



ACNS ソフトウェア CLI コマンドの Content Distribution Manager GUI へ のマッピング

ここでは、ACNS 5.5 Content Distribution Manager GUI でサポートされている CLI コマンドとサポートされていない CLI コマンドをリストします。この章の内容は、次のとおりです。

- [Content Distribution Manager GUI でサポートされている CLI コマンド \(p.D-2\)](#)
- [Content Distribution Manager GUI でサポートされていない CLI コマンド \(p.D-24\)](#)

Content Distribution Manager GUI でサポートされている CLI コマンド

表 D-1 では、ACNS ソフトウェア CLI コマンドを対応する Content Distribution Manager GUI 手順にマッピングする方法を示しています。ソフトウェア CLI コマンドは、最初の列でアルファベット順に一覧表示されています。2 番目の列は、コマンドごとのデバイス グループ設定ウィンドウへの GUI ナビゲーションパスを示しています。3 番目の列は、このマニュアル内に記述されている GUI 設定手順へのリンクを説明します。ほとんどの場合、設定ウィンドウ、および GUI ウィンドウ内の各フィールドとその対応する CLI コマンドとのマッピングを示す表が手順の最後に掲載されています。



(注)

このマニュアルでは、ほとんどの場合、個々のデバイスに対する設定手順を説明していますが、次の表では、デバイス グループの設定ウィンドウへの GUI ナビゲーションパスを示しています。デバイス グループおよび個々のデバイスを設定する手順は、ほとんど同じです。

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング

コマンド	GUI ナビゲーションパス	参照先
<code>aaa accounting {commands {0 15} default {start-stop stop-only wait-start} tacacs exec default {start-stop stop-only wait-start} tacacs system default {start-stop stop-only} tacacs}</code>	Devices > Device Groups > General Settings > Authentication > AAA Accounting の順に選択	AAA アカウンティングの設定 (p.12-31)
<code>access-lists 300 {deny groupname {any [position number] groupname [position number]}} {permit groupname {any [position number] groupname [position number]}}</code>	Devices > Devices ¹ > General Settings > Authentication > Access List > Configure Access Control List の順に選択	グループ許可に対する ACL の設定 (p.18-2)
<code>access-lists enable</code>	Devices > Devices > General Settings > Authentication > Access List > Enable Access Control List の順に選択	ACL のイネーブル化 (p.18-3)
<code>acquirer proxy authentication outgoing ipaddress port_num username [password password] [ntlm domain [basic-auth-disable]]</code>	Devices > Device Groups > Applications > Web > HTTP > HTTP Connections の順に選択	Content Distribution Manager GUI を使用した HTTP プロキシ認証の設定 (p.6-44)
<code>acquirer proxy authentication transparent username [password password] [ntlm domain [basic-auth-disable]]</code>	Devices > Device Groups > Prepositioning > Acquirer WCCP Proxy Authentication の順に選択	Content Distribution Manager GUI を使用した WCCP プロキシ認証の設定 (p.6-45)
<code>asset tag name</code>	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > Asset Tag の順に選択	SNMP アセット タグの設定 (p.22-14)
<code>authentication {configuration login} {local radius tacacs} enable primary [secondary tertiary]</code>	Devices > Device Groups > General Settings > Authentication > Login Authentication の順に選択	ログイン認証と許可に対するデバイスの設定 (p.12-8)
<code>authentication fail-over server-unreachable</code>		
<code>bandwidth {real-proxy {incoming kbits outgoing kbits} real-server kbits wmm {incoming kbits outgoing kbits} cisco-streaming-engine kbits http kbits} {start-time weekday time end-time weekday time}</code>	Devices > Device Groups > Applications > Bandwidth Schedules の順に選択	予定帯域幅の設定 (p.9-47)

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
bandwidth { real-proxy { incoming <i>kbits</i> outgoing <i>kbits</i> } real-server <i>kbits</i> wmt { incoming <i>kbits</i> outgoing <i>kbits</i> } cisco-streaming-engine <i>kbits</i> http <i>kbits</i> } { default max-bandwidth }	Devices > Device Groups > Applications > Default and Maximum Bandwidth の順に選択	コンテンツ サービスのデフォルト帯域幅と最大帯域幅の設定 (p.9-46)
banner { motd login exec } message <i>message_text</i> banner enable	Devices > Device Groups > General Settings > Login Access Control > Message of the Day の順に選択	Content Engine の Message of the Day の設定 (p.20-5)
bitrate http default <i>bitrate</i>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings の順に選択	Content Engine の Windows Media プロキシの設定 (p.9-20)
bitrate wmt incoming <i>bitrate</i>		
bitrate wmt outgoing <i>bitrate</i>		
bypass auth-traffic enable	Devices > Device Groups > Request Routing > WCCP > Bypass の順に選択	WCCP バイパスの設定 (p.4-25)
bypass load { enable in-interval <i>seconds</i> out-interval <i>seconds</i> time-interval <i>minutes</i> }	Devices > Device Groups > Request Routing > WCCP > Bypass List の順に選択	WCCP バイパス リスト エントリの作成 (p.4-28)
bypass timer <i>minutes</i>	Devices > Device Groups > Request Routing > WCCP > Bypass の順に選択	WCCP バイパスの設定 (p.4-25)
bypass gateway <i>ipaddress</i>		
error-handling { reset-connection send-cache-error transparent }		
cdp enable	Devices > Device Groups > General Settings > Services > CDP の順に選択	CDP の設定 (p.20-8)
cdp holdtime <i>seconds</i>		
cdp timer <i>seconds</i>		
clock timezone <i>timezone offset</i>	Devices > Device Groups > General Settings > Services > Date/Time > Time Zone の順に選択	デバイス クロックと時間帯の設定 (p.20-14)
clock summertime <i>timezone</i> { date recurring }		
cms database maintenance full enable	Devices > Device Groups > General Settings > Services > Database Maintenance の順に選択	『Cisco ACNS Software Update and Maintenance Guide』 Release 5.x を参照
cms database maintenance full schedule { every-day <i>weekday at time</i> }		
cms database maintenance regular enable		
cms database maintenance regular schedule { every-day <i>weekday at time</i> }		
Content Router グローバル コンフィギュレーション コマンド : contentrouting leastloaded	Devices > Devices > Device Activation の順に選択	Content Router の負荷ベースのルーティングのイネーブル化 (p.4-61)
contentrouting servicemonitor { numberofsamples { all <i>number</i> cpu <i>number</i> disk <i>number</i> wmt <i>number</i> } sampleperiod { all <i>seconds</i> cpu <i>seconds</i> disk <i>seconds</i> wmt <i>seconds</i> } threshold { cpu <i>percentage</i> wmt <i>percentage</i> } type { all cpu disk wmt }}	Devices > Device Groups > General Settings > Notification and Tracking > Service Monitor の順に選択	負荷ベース ルーティングに対する Content Engine のスレッショールド制限の設定 (p.4-61)
dns min-ttl <i>seconds</i>	Devices > Devices ¹ > Applications > DNS > DNS Caching Server の順に選択	Content Engine の DNS キャッシング サーバの設定 (p.8-80)
dns max-ttl <i>seconds</i>		
dns user-expired enable		

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
dns max-cache-memory <i>mbytes</i>	Devices > Device Groups > General Settings > Services > DNS の順に選択	HTTP プロキシキャッシングの DNS サーバの設定 (p.8-87)
	Devices > Devices ¹ > Applications > DNS > DNS Caching Server の順に選択	Content Engine の DNS キャッシングサーバの設定 (p.8-80)
dns enable	Devices > Device Groups > General Settings > Services > DNS の順に選択	HTTP プロキシキャッシングの DNS サーバの設定 (p.8-87)
	Devices > Devices ¹ > Applications > DNS > DNS Caching Server の順に選択	Content Engine の DNS キャッシングサーバの設定 (p.8-80)
dns listen { all <i>ipaddress</i> } port <i>port_num</i> hostname <i>hostname</i>	Devices > Devices ¹ > Applications > DNS > DNS Server Binding の順に選択	Content Engine の DNS サーババインディングの設定 (p.8-83)
dns use-original-server { only after-configured before-configured }	Devices > Devices ¹ > Applications > DNS > DNS Caching Server の順に選択	Content Engine の DNS キャッシングサーバの設定 (p.8-80)
dns pin { forward <i>hostname ipaddress</i> reverse <i>hostname ipaddress</i> both <i>hostname ipaddress</i> cname <i>records</i> }	Devices > Device Groups > Request Routing > DNS > A-Record Mapping の順に選択	Content Engine の DNS アドレスレコードのマッピングの設定 (p.8-84)
	Devices > Device Groups > Request Routing > DNS > CNAME Record Mapping	Content Engine の DNS 正規名レコードのマッピング設定 (p.8-86)
dns retry-period <i>seconds</i>	Devices > Devices ¹ > Applications > DNS > DNS Caching Server の順に選択	Content Engine の DNS キャッシングサーバの設定 (p.8-80)
dns retry-timeout <i>seconds</i>		
dns serial-lookup	Devices > Device Groups > General Settings > Services > DNS の順に選択	HTTP プロキシキャッシングの DNS サーバの設定 (p.8-87)
	Devices > Devices ¹ > Applications > DNS > DNS Caching Server の順に選択	Content Engine の DNS キャッシングサーバの設定 (p.8-80)
exec-timeout <i>minutes</i>	Devices > Device Groups > General Settings > Login Access Control > Exec Timeout の順に選択	Exec Timeout の設定 (p.20-6)
ftp-native access-list { in out } { <i>std_acl_number</i> <i>acl_name</i> }	Devices > Devices > General Settings > Network > IP ACL Feature Usage の順に選択	IP ACL とアプリケーションとの関連付け (p.17-12)
EXEC モード ftp-native custom-message { download { acl-denied <i>url</i> welcome <i>url</i> } reset { acl-denied all welcome } upload <i>host directory filename</i> { welcome acl-denied }}	Devices > Devices > Applications > Web > FTP > FTP Messages > Upload の順に選択	ネイティブ FTP カスタムメッセージの設定 (p.8-69)
	Devices > Device Groups > Applications > Web > FTP > FTP Messages > Download の順に選択	

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
<code>ftp-native object max-size <i>kilobytes</i></code>	Devices > Device Groups > Applications > Web > FTP > Native FTP Cache Freshness の順に選択	ネイティブ FTP キャッシュのフレッシュネス設定 (p.8-67)
<code>ftp-native proxy active-mode enable</code>	Devices > Device Groups > Applications > Web > FTP > Native FTP Connections の順に選択	ネイティブ FTP 接続の設定 (p.8-65)
<code>ftp-native proxy authentication enable</code>		
<code>ftp-native proxy incoming <i>portnum</i></code>		
<code>ftp-over-http age-multiplier directory-listing <i>dl_time</i> file <i>fo_time</i></code>	Devices > Device Groups > Applications > Web > FTP > FTP Over HTTP Cache Freshness の順に選択	FTP-over-HTTP キャッシュフレッシュネスの設定 (p.8-61)
<code>ftp-over-http max-ttl {days directory-listing <i>dlmax_days</i> file <i>fmax_days</i> hours directory-listing <i>dlmax_hours</i> file <i>fmax_hours</i> minutes directory-listing <i>dlmax_min</i> file <i>fmax_min</i> seconds directory-listing <i>dlmax_sec</i> file <i>fmax_sec</i>}</code>		
<code>ftp-over-http min-ttl <i>min_minutes</i></code>		
<code>ftp-over-http object max-size <i>size</i></code>		
<code>ftp-over-http proxy incoming <i>ports</i></code>		
<code>ftp-over-http proxy outgoing origin-server</code>	Devices > Device Groups > Applications > Web > FTP > FTP Over HTTP Connections の順に選択	FTP-over-HTTP 接続の設定 (p.8-57)
<code>ftp-over-http proxy outgoing connection-timeout</code>		
<code>ftp-over-http proxy outgoing monitor</code>		
<code>ftp-over-http proxy outgoing host {<i>hostname</i> <i>ipaddress</i>} <i>port</i></code>		
<code>ftp-over-http proxy anonymous-pswd <i>passwd</i></code>		
<code>ftp-over-http proxy active-mode enable</code>		
<code>ftp-over-http reval-each-request {all none directory-listing}</code>	Devices > Device Groups > Applications > Web > FTP > FTP Over HTTP Cache Freshness の順に選択	FTP-over-HTTP キャッシュフレッシュネスの設定 (p.8-61)
<code>gui-server enable</code>	Devices > Device Groups > General Settings > Login Access Control > GUI Server の順に選択	セキュアなアクセスまたはセキュアではないアクセスに対する Content Engine GUI の設定 (p.16-64)
<code>gui-server secure enable</code>		
<code>gui-server port <i>port_num</i></code>		
<code>gui-server secure port <i>port_num</i></code>		
<code>hostname <i>name</i></code>	Devices > Devices > Device Activation の順に選択	Content Engine のプロパティの変更 (p.13-10)
<code>http add-method <i>method</i></code>	Devices > Device Groups > Applications > Web > HTTP > HTTP Method の順に選択	Content Engine へのその他の HTTP 要求方式の追加または変更 (p.8-26)
<code>http age-multiplier text <i>num</i> binary <i>num</i></code>	Devices > Device Groups > Applications > Web > HTTP > HTTP Cache Freshness の順に選択	HTTP キャッシュフレッシュネスの設定 (p.8-12)
<code>http always-resolve-host</code>	Devices > Device Groups > Applications > Web > HTTP > HTTP Caching の順に選択	HTTP キャッシュの設定 (p.8-7)
<code>http anonymizer enable</code>		

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
<code>http append via-header</code>	Devices > Device Groups > Applications > Web > HTTP > Authenticated HTTP Caching の順に選択	認証済み HTTP キャッシュの設定 (p.8-16)
<code>http append host-header</code>		
<code>http append x-forwarded-for-header</code>		
<code>http append x-forwarded-for-header multiple-ip-address</code>		
<code>http append proxy-auth-header {ipaddress hostname}</code>		
<code>http append www-auth-header {hostname ipaddress}</code>		
<code>http authenticate-strip-ntlm</code>	Devices > Device Groups > Applications > Web > HTTP > Authenticated HTTP Caching の順に選択	認証済み HTTP キャッシュの設定 (p.8-16)
<code>http authentication cache timeout minutes</code>		
<code>http authentication cache max-entries entries</code>		
<code>http authentication header {401 407}</code>		
<code>http authentication realm line</code>		
<code>http cache-authenticated basic</code>		
<code>http cache-authenticated ntlm</code>	Devices > Device Groups > Applications > Web > HTTP > HTTP Caching の順に選択	HTTP キャッシュの設定 (p.8-7)
<code>http cache-authenticated all</code>		
<code>http cache-cookies</code>		
<code>http cache-on-abort enable</code>		
<code>http cache-on-abort max-threshold max_thresh</code>		
<code>http cache-on-abort min-threshold min_thresh</code>		
<code>http cache-on-abort percent percentthresh</code>	Devices > Device Groups > Applications > Web > HTTP > Advanced HTTP Caching の順に選択	拡張 HTTP キャッシュの設定 (p.8-22)
<code>http cache-vary-user-agent sub-string string</code>		
<code>http cache-vary-user-agent cache-string string</code>		
<code>http cache-vary-user-agent enable</code>		
<code>http client-no-cache-request {ignore revalidate}</code>		
<code>http cluster max-delay seconds</code>		
<code>http cluster misses num</code>	Devices > Device Groups > Applications > Web > HTTP > Advanced HTTP Caching の順に選択	拡張 HTTP キャッシュの設定 (p.8-22)
<code>http cluster http-port num</code>		
<code>http cluster heal-port num</code>		
<code>http destination-port {allow deny}</code>		
<code>http dns-cache size max-num</code>	Devices > Device Groups > Request Routing > DNS Caching > DNS Caching Server の順に選択	Content Engine の DNS キャッシングサーバの設定 (p.8-80)
<code>http dns-cache serial-lookup</code>		
<code>http fast-response enable</code>	Devices > Device Groups > Applications > Web > HTTP > HTTP Caching の順に選択	HTTP キャッシュの設定 (p.8-7)
<code>http l4-switch {enable spoof-client-ip enable}</code>		

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
http max-ttl { <i>days text textdays binary bindays</i> <i>hours text texthours binary binhours</i> <i>minutes text textminutes binary binminutes</i> <i>seconds text textseconds binary binseconds</i> }	Devices > Device Groups > Applications > Web > HTTP > HTTP Cache Freshness の順に選択	HTTP キャッシュ フレッシュネスの設定 (p.8-12)
http min-ttl <i>minutes</i>		
http monitor url { <i>url</i> { <i>interval seconds</i> <i>acceptable-delay seconds</i> }}	Devices > Device Groups > Applications > Web > HTTP > HTTP Monitor URL の順に選択	指定した HTTP URL のモニタリング (p.21-24)
http object max-size <i>kbytes</i>	Devices > Device Groups > Applications > Web > HTTP > HTTP Caching の順に選択	HTTP キャッシュの設定 (p.8-7)
http object url-validation enable		
http persistent-connections [<i>all</i> <i>server-only</i> <i>client-only</i>]	Devices > Device Groups > Applications > Web > HTTP > Advanced HTTP Caching の順に選択	拡張 HTTP キャッシュの設定 (p.8-22)
http persistent-connections timeout <i>seconds</i>		
http proxy incoming ports	Devices > Device Groups > Applications > Web > HTTP > HTTP Connections の順に選択	HTTP キャッシュの設定 (p.8-7)
http proxy outgoing { <i>connection-timeout microsecs</i> <i>host</i> { <i>hostname</i> <i>ipaddress</i> } <i>port</i> [<i>primary</i>] <i>monitor seconds</i> <i>origin-server</i> <i>preserve-407</i> }		
http request-header host unmodified	Devices > Device Groups > Applications > Web > HTTP > HTTP Caching の順に選択	HTTP キャッシュの設定 (p.8-7)
http reval-each-request all	Devices > Device Groups > Applications > Web > HTTP > HTTP Cache Freshness の順に選択	HTTP キャッシュ フレッシュネスの設定 (p.8-12)
http reval-each-request none		
http reval-each-request text		
http serve-ims text percentage binary percentage		
http smart-range enable	Devices > Device Groups > Applications > Web > HTTP > HTTP Caching の順に選択	HTTP キャッシュの設定 (p.8-7)
http smart-range max-start offset max-interval interval		
http strict-request-content-length-checking enable		
http tcp-keepalive enable	Devices > Device Groups > Applications > Web > HTTP > Advanced HTTP Caching の順に選択	拡張 HTTP キャッシュの設定 (p.8-22)
https proxy incoming ports	Devices > Device Groups > Applications > Web > HTTPS > HTTPS Proxy の順に選択	HTTPS プロキシの設定 (p.8-41)
https proxy outgoing host { <i>ipaddress</i> <i>hostname</i> } <i>port</i>		
https destination-port { <i>allow</i> <i>deny</i> } { <i>range</i> <i>all</i> }		
https tcp-rw-timeout <i>seconds</i>		
https server name	Devices > Device Groups > Applications > Web > HTTPS > HTTPS Servers の順に選択	HTTPS サーバの設定 (p.8-47)

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
https <i>server name</i> { cert <i>cert_name</i> certgroup { chain <i>chainname</i> serverauth <i>chainname</i> } enable host { <i>hostname</i> <i>ipaddress</i> } key <i>keyname</i> password <i>password</i> protocol-version { ssl2-only ssl23-tls1 ssl3-only tls1-only } serverauth { enable ignore { cert-not-yet-valid domain-name expired-date invalid-ca }} session-cache { size <i>size</i> timeout <i>timeout</i> }}	Devices > Device Groups > Applications > Web > HTTPS > Certificates の順に選択	HTTPS 証明書の設定 (p.8-31)
	Devices > Device Groups > Applications > Web > HTTPS > Certificate Groups の順に選択	HTTPS 証明書グループの設定 (p.8-35)
	Devices > Device Groups > Applications > Web > HTTPS > Keys の順に選択	HTTPS キーの設定 (p.8-38)
icap append-x-headers { x-client-ip x-server-ip }	Devices > Device Groups > Request Processing > ICAP の順に選択	ICAP の設定 (p.16-3)
icap apply { all rules-template }		
icap bypass streaming-media		
icap logging { format standard enable }		
icap rescan-cache IStag-change		
icap service <i>service_id</i>	Devices > Device Groups > Request Processing > ICAP Services の順に選択	ICAP サービスの設定 (p.16-6)
ICAP サービス コンフィギュレーション モード (config-icap-service)# icap service <i>service_id</i> [enable vector-point { reqmod-precache reqmod-postcache respmode-precache } error-handling { bypass return-error } load-balancing { round-robin client-ip-hash server-ip-hash weighted-load }]		
ICAP サービス コンフィギュレーション モード (config-icap-service)# icap service server <i>server_url</i> { max-connections <i>num</i> weight <i>num</i> }	Devices > Device Groups > Request Processing > ICAP Services の順に選択	ICAP サービス用の ICAP サーバの設定 (p.16-10)
icp client add-remote-server { <i>hostname</i> <i>ipaddress</i> } { parent sibling } icp-port <i>icpport</i> http-port <i>httpport</i> [restrict <i>domainnames</i>]	Devices > Device Groups > Applications > Web > HTTP > ICP > Remote Servers の順に選択	ICP リモートサーバの設定 (p.8-94)
icp client enable	Devices > Device Groups > Applications > Web > HTTP > ICP > Client の順に選択	ICP クライアントの設定 (p.8-90)
icp client exclude <i>domainnames</i>		
icp client max-fail <i>retries</i>		
icp client max-wait <i>timeout</i>		
icp client modify-remote-server { <i>hostname</i> <i>ipaddress</i> } { http-port <i>port</i> icp-port <i>port</i> parent restrict <i>domainnames</i> sibling }	Devices > Device Groups > Applications > Web > HTTP > ICP > ICP Remote Servers の順に選択	ICP リモートサーバの設定 (p.8-94)
icp server enable	Devices > Device Groups > Applications > Web > HTTP > ICP > Server の順に選択	ICP サーバの設定 (p.8-93)
icp server http-port <i>httpport</i>		
icp server port <i>icpport</i>		
icp server remote-client { <i>hostname</i> <i>ipaddress</i> } { fetch no-fetch }	Devices > Device Groups > Applications > Web > HTTP > ICP > Remote Clients の順に選択	ICP リモートクライアントの設定 (p.8-92)

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
<code>inetd enable ftp</code>	Devices > Device Groups > Applications > Web > FTP > Inetd FTP の順に選択	Inetd FTP サービスのイネーブル化 (p.8-68)
<code>inetd enable tftp</code>	Devices > Device Groups > Applications > Web > TFTP > TFTP General Settings の順に選択	TFTP の一般設定 (p.8-73)
<code>inetd enable rep</code>	Devices > Device Groups > General Settings > Network > Inetd RCP の順に選択	Content Engine 上での RCP サービスのイネーブル化 (p.20-10)
<code>interface {FastEthernet GigabitEthernet} slot/port cdp enable</code>	Devices > Devices ¹ > General Settings > Network > Network Interfaces の順に選択	ファストイーサネットまたはギガビットイーサネットの設定の変更 (p.14-9)
<code>interface {FastEthernet GigabitEthernet} slot/port shutdown</code>		
<code>interface {FastEthernet GigabitEthernet} slot/port autosense</code>		
<code>interface {FastEthernet GigabitEthernet} slot/port bandwidth {10 100 1000}</code>		
<code>interface {FastEthernet GigabitEthernet} slot/port [full-duplex half-duplex]</code>		
<code>interface {FastEthernet GigabitEthernet} slot/port mtu size</code>		
<code>interface {FastEthernet GigabitEthernet} slot/port ip address ipaddress netmask [secondary]</code>		
<code>interface {FastEthernet GigabitEthernet} slot/port standby groupnum ip ipaddress netmask</code>	Devices > Devices ¹ > General Settings > Network > Network Interfaces の順に選択	
<code>interface {FastEthernet GigabitEthernet} slot/port standby groupnum errors num</code>		
<code>interface {FastEthernet GigabitEthernet} slot/port standby groupnum priority priority</code>	Devices > Devices ¹ > General Settings > Network > Network Interfaces の順に選択	インターフェイス優先順位の設定 (p.14-5)
<code>interface {FastEthernet GigabitEthernet} slot/port ip address dhcp {client-id id hostname name hostname name client-id id}</code>		DHCP 用のインターフェイスの設定 (p.14-17)
<code>interface FibreChannel slot/port [mode {autosense direct-attached switched} speed {1 2 autosense}]</code>		ファイバチャネルインターフェイスの設定 (p.14-12)
<code>interface PortChannel {1 2} [ip address ipaddress netmask shutdown]</code>	Devices > Devices ¹ > General Settings > Network > Network Interfaces の順に選択	EtherChannel の設定 (p.14-14)
<code>interface {FastEthernet GigabitEthernet} slot/port ip access-group {accesslistnumber accesslistname} {in out}</code>	Devices > Devices ¹ > General Settings > Network > Network Interfaces の順に選択	インターフェイスへの IP ACL の適用 (p.17-13)
<code>ip access-list {standard extended} {acl_name acl_num}</code>	Devices > Devices ¹ > General Settings > Network > IP ACL の順に選択	IP ACL の作成または変更 (p.17-3)
標準 IP ACL および 拡張 IP ACL 用の他のコンフィギュレーション コマンドを含みます。		

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
<p>拡張 ACL コンフィギュレーション モード (config-ext-nacl)#</p> <p>[insert line_num] {deny permit} {gre ip proto_num} {source_ip [wildcard] host source_ip any} {dest_ip [wildcard] host dest_ip any}</p> <p>[insert line_num] {deny permit} tcp {source_ip [wildcard] host source_ip any} [operator port [port]] {dest_ip [wildcard] host dest_ip any} [operator port [port]] [established]</p> <p>[insert line_num] {deny permit} udp {source_ip [wildcard] host source_ip any} [operator port [port]] {dest_ip [wildcard] host dest_ip any} [operator port [port]]</p> <p>[insert line_num] {deny permit} icmp {source_ip [wildcard] host source_ip any} {dest_ip [wildcard] host dest_ip any} [icmp_type [code] icmp_msg]</p> <p>delete line_num list [start_line_num [end_line_num]] move oldline_num newline_num exit</p>	<p>Devices > Devices¹ > General Settings > Network > IP ACL の順に 選択</p>	<p>IP ACL への条件の追加 (p.17-4)</p>
<p>標準 ACL コンフィギュレーション モード (config-std-nacl)#</p> <p>[insert line_num] {deny permit} {source_ip [wildcard] host source_ip any}</p> <p>delete line_num list [start_line_num [end_line_num]] move oldline_num newline_num exit</p>	<p>Devices > Devices¹ > General Settings > Network > IP ACL の順に 選択</p>	<p>IP ACL への条件の追加 (p.17-4)</p>
<p>ip default-gateway ipaddress</p>	<p>Devices > Devices¹ > General Settings > Network > Network Interfaces の順に選択</p>	<p>Content Distribution Manager GUI を使用したスタンバイ インターフェイスの設定 (p.14-4) ファストイーサネットまたはギガビットイーサネットの設定の変更 (p.14-9)</p>
<p>ip domain-name name1 name2 name3</p> <p>ip name-server ipaddress</p>	<p>Devices > Device Groups > General Settings > Network > DNS の順に 選択</p>	<p>HTTP プロキシキャッシングの DNS サーバの設定 (p.8-87)</p>
<p>ip dscp {client {cache-hit {match-server set-dscp dscp-packets set-tos tos-packets} cache-miss {match-server set-dscp dscp-packets set-tos tos-packets}} server {match-client set-dscp dscp-packets set-tos tos-packets}}</p> <p>ip path-mtu-discovery enable</p>	<p>Devices > Device Groups > General Settings > Network > IP General Settings の順に選択</p>	<p>IP ディファレンシエーテッド サービスの設定 (p.10-10)</p>
<p>ip route dest_addr netmask gateway_addr</p>	<p>Devices > Devices¹ > General Settings > Network > IP Routes の順 に選択</p>	<p>スタティック IP ルートの設定 (p.14-19)</p>

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
<code>kernal kdb</code>	Devices > Device Groups > General Settings > Troubleshooting > Kernal Debugger の順に選択	カーネル デバッガのイネーブル化 (p.21-27)
<code>ldap server administrative-dn name</code>	Devices > Device Groups > General Settings > Authentication > LDAP Server の順に選択	LDAP サーバの設定 (p.15-18)
<code>ldap server administrative-passwd passwd</code>		
<code>ldap server allow-mode</code>		
<code>ldap server base baseword</code>		
<code>ldap server enable</code>	Devices > Device Groups > General Settings > Authentication > Authentication Scheme の順に選択	要求認証の認証方式の設定 (p.15-38)
<code>ldap server filter filterword</code>	Devices > Device Groups > General Settings > Authentication > LDAP Server の順に選択	LDAP サーバの設定 (p.15-18)
<code>ldap server group active-directory enable</code>		
<code>ldap server group {organizationUnit enable custom name enable static {group-attribute name member-attribute {member uniquemember custom-member name} enable nested {enable level number}}}</code>	Devices > Device Groups > General Settings > Authentication > LDAP Server の順に選択	LDAP サーバの設定 (p.15-18)
<code>ldap server host {hostipaddress hostname} [primary secondary]</code>		
<code>ldap server password-expiry {enable redirect-url url}</code>		
<code>ldap server policy-redirect {enable redirect-url url attribute name version-number number}</code>		
<code>ldap server policy-redirect append-request-url</code>		
<code>ldap server port port_num</code>		
<code>ldap server retransmit retries</code>		
<code>ldap server timeout seconds</code>		
<code>ldap server userid-attribute useridword</code>		
<code>ldap server version ver_num</code>		
<code>line console carrier-detect</code>	Devices > Device Groups > General Settings > Login Access Control > Console Carrier Detect の順に選択	ライン コンソール キャリア検知の設定 (p.20-7)

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
logging host {ipaddress hostname}	Devices > Device Groups > General Settings > Notification and Tracking > System Logs の順に選択	Content Distribution Manager GUI を使用したシステム イベント ロギングの設定 (p.21-7)
logging host priority {alert critical debug emergency error information notice warning}		
logging disk enable		
logging disk filename filename		
logging disk recycle size		
logging disk priority {alert critical debug emergency error information notice warning}		
logging console enable		
logging console priority {alert critical debug emergency error information notice warning}		
logging facility {auth daemon kernel local0 local1 local2 local3 local4 local5 local6 local7 mail news syslog user uucp}		
multicast license-key key	Devices > Device Groups > Prepositioning > Multicast Distribution License の順に選択	Content Engine でのマルチキャストのイネーブル化 (p.5-36)
multicast accept-license-agreement multicast enable		
multicast evaluate		
network-filesystem server {samba cifs} {enable authentication-mode {public ce-user cifs-user password-server} max-connections num}	Devices > Device Groups > General Settings > File Sharing > CIFS Server の順に選択	CIFS サーバの設定 (p.13-18)
network-filesystem server {samba cifs} {share-web-site site_name [share-auth-content protect-auth-content]}	Devices > Device Groups > General Settings > File Sharing > CIFS Server Access Control の順に選択	CIFS サーバ Web サイト アクセス制御の設定 (p.13-20)
network-filesystem client {cifs {hostname ipaddress} directory {cdnfs mediafs} reserved-disk-space space username name password password [domain domain] nfs {hostname ipaddress} directory {cdnfs mediafs} reserved-disk-space space}	Devices > Devices ¹ > General Settings > Storage > ネットワーク アクセス サーバ の順に選択	『Cisco ACNS Software Update and Maintenance Guide』 Release 5.x の「Attaching and Detaching NAS Shares Using the Content Distribution Manager GUI」を参照
ntlm server ad-group-search {enable enum-user gc-server groupname-attribute ldap-referral ldap-search-port membership-attribute user-objectclass username-attribute}	Devices > Device Groups > General Settings > Authentication > NTLM Server の順に選択	NTLM サーバの設定 (p.15-24)
ntlm server ad-group-search mem-cache {enable size kilobytes max-ttl minutes}	Devices > Device Groups > General Settings > Authentication > NTLM Server の順に選択	NTLM サーバの LDAP メモリ キャッシュの設定 (p.15-29)
ntlm allow-domain {enable domain domainname}	Devices > Device Groups > General Settings > Authentication > NTLM Allow Domain の順に選択	HTTP 要求認証の NTLM 許可ドメインの設定 (p.15-32)
ntlm server enable	Devices > Device Groups > General Settings > Authentication > Authentication Scheme の順に選択	要求認証の認証方式の設定 (p.15-38)
ntlm server host {hostname ipaddress}	Devices > Device Groups > General Settings > Authentication > NTLM Server の順に選択	NTLM サーバの設定 (p.15-24)
ntlm server domain name		

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
<code>ntp server {hostname ipaddress}</code>	Devices > Device Groups > General Settings > Network > NTP の順に選択	NTP の設定 (p.20-13)
<code>offline-operation enable</code>	Devices > Device Groups > Applications > Web > Offline Operations の順に選択	ネットワーク デバイスのオフライン動作のイネーブル化 (p.20-32)
<code>port-channel load-balance {dst-ip dst-mac round-robin}</code>	Devices > Devices ¹ > General Settings > Network > Network Interfaces の順に選択	EtherChannel の設定 (p.14-14)
<code>proxy-auto-config enable</code>	Devices > Device Groups > Applications > Web > Client Proxy Autoconfiguration の順に選択	クライアント プロキシ自動設定の設定 (p.4-43)
<code>proxy-protocols outgoing-proxy exclude {enable list word}</code>	Devices > Device Groups > Applications > Web > Outgoing Proxy Exclusions の順に選択	HTTP と HTTPS 発信プロキシの除外の設定 (p.8-53)
<code>proxy-protocols transparent {default-server original-proxy reset}</code>		
<code>qos camiant-cdn-am-service config-file filename</code> または URL	Devices > Device Groups > Request Processing > PCMM > QoS Policy Service の順に選択	Content Engine 用 QoS ポリシーサーバの設定 (p.16-68)
<code>qos camiant-cdn-am-service enable</code>		
<code>radius-server key key</code>	Devices > Device Groups > General Settings > Authentication > RADIUS Server の順に選択	RADIUS サーバの設定 (p.15-33)
<code>radius-server timeout seconds</code>		
<code>radius-server enable</code>	Devices > Device Groups > General Settings > Authentication > Authentication Scheme の順に選択	要求認証の認証方式の設定 (p.15-38)
<code>radius-server host {hostname ipaddress} {auth-port port}</code>	Devices > Device Groups > General Settings > Authentication > RADIUS Server の順に選択	RADIUS サーバの設定 (p.15-33)
<code>radius-server retransmit retries</code>		
<code>radius-server redirect enable</code>		
<code>radius-server redirect message reply location url</code>		
<code>rtsp advanced max-initial-setup-delay seconds</code>	Devices > Device Groups > Applications > Streaming > RTSP Gateway の順に選択	RTSP ゲートウェイの設定 (p.9-10)
<code>rtsp advanced max-request-rate number</code>		
<code>rtsp proxy media-real enable</code>	Devices > Device Groups > Applications > Streaming > Real Networks > Real Proxy License の順に選択	RealProxy のイネーブル化 (p.9-12)
<code>rtsp proxy media-real evaluate</code>		
<code>rtsp proxy media-real license-key key</code>		
<code>rtsp proxy media-real accept-license-agreement</code>		
<code>rtsp server real-subscriber license-key key</code>	Devices > Device Groups > Applications > Streaming > Real Networks > Real Subscriber License の順に選択	RealSubscriber のイネーブル化 (p.9-14)
<code>rtsp server real-subscriber accept-license-agreement</code>		
<code>rtsp server real-subscriber evaluate</code>		
<code>rtsp server real-subscriber enable</code>		
<code>rtsp l4-switch enable</code>	Devices > Device Groups > Applications > Streaming > RTSP Gateway の順に選択	RTSP ゲートウェイの設定 (p.9-10)
<code>rtsp port incoming port_num</code>		
<code>rtsp ip-address ipaddress</code>		

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
rtsp server cisco-streaming-engine enable	Devices > Device Groups > Applications > Streaming > Cisco Streaming Engine の順に選択	Cisco Streaming Engine のイネーブル化 (p.9-17)
rtsp server cisco-streaming-engine broadcast port-list <i>list_num port_num</i>	Services > Video > Programs > Live Streaming (indirect support) の順に選択	Cisco Streaming Engine ライブプログラムのライブストリームの設定 (p.7-23)
rtsp server cisco-streaming-engine broadcast id <i>id</i> source { source-rtsp <i>rtsp_url</i> source-udp <i>url srce_ip_addr recv_ip_addr recv_port_list_num</i> } { track-count <i>1-4</i> } destination { destination-pull destination-udp <i>ttl dest_ip_addr dest_list_num</i> }		
rule enable	Devices > Device Groups > Request Processing > Enable Rules の順に選択	ルール設定のイネーブル化 (p.16-13)
rule action rule action allow pattern-list <i>list_num</i> [protocol { all http https rtsp }] rule action append-username-header pattern-list <i>list_num</i> [protocol { all http https rtsp }] rule action block pattern-list <i>list_num</i> [protocol { all http https rtsp }] rule action cache-non-cacheable ttl { day <i>days</i> pattern-list <i>list_num</i> [protocol { all http https }]} hours <i>hours</i> pattern-list <i>list_num</i> [protocol { all http https }]} minutes <i>minutes</i> pattern-list <i>list_num</i> [protocol { all http https }]} seconds <i>seconds</i> pattern-list <i>list_num</i> [protocol { all http https }]}	Devices > Device Groups > Request Processing > Service Rules の順に選択	サービス ルールの設定 (p.16-13)
rule action cache-only pattern-list <i>list_num</i> [protocol { all http https }] rule action dscp client cache-hit { match-server pattern-list <i>list_num</i> [protocol { all http https }]} set-dscp <i>dscpvalue</i> set-tos <i>tosvalue</i> } rule action dscp client cache-miss { match-server pattern-list <i>list_num</i> [protocol { all http https }]} set-dscp <i>dscpvalue</i> set-tos <i>tosvalue</i> } rule action dscp server { match-client pattern-list <i>list_num</i> [protocol { all http https }]} set-dscp <i>dscpvalue</i> set-tos <i>tosvalue</i> }	Devices > Device Groups > Request Processing > Service Rules の順に選択	サービス ルールの設定 (p.16-13)

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
rule action freshness-factor <i>exp_time</i> pattern-list <i>list_num</i> [protocol { all http https }] rule action generate-url-signature [include-client-src-ip] key-id-owner <i>owner_num</i> key-id-number <i>id_num</i> pattern-list <i>list_num</i> [protocol { all http }] rule action insert-no-cache pattern-list <i>list_num</i> [protocol { all http https }] rule action no-auth pattern-list <i>list_num</i> [protocol { all http https rtsp }] rule action no-cache pattern-list <i>list_num</i> [protocol { all http https }] rule action no-persistent-connection { all client server } pattern-list <i>list_num</i> [protocol { all http https }]	Devices > Device Groups > Request Processing > Service Rules の順に選択	サービス ルールの設定 (p.16-13)
rule action no-proxy pattern-list <i>list_num</i> [protocol { all http https }] rule action redirect <i>url</i> pattern-list <i>list_num</i> [protocol { all http https rtsp }] rule action redirect-url-for-cdn pattern-list <i>list_num</i> [protocol { all http https rtsp }] rule action refresh pattern-list <i>list_num</i> [protocol { all http https }] rule action reset pattern-list <i>list_num</i> [protocol { all http https rtsp }] rule action rewrite pattern-list <i>list_num</i> [protocol { all http https rtsp }]	Devices > Device Groups > Request Processing > Service Rules の順に選択	サービス ルールの設定 (p.16-13)

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
rule action use-dns-server {hostname ipaddress} pattern-list list_num [protocol {all http https}] rule action use-icap-service service_name pattern-list list_num [protocol {all http https}] rule action use-proxy {hostname ipaddress} port pattern-list list_num [protocol {all http https}] rule action use-proxy {hostname ipaddress} port [failover] pattern-list list_num [protocol {all http https}] rule action use-server {hostname ipaddress} port pattern-list list_num [protocol {all http https}] rule action use-xforward-clt-ip pattern-list list_num [protocol {all http https}] rule action validate-url-signature error-redirect-url url pattern-list list_num [protocol {all http rtsp}]	Devices > Device Groups > Request Processing > Service Rules の順に選択	サービス ルールの設定 (p.16-13)
rule pattern-list list_num domain dn_regexp rule pattern-list list_num dst-ip d_ipaddress d_subnet rule pattern-list list_num dst-port port rule pattern-list list_num groupname name rule pattern-list list_num groupname-regex group_name_regexp rule pattern-list list_num group-type {and or} rule pattern-list list_num header-field {referer ref_regexp request-line req_regexp user-agent ua_regexp} rule pattern-list list_num header-field x-forwarded-for ipaddress rule pattern-list list_num header-field-sub {referer ref_regexp ref_sub request-line req_regexp req_sub user-agent ua_regexp ua_sub}	Devices > Device Groups > Request Processing > Service Rules の順に選択	サービス ルールの設定 (p.16-13)
rule pattern-list list_num icap-attribute icap_attribute icap_value rule pattern-list list_num mime-type mt_regexp rule pattern-list list_num src-ip s_ipaddress s_subnet rule pattern-list list_num url-regex url_regexp rule pattern-list list_num url-regex url_regexp url_sub rule pattern-list list_num username user_name	Devices > Device Groups > Request Processing > Service Rules の順に選択	サービス ルールの設定 (p.16-13)

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
<code>snmp-server contact line</code>	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > General Settings の順に選択	SNMP トラップの設定 (p.22-3)
<code>snmp-server enable traps [config content-engine [disk-fail disk-read disk-write overload-bypass transaction-log] entity event snmp [authentication cold-start]]</code>		
<code>snmp-server host {hostname ipaddress} communitystring [v2c [retry num] [timeout seconds]] [v3 {auth [retry num] [timeout seconds] noauth [retry num] [timeout seconds] priv [retry num] [timeout seconds]}]</code>	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > Host の順に選択	SNMP ホストの設定 (p.22-12)
<code>snmp-server location line</code>	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > General Settings の順に選択	SNMP トラップの設定 (p.22-3)
<code>snmp-server user name group [auth {md5 password [priv password] sha password [priv password]} remote octetstring [auth {md5 password [priv password] sha password [priv password]}]]</code>	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > User の順に選択	SNMP ユーザの設定 (p.22-9)
<code>snmp-server group name {v1 [notify name] [read name] [write name] v2c [notify name] [read name] [write name] v3 {auth [notify name] [read name] [write name] noauth [notify name] [read name] [write name] priv [notify name] [read name] [write name]}}</code>	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > Group の順に選択	SNMP グループの設定 (p.22-8)
<code>snmp-server community string [group groupname rw]</code>	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > Community の順に選択	SNMP コミュニティの設定 (p.22-6)
<code>snmp-server view viewname MIBfamily {excluded included}</code>	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > View の順に選択	SNMPv2 ビューの設定 (p.22-11)
<code>snmp-server notify inform</code>	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > General Settings の順に選択	SNMP トラップの設定 (p.22-3)
<code>snmp-server mib persist event</code>		
<code>snmp-server access-list {std_acl_number acl_name}</code>	Devices > Devices ¹ > General Settings > Network > IP ACL Feature Usage の順に選択	IP ACL とアプリケーションとの関連付け (p.17-12)
<code>sshd enable</code>	Devices > Device Groups > General Settings > Network > SSH の順に選択	SSH の設定 (p.20-2)
<code>sshd timeout seconds</code>		
<code>sshd password-guesses num</code>		
<code>ssh-key-generate key-length length</code>		

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
tacacs enable	Devices > Device Groups > General Settings > Authentication > TACACS+ Server の順に選択	TACACS+ サーバの設定 (p.15-35)
tacacs password ascii		
tacacs timeout		
tacacs retransmit		
tacacs key		
tacacs host {ipaddress hostname} [primary]		
tcp ecn enable	Devices > Device Groups > General Settings > Network > TCP の順に選択	キャッシュ パフォーマンスを向上させる TCP の設定 (p.10-2)
tcp type-of-service enable		
tcp cwnd-base segments		
tcp increase-xmit-timer-value value		
tcp init-ss-threshold value		
tcp keepalive-probe-cnt count		
tcp keepalive-probe-interval seconds		
tcp keepalive-timeout seconds		
tcp client-satellite		
tcp client-mss max_seg_size		
tcp client-receive-buffer kbytes		
tcp client-rw-timeout seconds		
tcp client-send-buffer kbytes		
tcp server-satellite		
tcp server-mss max_seg_size		
tcp server-receive-buffer kbytes		
tcp server-rw-timeout seconds		
tcp server-send-buffer kbytes		
telnet enable	Devices > Device Groups > General Settings > Network > Telnet の順に選択	Content Engine 上での Telnet サービスのイネーブル化 (p.20-2)
tftp max-connections number	Devices > Device Groups > Applications > Web > TFTP > TFTP General Settings の順に選択	TFTP の一般設定 (p.8-73)
tftp-server dir directory	Devices > Device Groups > Applications > Web > TFTP > TFTP Directory の順に選択	TFTP ディレクトリの設定 (p.8-77)
tftp-server access-list {std_acl_number acl_name}	Devices > Devices ¹ > General Settings > Network > IP ACL Feature Usage の順に選択	IP ACL とアプリケーションとの関連付け (p.17-12)
tftp-server gw proto ftp server {hostname ipaddress} pri priority [name name passwd password] [path directory]	Devices > Device Groups > Applications > Web > TFTP > TFTP Proxy の順に選択	TFTP プロキシ サーバの設定 (p.8-74)
tftp-server gw proto http server {hostname ipaddress} [port port_num] pri priority [name name passwd password] [path directory]		

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
<code>transaction-logs archive max-file-size kbytes</code>	Devices > Device Groups > General Settings > Notification and Tracking > Transaction Logs の順に選択	Content Distribution Manager GUI によるトランザクション ロギングのイネーブル化 (p.19-12)
<code>transaction-logs archive interval {seconds every-week [on weekdays at hour:minute] every-day {at hour:minute every hours} every-hour {at minute every minutes} }</code>		
<code>transaction-logs enable</code>		
<code>transaction-logs export enable</code>		
<code>transaction-logs export ftp-server {hostname ipaddress} login password directory</code>		
<code>transaction-logs export sftp-server {hostname ipaddress} login password directory</code>		
<code>transaction-logs export compress</code>	Devices > Device Groups > General Settings > Notification and Tracking > Transaction Logs の順に選択	Content Distribution Manager GUI によるトランザクション ロギングのイネーブル化 (p.19-12)
<code>transaction-logs export interval {minutes every-week [on weekdays at hour:minute] every-day {at hour:minute every hours} every-hour {at minute every minutes} }</code>		
<code>transaction-logs file-marker</code>		
<code>transaction-logs sanitize</code>		
<code>transaction-logs log-windows-domain</code>		
<code>transaction-logs format {squid extended-squid apache custom string}</code>		
<code>tvout signal {ntsc pal}</code>	Devices > Device Groups > Applications > Set Top Box > TV-out の順に選択	TV-Out 機能のイネーブル化 (p.7-36)
<code>tvout enable</code>		
<code>url-filter http {bad-sites-deny good-sites-allow} {enable file filename}</code>	Devices > Device Groups > Request Processing > URL Filter > HTTP > URL Filter Settings for HTTP Protocol の順に選択	Content Distribution Manager GUI を使用した URL フィルタリングの設定 (p.16-25)
<code>url-filter http websense allowmode enable</code>		
<code>url-filter http websense enable</code>		
<code>url-filter http websense server {ipaddress hostname} port 1-65535 timeout seconds connections 1-250</code>		
<code>url-filter http N2H2 allowmode enable</code>		
<code>url-filter http N2H2 enable</code>		
<code>url-filter http N2H2 server {ipaddress hostname} port 1-65535 timeout</code>		
<code>url-filter http smartfilter enable</code>		
<code>url-filter http smartfilter enable</code>		
<code>url-filter http custom-message dirname</code>	Devices > Device Groups > Request Processing > URL Filter の順に選択	Content Distribution Manager GUI を使用した URL フィルタリングの設定 (p.16-25)
		CLI を使用したカスタムブロッキング メッセージの設定 (p.16-30)

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
<code>url-filter wmt {bad-sites-deny good-sites-allow} {enable file filename }</code>	Devices > Device Groups > Request Processing > URL Filter > WMT > URL Filter Settings for WMT Protocol の順に選択	Content Distribution Manager GUI を使用した URL フィルタリングの設定 (p.16-25)
<code>url-filter rtsp {bad-sites-deny good-sites-allow} {enable file filename }</code>	Devices > Device Groups > Request Processing > URL Filter > RTSP > URL Filter Settings for RTSP Protocol の順に選択	
<code>url-signature key-id-owner number key-id-number number key encryption_key</code>	Devices > Device Groups > Request Processing > PCMM > URL Signature Key の順に選択	Content Engine 用新規 URL 署名キーの作成 (p.16-69)
<code>username name {cifs-password password privilege}</code>	Devices > Device Groups > General Settings > Login Access Control > Users > Usernames の順に選択	中央管理デバイスでのユーザーアカウントの作成 (p.12-16)
<code>wccp access-list {std_acl_number ext_acl_number acl_name}</code>	Devices > Devices ¹ > General Settings > Network > IP ACL Feature Usage の順に選択	IP ACL とアプリケーションとの関連付け (p.17-12)
<code>wccp custom-web-cache mask {[dst-ip-mask hex_num] [dst-port-mask port_hex_num] [src-ip-mask hex_num] [src-port-mask port_hex_num]}</code>	Devices > Device Groups > Request Routing > WCCP > Services の順に選択	Content Engine の WCCP サービスマスクの設定 (p.4-20)
<code>wccp custom-web-cache router-list-num num port port [assign-method-strict] [hash-destination-ip] [hash-destination-port] [hash-source-ip] [hash-source-port] [l2-redirect] [mask-assign] [password key] [weight percentage]</code>	Devices > Device Groups > Request Routing > WCCP > Services の順に選択	Content Engine の WCCP のサービス設定 (p.4-10)
<code>wccp dns mask {[dst-ip-mask hex_num] [dst-port-mask port_hex_num] [src-ip-mask hex_num] [src-port-mask port_hex_num]}</code>	Devices > Device Groups > Request Routing > WCCP > Services の順に選択	Content Engine の WCCP サービスマスクの設定 (p.4-20)
<code>wccp dns router-list-num num [hash-destination-ip] [hash-destination-port] [hash-source-ip] [hash-source-port] [l2-redirect] [mask-assign] [password key] [weight percentage]</code>	Devices > Device Groups > Request Routing > WCCP > Services の順に選択	Content Engine の WCCP のサービス設定 (p.4-10)
<code>wccp flow-redirect enable</code>	Devices > Device Groups > Request Routing > WCCP > General Settings の順に選択	Content Engine の WCCP 一般設定 (p.4-7)
<code>wccp ftp router-list-num num [assign-method-strict] [l2-redirect] [mask-assign] [password key] [weight percentage]</code>	Devices > Device Groups > Request Routing > WCCP > Services の順に選択	Content Engine の WCCP のサービス設定 (p.4-10)
<code>wccp ftp mask {[dst-ip-mask hex_num] [src-ip-mask hex_num]}</code>	Devices > Device Groups > Request Routing > WCCP > Services の順に選択	Content Engine の WCCP サービスマスクの設定 (p.4-20)
<code>wccp home-router ipaddress</code>	Devices > Device Groups > Request Routing > WCCP > General Settings の順に選択	Content Engine の WCCP 一般設定 (p.4-7)
<code>wccp https-cache accept-all</code>		

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
wccp https-cache mask {[dst-ip-mask hex_num] [dst-port-mask port_hex_num] [src-ip-mask hex_num] [src-port-mask port_hex_num]}	Devices > Device Groups > Request Routing > WCCP > Services の順に 選択	Content Engine の WCCP サービス マスクの設定 (p.4-20)
wccp https-cache router-list-num num port port [assign-method-strict] [hash-destination-ip] [hash-destination-port] [hash-source-ip] [hash-source-port] [l2-redirect] [mask-assign] [password key] [weight percentage]	Devices > Device Groups > Request Routing > WCCP > Services の順に 選択	Content Engine の WCCP のサー ビス設定 (p.4-10)
wccp port-list list_num port_num	Devices > Device Groups > Request Routing > WCCP > Services の順に 選択	Content Engine の WCCP ポート リストの設定 (p.4-18)
wccp rtsp mask {[dst-ip-mask hex_num] [dst-port-mask port_hex_num] [src-ip-mask hex_num] [src-port-mask port_hex_num]}	Devices > Device Groups > Request Routing > WCCP > Services の順に 選択	Content Engine の WCCP サービス マスクの設定 (p.4-20)
wccp rtsp router-list-num num [hash-destination-ip] [hash-destination-port] [hash-source-ip] [hash-source-port] [l2-redirect] [mask-assign] [password key] [weight percentage]	Devices > Device Groups > Request Routing > WCCP > Services の順に 選択	Content Engine の WCCP のサー ビス設定 (p.4-10)
wccp reverse-proxy mask [dst-ip-mask hex_num] [dst-port-mask port_hex_num] [src-ip-mask hex_num] [src-port-mask port_hex_num]	Devices > Device Groups > Request Routing > WCCP > Services の順に 選択	Content Engine の WCCP サービス マスクの設定 (p.4-20)
wccp reverse-proxy router-list-num num [assign-method-strict] [l2-redirect] [mask-assign] [password key] [weight percentage]	Devices > Device Groups > Request Routing > WCCP > Services の順に 選択	Content Engine の WCCP のサー ビス設定 (p.4-10)
wccp router-list list_num ipaddress	Devices > Device Groups > Request Routing > WCCP > Services の順に 選択	WCCP ルータ リストの作成 (p.4-14)
wccp service-number service_num router-list-num num port-list-num port application {cache streaming} [hash-destination-ip] [hash-destination-port] [hash-source-ip] [hash-source-port] [l2-redirect] [mask-assign] [match-source-port] [password key] [weight percentage]	Devices > Device Groups > Request Routing > WCCP > Services の順に 選択	Content Engine の WCCP のサー ビス設定 (p.4-10)
wccp service-number service_num mask {[dst-ip-mask hex_num] [dst-port-mask port_hex_num] [src-ip-mask hex_num] [src-port-mask port_hex_num]}	Devices > Device Groups > Request Routing > WCCP > Services の順に 選択	Content Engine の WCCP サービス マスクの設定 (p.4-20)
wccp shutdown max-wait seconds	Devices > Device Groups > Request Routing > WCCP > General Settings の順に選択	Content Engine の WCCP 一般設 定 (p.4-7)
wccp slow-start enable		
wccp spoof-client-ip enable		
wccp version {1 2}		
wccp web-cache mask {[dst-ip-mask hex_num] [dst-port-mask port_hex_num] [src-ip-mask hex_num] [src-port-mask port_hex_num]}	Devices > Device Groups > Request Routing > WCCP > Services の順に 選択	Content Engine の WCCP サービス マスクの設定 (p.4-20)

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
wccp web-cache router-list-num <i>num</i> [assign-method-strict] [l2-redirect] [mask-assign] [password <i>key</i>] [weight <i>percentage</i>]	Devices > Device Groups > Request Routing > WCCP > Services の順に選択	Content Engine の WCCP のサービス設定 (p.4-10)
wccp wmt mask {[dst-ip-mask <i>hex_num</i>] [dst-port-mask <i>port_hex_num</i>] [src-ip-mask <i>hex_num</i>] [src-port-mask <i>port_hex_num</i>]}	Devices > Device Groups > Request Routing > WCCP > Services の順に選択	Content Engine の WCCP サービスマスクの設定 (p.4-20)
wccp wmt router-list-num <i>num</i> [assign-method-strict] [hash-destination-ip] [hash-destination-port] [hash-source-ip] [hash-source-port] [l2-redirect] [mask-assign] [password <i>key</i>] [weight <i>percentage</i>]	Devices > Device Groups > Request Routing > WCCP > Services の順に選択	Content Engine の WCCP のサービス設定 (p.4-10)
wccp wmt -rtspu router-list-num <i>num</i> [assign-method-strict] [hash-destination-ip] [hash-destination-port] [hash-source-ip] [hash-source-port] [l2-redirect] [mask-assign] [password <i>key</i>] [weight <i>percentage</i>]		
websense-server enable	Devices > Device Groups > Request Processing > URL Filter > HTTP > URL Filter Settings for HTTP Protocol の順に選択	Content Distribution Manager GUI を使用した URL フィルタリングの設定 (p.16-25)
websense-server service {edir-agent {activate edir-server administrative-passwd <i>password</i> } eim activate logon-agent activate network-agent activate policy {local activate remote host <i>hostname</i> or IP address port <i>portnum</i> } radius-agent activate user activate}	Devices > Device Groups > Request Processing > Websense Server の順に選択	Websense サーバ コンポーネントの Content Engine へのインストール (p.16-53)
wmt accelerate live-split enable	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings の順に選択	Content Engine の Windows Media プロキシの設定 (p.9-20)
wmt accelerate proxy-cache enable		
wmt accelerate vod enable		
wmt accept-license-agreement	Devices > Device Groups > Applications > Streaming > Windows Media > License の順に選択	Windows Media サービスのイネーブル化 (p.9-18)
wmt advanced client idle-timeout <i>seconds</i>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings の順に選択	Content Engine の Windows Media プロキシの設定 (p.9-20)
wmt advanced client max-packet-size <i>bytes</i>		
wmt advanced server log-forwarding enable		
wmt bandwidth incoming bypass-list { <i>ipaddress</i> <i>hostname</i> } [<i>ipaddress</i> <i>hostname</i>]	Devices > Devices ¹ > Applications > Streaming > Windows Media > Bypass List の順に選択	Windows Media 着信帯域幅バイパスリストの設定 (p.9-53)
wmt broadcast {alias-name <i>name</i> source <i>url</i> }	Devices > Device Groups > Applications > Streaming > Windows Media > Broadcast Alias の順に選択	Multicast-In Unicast-Out の設定 (p.9-38) Unicast-in Unicast-out の設定 (p.9-40)

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
<code>wmt cache enable</code>	Devices > Device Groups > Applications > Streaming > Windows Media > License の順に選択	Windows Media サービスのイネーブル化 (p.9-18)
<code>wmt cache max-obj-size <i>mbytes</i></code>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings の順に選択	Content Engine の Windows Media プロキシの設定 (p.9-20)
<code>wmt disallowed-client-protocols {[http rtspt rtspu]}</code>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings の順に選択	Windows Media サービスのイネーブル化 (p.9-18)
<code>wmt enable</code>	Devices > Device Groups > Applications > Streaming > Windows Media > License の順に選択	Windows Media サービスのイネーブル化 (p.9-18)
<code>wmt evaluate</code>	Devices > Device Groups > Applications > Streaming > Windows Media > License の順に選択	Windows Media サービスのイネーブル化 (p.9-18)
<code>wmt extended transaction-log enable</code>	Devices > Device Groups > General Settings > Notification and Tracking > Transaction Logs の順に選択	WMT トランザクション ロギングの使用 (p.19-17)
<code>wmt fast-start enable</code>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings の順に選択	Content Engine の Windows Media プロキシの設定 (p.9-20)
<code>wmt fast-cache max-delivery-rate <i>num</i></code>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings の順に選択	Content Engine の Windows Media プロキシの設定 (p.9-20)
<code>wmt fast-start enable</code>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings の順に選択	Content Engine の Windows Media プロキシの設定 (p.9-20)
<code>wmt fast-start max-bandwidth <i>kbits</i></code>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings の順に選択	Content Engine の Windows Media プロキシの設定 (p.9-20)
<code>wmt http allow extension <i>file_extensions</i></code>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings の順に選択	Content Engine の Windows Media プロキシの設定 (p.9-20)
<code>wmt l4-switch enable</code>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings の順に選択	Content Engine の Windows Media プロキシの設定 (p.9-20)
<code>wmt license-key <i>key</i></code>	Devices > Device Groups > Applications > Streaming > Windows Media > License の順に選択	Windows Media サービスのイネーブル化 (p.9-18)
<code>wmt live-url-stripping enable</code>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings の順に選択	Content Engine の Windows Media プロキシの設定 (p.9-20)
<code>wmt multicast {station-configuration <i>name</i> [{<i>dest_addr dest_port media_source</i>}] [log {local webserverserver <i>webserverserver_url</i>}] [nsc-reference {<i>ref_URL</i>}] [play-forever] [unicast-url <i>url</i>] failover {alternate-source <i>alt_src_url</i> retry-count <i>number</i> retry-interval <i>number</i>} schedule-start {<i>minute hour day month</i> now}} time-to-live <i>ttl</i>}</code>	Devices > Device Groups > Applications > Streaming > Windows Media > Multicast Stations の順に選択	Unicast-in Multicast-out の設定 (p.9-32) Multicast-In Multicast-Out の設定 (p.9-35)
<code>wmt max-concurrent-sessions <i>num</i></code>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings の順に選択	Content Engine の Windows Media プロキシの設定 (p.9-20)
<code>wmt multicast schedule-start <i>name minute hour day month</i></code>	Devices > Device Groups > Applications > Streaming > Windows Media > Multicast Station Schedules の順に選択	Windows Media マルチキャストステーションのスケジュールの設定 (p.9-42)

表 D-1 ACNS ソフトウェア CLI の Content Distribution Manager GUI へのマッピング (続き)

コマンド	GUI ナビゲーションパス	参照先
wmt multicast time-to-live <i>ttl</i>	Devices > Device Groups >	Content Engine の Windows Media プロキシの設定 (p.9-20)
wmt proxy outgoing http host <i>{hostname ipaddress}</i> <i>port</i>	Applications > Streaming > Windows Media> General Settings の順に選択	
wmt proxy outgoing rtsp host <i>{hostname ipaddress}</i> <i>port</i>		
wmt transaction-logs format <i>{extended {wms-41 wms-90} wms-41 wms-90}</i>	Devices > Device Groups > General Settings > Notification and Tracking > Transaction Logs の順に選択	WMT トランザクション ロギングの使用 (p.19-17)

1. このコマンドは、個々のデバイス上でのみ設定できます。デバイス グループ設定の場合、Content Distribution Manager GUI は、このコマンドをサポートしません。

Content Distribution Manager GUI でサポートされていない CLI コマンド

Content Distribution Manager GUI でサポートされていない CLI コマンドは、次のとおりです。

- **auto-register enable** *{FastEthernet number number | GigabitEthernet number number}*
- **bandwidth advanced config-file** *string*
- **cdm ip** *string*
- **cdm** *{role {primary | standby} | ui port number}*
- **cms enable**
- **cms rpc timeout** *{connection number transfer number | incoming-wait number}*
- **content-routing-api enable**
- **device mode**
- **exception** *{debug | coredump}*
- **multicast back-version-compatibility** *acns-5-0*
- **multicast sender-delay** *number*
- **multicast max-concurrent-jobs** *number minimal-target-rate number*
- **multicast priority-weight** *number*
- **multicast fixed-carousel enable**
- **pre-load**
- **rtsp server cisco-streaming-engine broadcast port-list** *number number*
- **rtsp server cisco-streaming-engine broadcast id** *string source {source-rtsp string | source-udp string ipaddress ipaddress number} {track-count number} destination {destination-pull | destination-udp number ipaddress number}*