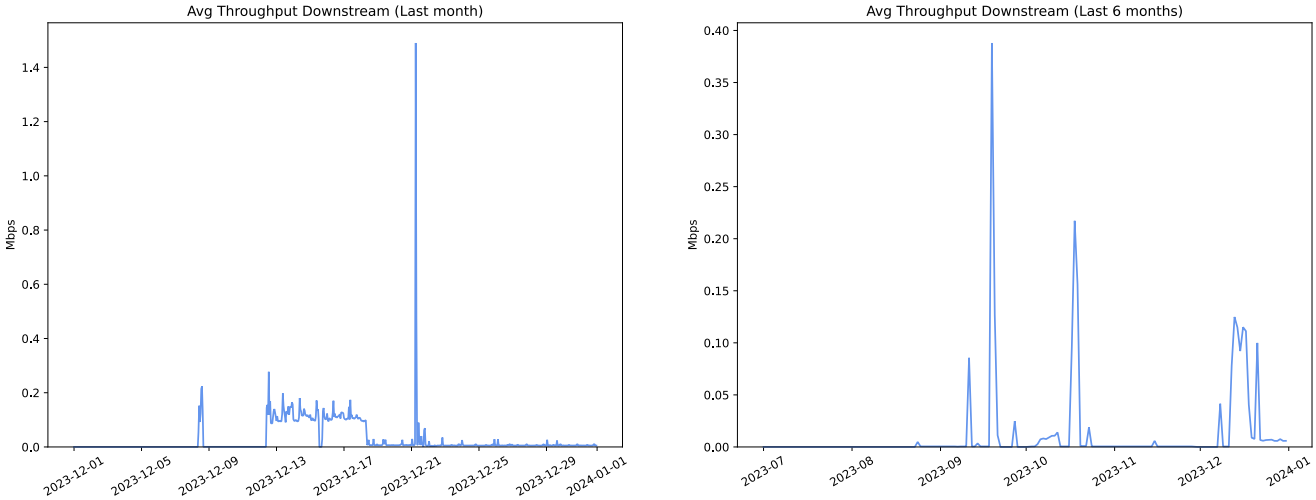

図 4. 平均スループット(Downstream)

1.2.5. パケット損失率(Upstream)

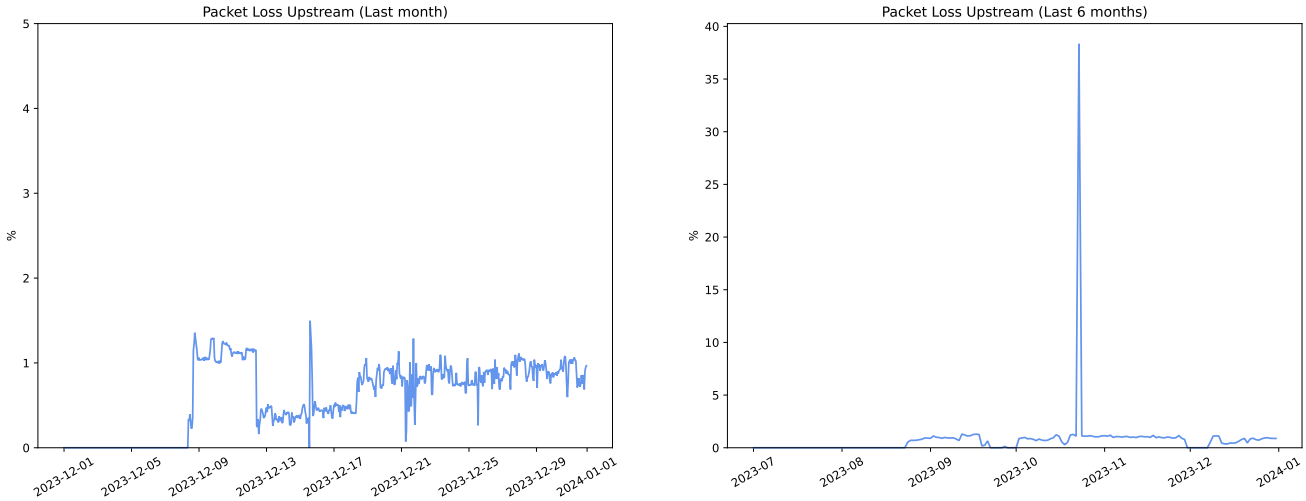

図 5. パケット損失率(Upstream)

1.2.6. パケット損失率(Downstream)

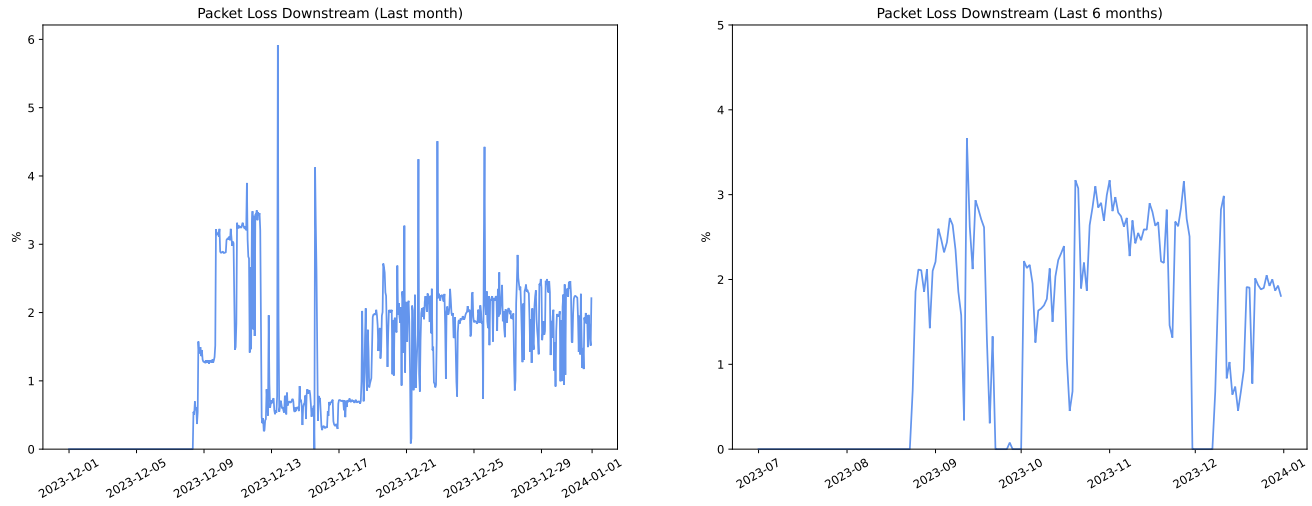

図 6. パケット損失率(Downstream)

1.2.7. パケット破棄率(Upstream)

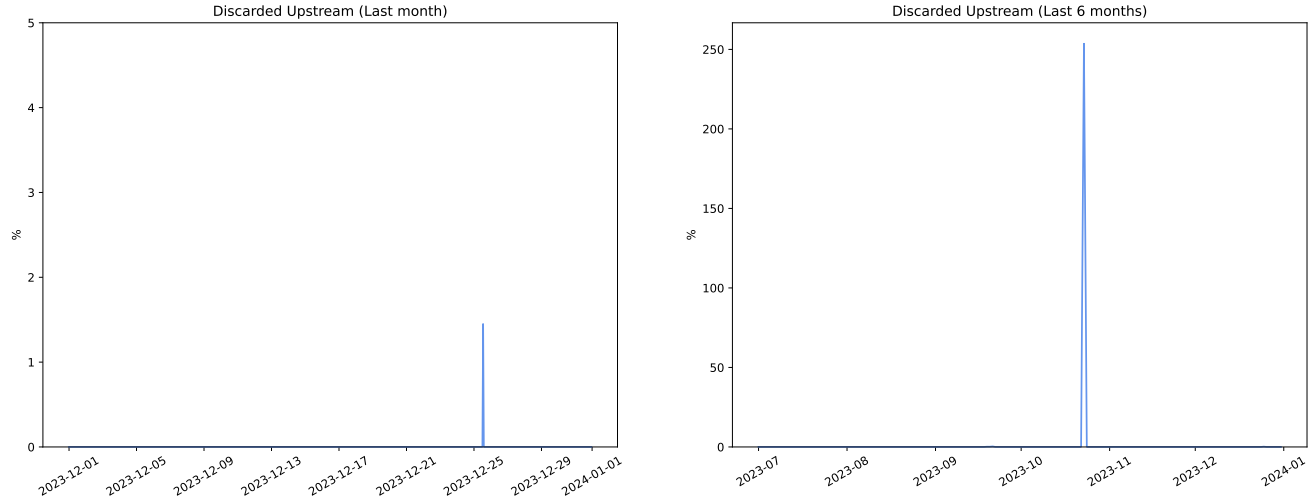

図 7. パケット破棄率(Upstream)

1.2.8. パケット破棄率(Downstream)

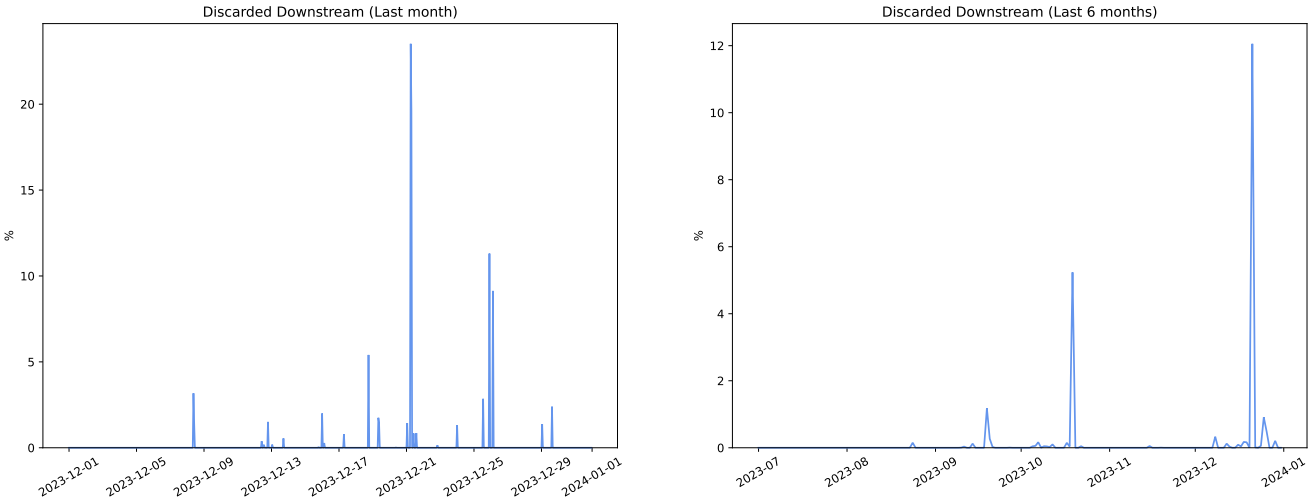

図 8. パケット破棄率(Downstream)

1.2.9. ジッタ(Upstream)

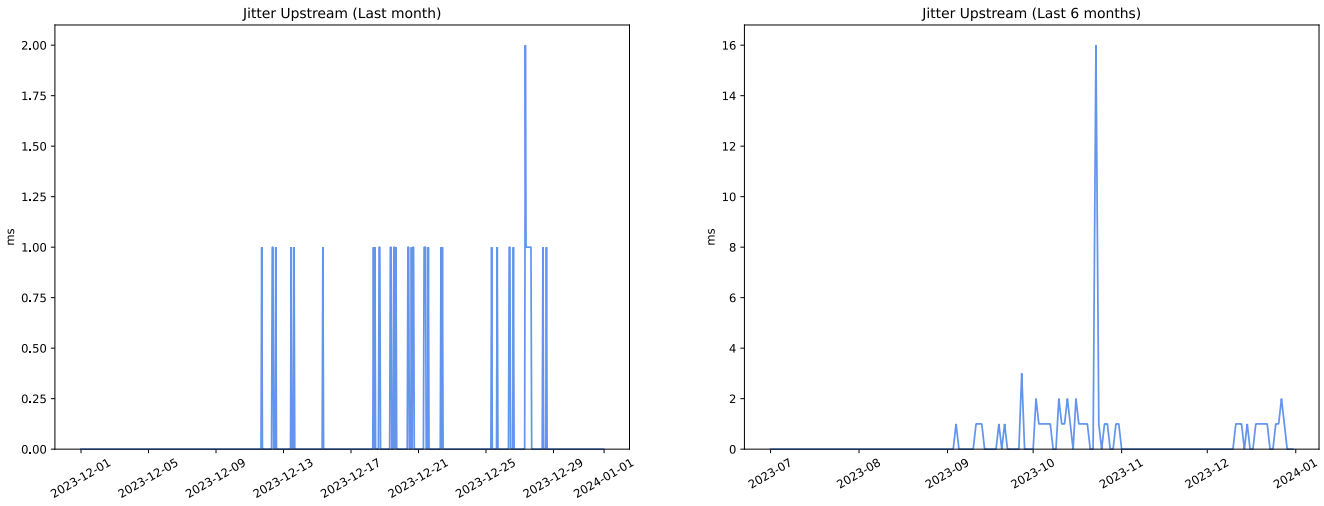

図 9. ジッタ(Upstream)

1.2.10. ジッタ(Downstream)

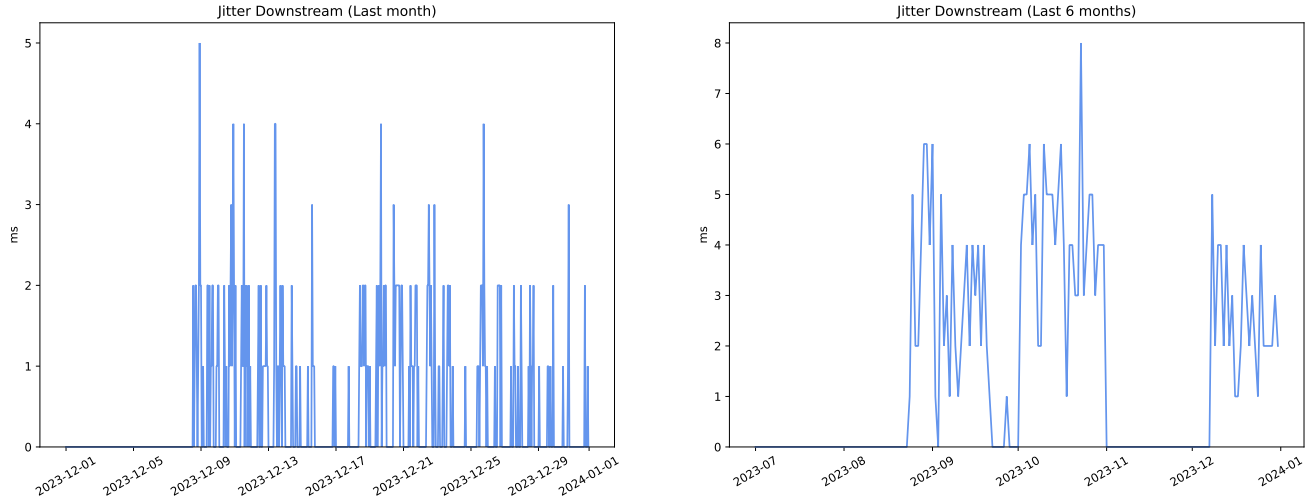

図 10. ジッタ(Downstream)

1.2.11. ラウンドトリップタイム

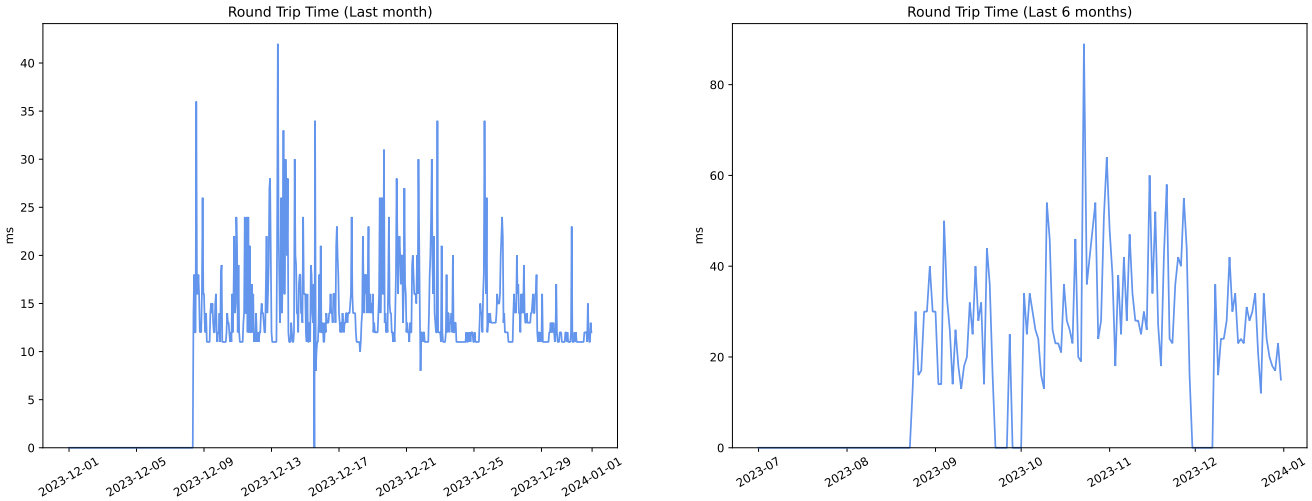

図 11. ラウンドトリップタイム

1.2.12. ラストマイルパケット損失

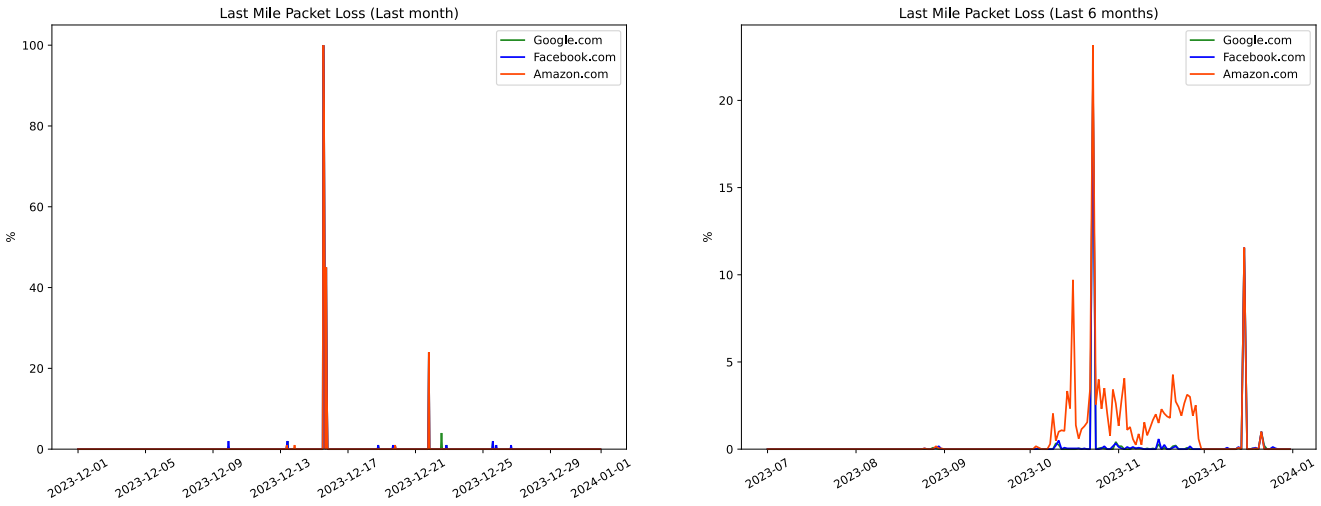

図 12. ラストマイルパケット損失

1.2.13. ラストマイル距離

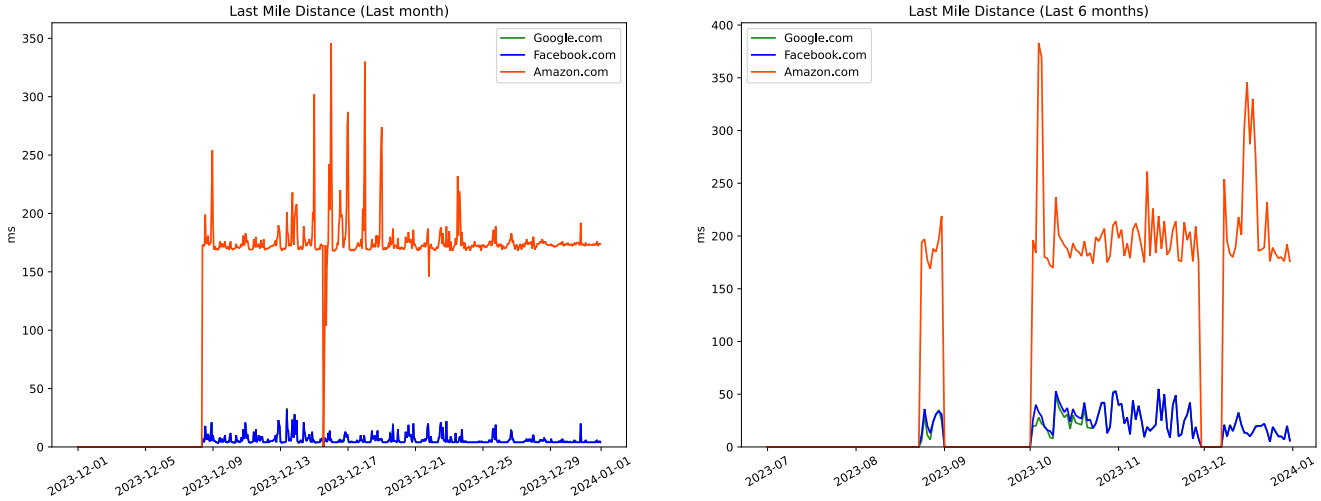

図 13. ラストマイル距離

1.3. サイト : PoCサイト

データがありません。

2. イベント分析

2.1. 発生イベント集計

表 2. 発生イベント集計

Event Type	Event Sub Type	2023年11月	2023年12月
Connectivity	ApiKey	606	623
	Cato Management Application	2	17
	Changed Pop	6	27
	Client Connectivity Policy	150	575
	Connected	100	110
	DHCP Lease	1	38
	Disconnected	98	95
	Reconnected	55	153
	小計	**1,018**	**1,638**
Routing	BGP Routing	139	0
	BGP Session	23	0
	VPN Never-Off Bypass	15	47
	小計	**177**	**47**
Security	Anti Malware	509	779
	Apps Security	28	32
	DNS Protection	0	21
	IPS	0	2
	Internet Firewall	33,107	533,823
	LAN Firewall	0	3,221
	NG Anti Malware	0	1
	SaaS Security API Data Protection	7	0
	Suspicious Activity	2	572
	TLS	3,182	324,199
	WAN Firewall	70	124
	小計	**36,905**	**862,774**
Sockets Management	Socket Upgrade	6	2
	Socket WebUI Access	7	21
	小計	**13**	**23**
System	Sdp license	2	5
	小計	**2**	**5**

2.2. Socket接続履歴

2.2.1. イベントサマリー

表 3. Socket接続イベントサマリー

サイト名	Connected 回数	Disconnected 回数	Changed Pop 回数
本社サイト	7	6	6

※上表に記載のないサイトのSocketでは接続変更に関するイベントは発生していませんでした。

2.2.2. 本社サイト

表 4. Socket接続履歴 (本社サイト)

日時 (日本時間)	Event Sub Type	Role	Interface	PoP
2023-12-08 09:34:33	Connected	-	WAN1	Osaka
2023-12-15 12:48:42	Disconnected	-	WAN1	Osaka
2023-12-15 14:26:09	Connected	-	WAN1	Osaka
2023-12-15 14:49:37	Disconnected	-	WAN1	Osaka
2023-12-15 15:07:55	Connected	-	WAN1	Tokyo_DC2
2023-12-15 16:04:45	Changed Pop	-	WAN1	Osaka
2023-12-15 16:05:04	Changed Pop	-	WAN1	Osaka
2023-12-15 17:26:42	Disconnected	-	WAN1	Osaka
2023-12-15 17:37:34	Connected	-	WAN1	Tokyo
2023-12-15 17:42:40	Disconnected	-	WAN1	Tokyo
2023-12-15 17:51:39	Connected	-	WAN1	Tokyo_DC2
2023-12-15 18:13:12	Disconnected	-	WAN1	Tokyo_DC2
2023-12-15 18:18:45	Connected	-	WAN1	Osaka
2023-12-21 19:27:59	Disconnected	-	WAN1	Osaka
2023-12-21 19:32:56	Connected	-	WAN1	Tokyo
2023-12-21 19:36:39	Changed Pop	-	WAN1	Tokyo_DC2
2023-12-21 20:30:32	Changed Pop	-	WAN1	Osaka
2023-12-21 20:30:32	Changed Pop	-	WAN1	Tokyo_DC2
2023-12-21 20:30:54	Changed Pop	-	WAN1	Osaka

2.3. Socketアップグレード履歴

表 5. Socketアップグレード履歴

サイト	日時 (日本時間)	Role	実行結果	旧バージョン	新バージョン
本社サイト	2023-12-01 12:16:19	-	Succeeded	19.0.17412	19.0.17463
本社サイト	2023-12-02 12:15:34	-	Succeeded	19.0.17463	19.0.17557

2.4. Internet Firewall

2.4.1. ルール適用数

表 6. Internet Firewall ルール適用数

ルール	Action	2023年11月	2023年12月
Any Allow	Monitor	30,735	530,717
Block QUIC apps	Block	278	952
Block QUIC services	Block	1,857	2,010
Default block for Categories	Block	40	60
Default prompt for Categories	Prompt	127	77
RBI Test	RBI	70	7
	合計	**33,107**	**533,823**

※トラッキング対象で上表に記載のないルールは、適用された通信がなかったことを示しています。

2.4.2. カテゴリ内訳 (ルール：Default block for Categories)

表 7. カテゴリ内訳 (ルール：Default block for Categories)

カテゴリ	2023年11月	2023年12月
Games	40	58
General	3	50
Malware	0	2
Business Systems	3	0

※複数のカテゴリに該当する通信は重複カウントしています。

2.4.3. カテゴリ内訳 (ルール：Default prompt for Categories)

表 8. カテゴリ内訳 (ルール：Default prompt for Categories)

カテゴリ	2023年11月	2023年12月
Anonymizers	62	69
Network Utilities	53	52
General	13	36
DNS over HTTPS	23	17
Information Security	27	16
Parked domains	65	8
Computers and Technology	54	1
Business Systems	1	0

※複数のカテゴリに該当する通信は重複カウントしています。

2.5. WAN Firewall

表 9. WAN Firewall ルール適用数

ルール	Action	2023年11月	2023年12月
LAN FW TEST	Block	0	87
test_20230919	Monitor	70	37
	合計	**70**	**124**

※トラッキング対象で上表に記載のないルールは、適用された通信がなかったことを示しています。

2.6. Suspicious Activity

表 10. Suspicious Activity

Risk Level	宛先国名	プロトコル	宛先ドメイン	宛先ポート	Threat Name	検知数
Medium	Japan	TCP	xxx.xxx.jp	44301	HTTP Requests Over Non Standard Ports To Low Popularity Destinations	152
Medium	Japan	TCP	yyy.yyy.jp	443	Microsoft BITS over HTTP to low popularity domains	420
					合計	**572**

※Catoによって脅威として判定されたイベント (Risk Level が空欄でないもの) のみ記載しています。

イベントの詳細内容は Cato Management Application で確認してください。

2.7. DNS Protection

表 11. DNS Protection

Action	カテゴリ	DNSクエリ	Mitre Attack Tactics	検知数
Block	Malicious Domains	xxx.pl	Command and Control (TA0011)	12
Block	Malicious Domains	yyy.co.uk	Command and Control (TA0011)	5
Block	Command and Control (C&C)	zzz.pl	Command and Control (TA0011)	4
			合計	**21**

2.8. TLS

表 12. TLS

ドメイン	宛先ポート	アプリケーション	エラー内容	エラー数
business.bing.com	443	Bing	certificate unknown	2
edgeservices.bing.com	443	Bing	certificate unknown	7
www.bing.com	443	Bing	certificate unknown	4

ドメイン	宛先ポート	アプリケーション	エラー内容	エラー数
google.com	443	Google applications	certificate unknown	4
accounts.google.com	443	Google applications	certificate unknown	11
adservice.google.com	443	Google applications	certificate unknown	5
clients2.google.com	443	Google applications	certificate unknown	39
id.google.com	443	Google applications	certificate unknown	6
support.google.com	443	Google applications	certificate unknown	1
(サンプルのため省略)				
			合計	**48,123**

3. ユーザ分析

3.1. 当月接続のないユーザ

当月に Cato Client によるリモート接続のないユーザの一覧です。

表 13. 当月接続のないユーザ

名前	メールアドレス	最終接続日
Taro SCSK	scsk-taro@example.com	2023年6月26日
Jiro SCSK	scsk-jiro@example.com	2023年7月23日
Saburo SCSK	scsk-saburo@example.com	-
合計		**3**

※最終接続日が - となっているユーザは、リモート接続した形跡が過去のログにも残っていないことを示しています。