第 5 章　付録)システムログについて

本章では、システムログに出力されるログの内容について記載します

1. 状態監視ログ

以下の状態監視ログが出力されます。

－本装置の状態（セッション制限、帯域制限、スパム制限）

－登録された監視対象の死活監視

【セッション制限】

＞利用者のセッション数が「オプション設定-セッション制限」の"1 利用者あたりセッション数の上限"を超えた場合、ログが出力されます（独自ログフォーマット）。

No	項目名	内容	例
1	日時	ログ出力日時	Jun 10 15:48:46 ALERT
2	監視項目	セッション	[Router] Session
3	状態	WARNING（閾値ｵｰﾊﾞｰ） CRITICAL（閾値ｵｰﾊﾞｰ） OK（状態復旧）	Session CRITICAL-セッション制限中
4	部屋番号	閾値オーバーを検出した部屋番号（部屋管理設定を行っていない場合は「（未検出）」と表示）	306 号室
5	MAC アドレス	閾値オーバーによって制限中の端末の MAC アドレス	00:19:DB:00:00:40
6	IP アドレス	閾値オーバーによって制限中の端末の IP アドレス	192.168.1.199
7	該当端末のセッション数	閾値オーバーを検出した時点の該当端末が張っているセッション数（セッション数がしきい値以下になった場合は表示されません）	(649)
8	装置全体のセッション数	ログ出力時点の装置全体のセッション数（TCP および UDP の合計）	(715)
9	セッション制限の閾値	セッション制限の閾値（例では 1 利用者あたりセッション数の上限(1)：500、1 利用者あたりセッション数の上限(2)：750）	(limit 500-750s/1user)

※306 号室の端末で 649 セッション使用され、セッション制限がかかっている場合

Jun 10 15:48:46 ALERT: [Router] Session | Session CRITICAL - セッション制限中[306 号室

/00:19:DB:00:00:40/192.168.1.199(649)] (715) (limit 500-750s/1user)

【スパム制限】
＞利用者のメール送信数が「オプション設定-スパム制限」の"1 利用者あたりメール送信の上限"を超えた場合、ログが出力されます（独自ログフォーマット）。

No	項目名	内容	例
1	日時	ログ出力日時	Jun 10 16:09:40 ALERT
2	監視項目	スパムメール	spam mail
3	状態	WARNING（閾値ｵｰﾊﾞｰ） CRITICAL（閾値ｵｰﾊﾞｰ） OK（状態復旧）	Spam Mail CRITICAL - スパム制限中
4	部屋番号	閾値オーバーを検出した部屋番号（部屋管理設定を行っていない場合は「（未検出）」と表示）	306 号室
5	MAC アドレス	閾値オーバーによって制限中の端末の MAC アドレス	00:19:DB:00:00:40
6	IP アドレス	閾値オーバーによって制限中の端末の IP アドレス	192.168.1.199
7	メール送信数	閾値オーバーを検出した時点に該当端末が送信したメール送信数（初回しか表示されません）	(101)
8	スパム制限の閾値	スパム制限の閾値（例では 1 利用者あたりのメール送信数の上限：10 通／1 分）	(limit 10mail/1user)

※306 号室で 101 通の送信を行ったのでスパム制限にかかっている場合。
Jun 10 16:09:40 ALERT: spam mail | Spam Mail CRITICAL - スパム制限中 [306 号室 /00:19:DB:00:00:40/192.168.1.199(101)] (limit 10mail/1user)

【帯域制限】

＞利用者の帯域量が「オプション設定-帯域制限」の"1 利用者あたり帯域使用量の上限"を超えた場合、ログが出力されます（独自ログフォーマット）。

No	項目名	内容	例
1	日時	ログ出力日時	Jun 10 16:09:40 ALERT
2	監視項目	トラフィック	[Net] Traffic
3	状態	CRITICAL（閾値ｵｰﾊﾞｰ） OK（状態復旧）	Traffic CRITICAL -帯域制限中
4	部屋番号	閾値オーバーを検出した部屋番号（部屋管理設定を行っていない場合は「（未検出）」と表示）	306 号室
5	MAC アドレス	閾値オーバーによって制限中の端末の MAC アドレス	00:19:DB:00:00:40
6	IP アドレス	閾値オーバーによって制限中の端末の IP アドレス	192.168.1.199
7	トラフック量	閾値オーバーを検出した時点に該当端末が送受信したトラフィック量	(97.47Mbps) TX 97472648bps, RX 1745448bps
8	トラフィック量の閾値	帯域制限の閾値（例では 1 利用者あたりのトラフィックの上限：10Mbps／1 分）	(limit 10Mbps/1user)

※306 号室で 97.47Mbps の送信を行ったので帯域制限にかかっている場合。

Jun 10 16:09:40 ALERT: [Net] Traffic | Traffic CRITICAL -帯域制限中[TX 306 号室 /00:19:DB:00:00:40/192.168.1.199(97.47Mbps)] TX 97472648bps, RX 1745448bps (limit 10Mbps/1user)

【登録された監視対象の死活監視】

監視対象から ping 応答が正常に返らない場合、ログが出力されます。（独自ログフォーマット）

No	項目名	内容	例
1	日時	ログ出力日時	Jun 15 11:51:07 ALERT
2	監視項目	PING	[ping]
3	監視対象タイプ	監視設定で登録された監視対象タイプ（英数 5 文字まで）	SWHUB
4	監視対象 IP アドレス	監視設定で登録された監視対象の IP アドレス	192.168.1.250
5	状態	CRITICAL（疎通なし） OK（状態復旧）	CRITICAL - Host Unreachable (192.168.1.250)

※192.168.1.250 のスイッチ機器に対して PING 疎通がない場合。

Jun 15 11:51:07 ALERT: [ping] SWHUB 192.168.1.250 | CRITICAL - Host Unreachable (192.168.1.250)

2. DHCP ログ

本装置上で稼動している DHCP サービスのログが出力されます。

3. メールログ

本装置上で稼働している SMTP サーバのログが出力されます。
※「オプション設定-SMTP 代理送信」が有効（使用する）の場合のみ有効です。

4. 認証ログ

接続開始（認証）、接続終了（認証切断）に関するログが出力されます。（独自ログフォーマット）
※出力項目は、接続開始、接続終了とで異なります。

No	項目名	内容	接続開始	接続終了
1	日時	ログ出力日時	○	○
2	（未使用）	（未使用）	-	-
3	部屋番号	利用者の部屋番号 ＊部屋管理設定を行っていない場合は「（未検出）」と出力	○	-
4	接続開始時間	接続開始した時間	○	-
5	接続終了時間	接続終了した時間	-	○
6	課金金額	課金金額	○	-
7	認証方式	none：「ベーシック認証」による接続開始 auto：「フリー認証」による接続開始 otp：「アクセス ID 認証」による接続開始 preauth：自動認証設定による接続開始 radius：「Radius 認証」による接続開始 roaming：認証ローミングによる接続開始 extauth：「@Cloud 認証」による接続開始	○	○
8	アクセス ID	「アクセス ID 認証」にて使用されたアクセス ID、または「Radius 認証」にて使用されたアカウント	○	-
9	IP アドレス	利用者端末の IP アドレス	○	○
10	MAC アドレス	利用者端末の MAC アドレス	○	○
11	接続ポート	利用者端末が接続されたポートもしくはタグ VLAN の ID	○	-
12	Global 接続アドレス	利用者端末に割り当てられた Global 接続アドレス	○	-
13	言語	ブラウザの言語設定	○	-
14	ユーザエージェント	ユーザエージェント情報	○	-
15	ログ ID	@Cloud のログとの紐付け ID(@Cloud 使用時に出力)	○	○

> 306 号室でアクセス ID による Global 接続による認証の場合

Jun 20 22:22:37:, ,306 号室,2012/06/20 22:22:37,,1000,otp,PWD00020,10.10.10.10,00:00:00:00:0

0:21,10,10.10.10.10, en-US,Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.81 Safari/537.3,7c8ee50d7f1b7653a2217e3384ee90ef

5. アクティブログ

接続開始（認証）、接続終了（認証切断）に関するログが出力されます。（独自ログフォーマット）

※認証ローミング、@クラウドオプション利用時のみ有効。

対象機能利用時、認証ログに追加して、認証中の端末で未接続状態が 15 分間続くと接続終了の記録がされ、認証中の再接続時には、接続開始の記録がされます。

No	項目名	内容	接続開始	接続終了
1	日時	ログ出力日時	○	○
2	（未使用）	（未使用）	-	-
3	部屋番号	利用者の部屋番号 ＊部屋管理設定を行っていない場合は「（未検出）」と出力	○	-
4	接続開始時間	接続開始した時間	○	-
5	接続終了時間	接続終了した時間	-	○
6	課金金額	課金金額	○	-
7	認証方式	none：「ベーシック認証」による接続開始 auto：「フリー認証」による接続開始 otp：「アクセス ID 認証」による接続開始 preauth：自動認証設定による接続開始 radius：「Radius 認証」による接続開始 roaming：認証ローミングによる接続開始 extauth：「@Cloud 認証」による接続開始	○	○
8	アクセス ID	「アクセス ID 認証」にて使用されたアクセス ID、または「Radius 認証」にて使用されたアカウント	○	-
9	IP アドレス	利用者端末の IP アドレス	○	○
10	MAC アドレス	利用者端末の MAC アドレス	○	○
11	接続ポート	利用者端末が接続されたポートもしくはタグ VLAN の ID	○	-
12	Global 接続アドレス	利用者端末に割り当てられた Global 接続アドレス	○	-
13	言語	ブラウザの言語設定	○	-
14	ユーザエージェント	ユーザエージェント情報	○	-
15	ログ ID	@Cloud のログとの紐付け ID(@Cloud 使用時に出力)	○	○

> 306 号室でアクセス ID による Global 接続による認証の場合

Jun 20 22:22:37:, ,306 号室,2012/06/20 22:22:37,,1000,otp,PWD00020,10.10.10.10,00:00:00:00:00:21,10,10.10.10.10, en-US,Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.81 Safari/537.3,7c8ee50d7f1b7653a2217e3384ee90ef

6. トラフィックログ

＞POPCHAT の帯域量のログが出力されます (独自ログフォーマット)。

No	項目名	内容	例
1	日時	ログ出力日時	Jun 10 16:09:40
2	トラフィック量(上り)	トラフィック量 (上り) : Traffic TX ※単位 bps	TX 97472648bps
3	トラフィック量(下り)	トラフィック量 (下り) : Traffic RX ※単位 bps	RX 1745448bps

※例

Jun 10 16:09:40 Traffic TX 97472648bps, RX 1745448bps

7. セッションログ

＞POPCHAT の全体のセッションのログが出力されます (独自ログフォーマット)。

No	項目名	内容	例
1	日時	ログ出力日時	Jun 10 15:48:46
2	セッション数	セッション : Session	Session 715

※例

Jun 10 15:48:46 Session 715

【セッション制限】

＞利用者のセッション数が「オプション設定-セッション制限」の"1 利用者あたりセッション数の上限"を超えた場合、ログが出力されます (独自ログフォーマット)。

8. アクティブユーザ

＞POPCHAT に接続中の利用者数のログが出力されます (独自ログフォーマット)。

No	項目名	内容	例
1	日時	ログ出力日時	Jun 10 15:48:46
2	アクティブユーザ数	アクティブユーザ数 : ActiveUser	ActiveUser 15

※例

Jun 10 15:48:46 ActiveUser 15