

Audit Policy Registry Format (<http://www.kazamiya.net/poladtev>)

HKLM\SECURITY\Policy\PolAdtEv

Offset 16進	Size	カテゴリ/サブカテゴリ(説明) (* 00 00: 監査しない, 01 00: 成功, 02 00: 失敗, 03 00: 成功および失敗)		Value
0	2	ヘッダ	不明	00 01
2	2		不明	00 00
4	2		カテゴリ数	n
6	2		不明	
8	2		カテゴリ1のサブセット数へのオフセット	x
A	2		不明	00 00
C	2	カテゴリ 1	サブカテゴリ 1	*
C+2y	2		サブカテゴリ y	*
	2	カテゴリ n	サブカテゴリ 1	*
	2		サブカテゴリ z	*
x-2	2	フッタ	不明	
x	2		カテゴリ1のサブカテゴリ数	y
x+2n	2		カテゴリnのサブカテゴリ数	z

rev. 4 (2017/01/29)

Offset 10進	Offset 16進	カテゴリ/サブカテゴリ(説明) (00 00: 監査しない, 01 00: 成功, 02 00: 失敗, 03 00: 成功および失敗)		Default (Vista)	Default (2008 x86)
0	0	ヘッダ	不明	00 01	00 01
2	2		不明	00 00	00 00
4	4		カテゴリ数	09 00	09 00
6	6		不明	<b>00 00</b>	<b>1F 00</b>
8	8		システム カテゴリのサブセット数へのオフセット	<b>76 00</b>	<b>76 00</b>
10	A		不明	00 00	00 00
12	C	システム	セキュリティ状態の変更	01 00	01 00
14	E		セキュリティ システムの拡張	00 00	00 00
16	10		システムの整合性	03 00	03 00
18	12		IPsec ドライバー	00 00	00 00
20	14		その他のシステム イベント	03 00	03 00
22	16	ログオン/ログオフ	ログオン	<b>01 00</b>	<b>03 00</b>
24	18		ログオフ	01 00	01 00
26	1A		アカウント ロックアウト	01 00	01 00
28	1C		IPsec メイン モード	00 00	00 00
30	1E		特殊なログオン	01 00	01 00
32	20		IPsec クイック モード	00 00	00 00
34	22		IPsec 拡張モード	00 00	00 00
36	24		その他のログオン/ログオフ イベント	00 00	00 00
38	26	ネットワーク ポリシー サーバー	<b>00 00</b>	<b>03 00</b>	
40	28	オブジェクト アクセス	ファイル システム	00 00	00 00
42	2A		レジストリ	00 00	00 00
44	2C		カーネル オブジェクト	00 00	00 00
46	2E		SAM	00 00	00 00
48	30		その他のオブジェクト アクセス イベント	00 00	00 00
50	32		証明書サービス	00 00	00 00
52	34		生成されたアプリケーション	00 00	00 00
54	36		ハンドル操作	00 00	00 00
56	38		ファイルの共有	00 00	00 00
58	3A	フィルタリング プラットフォーム パケットのドロップ	00 00	00 00	
60	3C	フィルタリング プラットフォームの接続	00 00	00 00	
62	3E	特権の使用	重要な特権の使用	00 00	00 00
64	40		重要でない特権の使用	00 00	00 00
66	42		その他の特権の使用イベント	00 00	00 00
68	44	詳細追跡	プロセス作成	00 00	00 00
70	46		プロセス終了	00 00	00 00
72	48		DPAPI アクティビティ	00 00	00 00
74	4A		RPC イベント	00 00	00 00
76	4C	ポリシーの変更	ポリシーの変更の監査	01 00	01 00
78	4E		ポリシーの変更の認証	01 00	01 00
80	50		ポリシーの変更の承認	00 00	00 00
82	52		MPSSVC ルールレベル ポリシーの変更	00 00	00 00
84	54		フィルタリング プラットフォームのポリシーの変更	00 00	00 00
86	56		その他のポリシー変更イベント	00 00	00 00
88	58	アカウント管理	ユーザー アカウント管理	01 00	01 00
90	5A		コンピューター アカウント管理	<b>00 00</b>	<b>01 00</b>
92	5C		セキュリティ グループ管理	01 00	01 00
94	5E		配布グループの管理	00 00	00 00
96	60		アプリケーション グループの管理	00 00	00 00
98	62		その他のアカウント管理イベント	00 00	00 00
100	64	DS アクセス	ディレクトリ サービス アクセス	<b>00 00</b>	<b>01 00</b>
102	66		ディレクトリ サービスの変更	00 00	00 00
104	68		ディレクトリ サービスのレプリケーション	00 00	00 00
106	6A		詳細なディレクトリ サービス レプリケーション	00 00	00 00
108	6C	アカウント ログオン	資格情報の確認	<b>00 00</b>	<b>01 00</b>
110	6E		Kerberos サービス チケット操作	<b>00 00</b>	<b>01 00</b>
112	70		その他のアカウント ログオン イベント	00 00	00 00
114	72		Kerberos 認証サービス	<b>00 00</b>	<b>01 00</b>
116	74	フッタ	不明	00 00	00 00
118	<b>76</b>		システム カテゴリのサブカテゴリ数	05 00	05 00
120	78		ログオン/ログオフ カテゴリのサブカテゴリ数	09 00	09 00
122	7A		オブジェクト アクセス カテゴリのサブカテゴリ数	0B 00	0B 00
124	7C		特権の使用 カテゴリのサブカテゴリ数	03 00	03 00
126	7E		詳細追跡 カテゴリのサブカテゴリ数	04 00	04 00
128	80		ポリシーの変更 カテゴリのサブカテゴリ数	06 00	06 00
130	82		アカウント管理 カテゴリのサブカテゴリ数	06 00	06 00
132	84		DS アクセス カテゴリのサブカテゴリ数	04 00	04 00
134	86		アカウント ログオン カテゴリのサブカテゴリ数	04 00	04 00

Offset 10進	Offset 16進	カテゴリ/サブカテゴリ(説明) (00 00: 監査しない, 01 00: 成功, 02 00: 失敗, 03 00: 成功および失敗)	Default (7)	Default (2008 x64)	
0	0	ヘッダ	不明	00 01	
2	2		不明	00 00	
4	4		カテゴリ数	09 00	
6	6		不明	00 00	
8	8		システム カテゴリのサブセット数へのオフセット	<b>78 00</b>	<b>78 00</b>
10	A		不明	00 00	00 00
12	C	システム	セキュリティ状態の変更	01 00	
14	E		セキュリティ システムの拡張	00 00	
16	10		システムの整合性	03 00	
18	12		IPsec ドライバー	00 00	
20	14	その他のシステム イベント	03 00	03 00	
22	16	ログオン/ログオフ	ログオン	<b>01 00</b>	
24	18		ログオフ	01 00	
26	1A		アカウント ロックアウト	01 00	
28	1C		IPsec メイン モード	00 00	
30	1E		特殊なログオン	01 00	
32	20		IPsec クイック モード	00 00	
34	22		IPsec 拡張モード	00 00	
36	24		その他のログオン/ログオフ イベント	00 00	
38	26	ネットワーク ポリシー サーバー	03 00	03 00	
40	28	オブジェクト アクセス	ファイル システム	00 00	
42	2A		レジストリ	00 00	
44	2C		カーネル オブジェクト	00 00	
46	2E		SAM	00 00	
48	30		その他のオブジェクト アクセス イベント	00 00	
50	32		証明書サービス	00 00	
52	34		生成されたアプリケーション	00 00	
54	36		ハンドル操作	00 00	
56	38		ファイルの共有	00 00	
58	3A		フィルタリング プラットフォーム パケットのドロップ	00 00	
60	3C	フィルタリング プラットフォームの接続	00 00		
62	3E	<b>詳細なファイル共有</b>	00 00	00 00	
64	40	特権の使用	重要な特権の使用	00 00	
66	42		重要でない特権の使用	00 00	
68	44		その他の特権の使用イベント	00 00	
70	46	詳細追跡	プロセス作成	00 00	
72	48		プロセス終了	00 00	
74	4A		DPAPI アクティビティ	00 00	
76	4C		RPC イベント	00 00	
78	4E	ポリシーの変更	ポリシーの変更の監査	01 00	
80	50		ポリシーの変更の認証	01 00	
82	52		ポリシーの変更の承認	00 00	
84	54		MPSSVC ルールレベル ポリシーの変更	00 00	
86	56		フィルタリング プラットフォームのポリシーの変更	00 00	
88	58		その他のポリシー変更イベント	00 00	
90	5A	アカウント管理	ユーザー アカウント管理	01 00	
92	5C		コンピューター アカウント管理	<b>00 00</b>	<b>01 00</b>
94	5E		セキュリティ グループ管理	01 00	
96	60		配布グループの管理	00 00	
98	62		アプリケーション グループの管理	00 00	
100	64		その他のアカウント管理イベント	00 00	
102	66	DS アクセス	ディレクトリ サービス アクセス	<b>00 00</b>	
104	68		ディレクトリ サービスの変更	00 00	
106	6A		ディレクトリ サービスのレプリケーション	00 00	
108	6C		詳細なディレクトリ サービス レプリケーション	00 00	
110	6E	アカウント ログオン	資格情報の確認	<b>00 00</b>	
112	70		Kerberos サービス チケット操作	<b>00 00</b>	
114	72		その他のアカウント ログオン イベント	00 00	
116	74		Kerberos 認証サービス	<b>00 00</b>	
118	76	フッタ	不明	00 00	
120	<b>78</b>		システム カテゴリのサブカテゴリ数	05 00	
122	7A		ログオン/ログオフ カテゴリのサブカテゴリ数	09 00	
124	7C		オブジェクト アクセス カテゴリのサブカテゴリ数	<b>0C 00</b>	
126	7E		特権の使用 カテゴリのサブカテゴリ数	03 00	
128	80		詳細追跡 カテゴリのサブカテゴリ数	04 00	
130	82		ポリシーの変更 カテゴリのサブカテゴリ数	06 00	
132	84		アカウント管理 カテゴリのサブカテゴリ数	06 00	
134	86		DS アクセス カテゴリのサブカテゴリ数	04 00	
136	88		アカウント ログオン カテゴリのサブカテゴリ数	04 00	

Offset 10進	Offset 16進	カテゴリ/サブカテゴリ(説明) (00 00: 監査しない, 01 00: 成功, 02 00: 失敗, 03 00: 成功および失敗)		Default (8.1)	Default (2012)
0	0	ヘッダ	不明	00 01	00 01
2	2		不明	00 00	00 00
4	4		カテゴリ数	09 00	09 00
6	6		不明	00 00	00 00
8	8		システム カテゴリのサブセット数へのオフセット	<b>7E 00</b>	<b>7E 00</b>
10	A		不明	00 00	00 00
12	C	システム	セキュリティ状態の変更	01 00	01 00
14	E		セキュリティ システムの拡張	00 00	00 00
16	10		システムの整合性	03 00	03 00
18	12		IPsec ドライバー	00 00	00 00
20	14		その他のシステム イベント	03 00	03 00
22	16	ログオン/ログオフ	ログオン	<b>01 00</b>	<b>03 00</b>
24	18		ログオフ	01 00	01 00
26	1A		アカウント ロックアウト	01 00	01 00
28	1C		IPsec メイン モード	00 00	00 00
30	1E		特殊なログオン	01 00	01 00
32	20		IPsec クイック モード	00 00	00 00
34	22		IPsec 拡張モード	00 00	00 00
36	24		その他のログオン/ログオフ イベント	00 00	00 00
38	26	ネットワーク ポリシー サーバー	03 00	03 00	
40	28		<b>ユーザー要求/デバイスの信頼性情報</b>	00 00	00 00
42	2A	オブジェクト アクセス	ファイル システム	00 00	00 00
44	2C		レジストリ	00 00	00 00
46	2E		カーネル オブジェクト	00 00	00 00
48	30		SAM	00 00	00 00
50	32		その他のオブジェクト アクセス イベント	00 00	00 00
52	34		証明書サービス	00 00	00 00
54	36		生成されたアプリケーション	00 00	00 00
56	38		ハンドルの操作	00 00	00 00
58	3A	ファイルの共有	00 00	00 00	
60	3C	フィルタリング プラットフォーム パケットのドロップ	00 00	00 00	
62	3E	フィルタリング プラットフォームの接続	00 00	00 00	
64	40	詳細なファイル共有	00 00	00 00	
66	42		<b>リムーバブル記憶域</b>	00 00	00 00
68	44		<b>集約型アクセス ポリシー ステージング</b>	00 00	00 00
70	46	特権の使用	重要な特権の使用	00 00	00 00
72	48		重要でない特権の使用	00 00	00 00
74	4A		その他の特権の使用イベント	00 00	00 00
76	4C	詳細追跡	プロセス作成	00 00	00 00
78	4E		プロセス終了	00 00	00 00
80	50		DPAPI アクティビティ	00 00	00 00
82	52		RPC イベント	00 00	00 00
84	54	ポリシーの変更	ポリシーの変更の監査	01 00	01 00
86	56		ポリシーの変更の認証	01 00	01 00
88	58		ポリシーの変更の承認	00 00	00 00
90	5A		MPSSVC ルールレベル ポリシーの変更	00 00	00 00
92	5C		フィルタリング プラットフォームのポリシーの変更	00 00	00 00
94	5E		その他のポリシー変更イベント	00 00	00 00
96	60	アカウント管理	ユーザー アカウント管理	01 00	01 00
98	62		コンピューター アカウント管理	<b>00 00</b>	<b>01 00</b>
100	64		セキュリティ グループ管理	01 00	01 00
102	66		配布グループの管理	00 00	00 00
104	68		アプリケーション グループの管理	00 00	00 00
106	6A		その他のアカウント管理イベント	00 00	00 00
108	6C	DS アクセス	ディレクトリ サービス アクセス	<b>00 00</b>	<b>01 00</b>
110	6E		ディレクトリ サービスの変更	00 00	00 00
112	70		ディレクトリ サービスのレプリケーション	00 00	00 00
114	72		詳細なディレクトリ サービス レプリケーション	00 00	00 00
116	74	アカウント ログオン	資格情報の確認	<b>00 00</b>	<b>01 00</b>
118	76		Kerberos サービス チケット操作	<b>00 00</b>	<b>01 00</b>
120	78		その他のアカウント ログオン イベント	00 00	00 00
122	7A		Kerberos 認証サービス	<b>00 00</b>	<b>01 00</b>
124	7C	フッタ	不明	<b>FE 7F</b>	<b>FD 7F</b>
126	<b>7E</b>		システム カテゴリのサブカテゴリ数	05 00	05 00
128	80		ログオン/ログオフ カテゴリのサブカテゴリ数	<b>0A 00</b>	<b>0A 00</b>
130	82		オブジェクト アクセス カテゴリのサブカテゴリ数	<b>0E 00</b>	<b>0E 00</b>
132	84		特権の使用 カテゴリのサブカテゴリ数	03 00	03 00
134	86		詳細追跡 カテゴリのサブカテゴリ数	04 00	04 00
136	88		ポリシーの変更 カテゴリのサブカテゴリ数	06 00	06 00
138	8A		アカウント管理 カテゴリのサブカテゴリ数	06 00	06 00
140	8C		DS アクセス カテゴリのサブカテゴリ数	04 00	04 00
142	8E		アカウント ログオン カテゴリのサブカテゴリ数	04 00	04 00

Offset 10進	Offset 16進	カテゴリ/サブカテゴリ(説明) (00 00: 監査しない, 01 00: 成功, 02 00: 失敗, 03 00: 成功および失敗)		Default (10 TP)	Default (Server TP)
0	0	ヘッダ	不明	00 01	00 01
2	2		不明	00 00	00 00
4	4		カテゴリ数	09 00	09 00
6	6		不明	00 00	00 00
8	8		システム カテゴリのサブセット数へのオフセット	<b>82 00</b>	<b>82 00</b>
10	A		不明	00 00	00 00
12	C	システム	セキュリティ状態の変更	01 00	01 00
14	E		セキュリティ システムの拡張	00 00	00 00
16	10		システムの整合性	03 00	03 00
18	12		IPsec ドライバー	00 00	00 00
20	14		その他のシステム イベント	03 00	03 00
22	16	ログオン/ログオフ	ログオン	<b>01 00</b>	<b>03 00</b>
24	18		ログオフ	01 00	01 00
26	1A		アカウント ロックアウト	01 00	01 00
28	1C		IPsec メイン モード	00 00	00 00
30	1E		特殊なログオン	01 00	01 00
32	20		IPsec クイック モード	00 00	00 00
34	22		IPsec 拡張モード	00 00	00 00
36	24		その他のログオン/ログオフ イベント	00 00	00 00
38	26		ネットワーク ポリシー サーバー	03 00	03 00
40	28		ユーザー要求/デバイスの信頼性情報	00 00	00 00
42	2A		<b>監査グループのメンバーシップ</b>	00 00	00 00
44	2C	オブジェクト アクセス	ファイル システム	00 00	00 00
46	2E		レジストリ	00 00	00 00
48	30		カーネル オブジェクト	00 00	00 00
50	32		SAM	00 00	00 00
52	34		その他のオブジェクト アクセス イベント	00 00	00 00
54	36		証明書サービス	00 00	00 00
56	38		生成されたアプリケーション	00 00	00 00
58	3A		ハンドル操作	00 00	00 00
60	3C		ファイルの共有	00 00	00 00
62	3E		フィルタリング プラットフォーム パケットのドロップ	00 00	00 00
64	40	フィルタリング プラットフォームの接続	00 00	00 00	
66	42	詳細なファイル共有	00 00	00 00	
68	44	リムーバブル記憶域	00 00	00 00	
70	46		集約型アクセス ポリシー ステージング	00 00	00 00
72	48	特権の使用	重要な特権の使用	00 00	00 00
74	4A		重要でない特権の使用	00 00	00 00
76	4C		その他の特権の使用イベント	00 00	00 00
78	4E	詳細追跡	プロセス作成	00 00	00 00
80	50		プロセス終了	00 00	00 00
82	52		DPAPI アクティビティ	00 00	00 00
84	54		RPC イベント	00 00	00 00
86	56		<b>PNP アクティビティ</b>	00 00	00 00
88	58	ポリシーの変更	ポリシーの変更の監査	01 00	01 00
90	5A		ポリシーの変更の認証	01 00	01 00
92	5C		ポリシーの変更の承認	00 00	00 00
94	5E		MPSSVC ルールレベル ポリシーの変更	00 00	00 00
96	60		フィルタリング プラットフォームのポリシーの変更	00 00	00 00
98	62		その他のポリシー変更イベント	00 00	00 00
100	64	アカウント管理	ユーザー アカウント管理	01 00	01 00
102	66		コンピューター アカウント管理	<b>00 00</b>	<b>01 00</b>
104	68		セキュリティ グループ管理	01 00	01 00
106	6A		配布グループの管理	00 00	00 00
108	6C		アプリケーション グループの管理	00 00	00 00
110	6E		その他のアカウント管理イベント	00 00	00 00
112	70	DS アクセス	ディレクトリ サービス アクセス	<b>00 00</b>	<b>01 00</b>
114	72		ディレクトリ サービスの変更	00 00	00 00
116	74		ディレクトリ サービスのレプリケーション	00 00	00 00
118	76		詳細なディレクトリ サービス レプリケーション	00 00	00 00
120	78	アカウント ログオン	資格情報の確認	<b>00 00</b>	<b>01 00</b>
122	7A		Kerberos サービス チケット操作	<b>00 00</b>	<b>01 00</b>
124	7C		その他のアカウント ログオン イベント	00 00	00 00
126	7E		Kerberos 認証サービス	<b>00 00</b>	<b>01 00</b>
128	80	フッタ	不明	<b>7F 8E</b>	<b>14 4F</b>
130	<b>82</b>		システム カテゴリのサブカテゴリ数	05 00	05 00
132	84		ログオン/ログオフ カテゴリのサブカテゴリ数	<b>0B 00</b>	<b>0B 00</b>
134	86		オブジェクト アクセス カテゴリのサブカテゴリ数	0E 00	0E 00
136	88		特権の使用 カテゴリのサブカテゴリ数	03 00	03 00
138	8A		詳細追跡 カテゴリのサブカテゴリ数	<b>05 00</b>	<b>05 00</b>
140	8C		ポリシーの変更 カテゴリのサブカテゴリ数	06 00	06 00
142	8E		アカウント管理 カテゴリのサブカテゴリ数	06 00	06 00
144	90		DS アクセス カテゴリのサブカテゴリ数	04 00	04 00
146	92		アカウント ログオン カテゴリのサブカテゴリ数	04 00	04 00

Offset 10進	Offset 16進	カテゴリ/サブカテゴリ(説明) (00 00: 監査しない, 01 00: 成功, 02 00: 失敗, 03 00: 成功および失敗)		Default (10 (1607))	Default (2016)
0	0	ヘッダ	不明	00 01	00 01
2	2		不明	00 00	00 00
4	4		カテゴリ数	09 00	09 00
6	6		不明	00 00	00 00
8	8		システム カテゴリのサブセット数へのオフセット	<b>84 00</b>	<b>84 00</b>
10	A		不明	00 00	00 00
12	C	システム	セキュリティ状態の変更	01 00	01 00
14	E		セキュリティ システムの拡張	00 00	00 00
16	10		システムの整合性	03 00	03 00
18	12		IPsec ドライバー	00 00	00 00
20	14		その他のシステム イベント	03 00	03 00
22	16	ログオン/ログオフ	ログオン	<b>01 00</b>	<b>03 00</b>
24	18		ログオフ	01 00	01 00
26	1A		アカウント ロックアウト	01 00	01 00
28	1C		IPsec メイン モード	00 00	00 00
30	1E		特殊なログオン	01 00	01 00
32	20		IPsec クイック モード	00 00	00 00
34	22		IPsec 拡張モード	00 00	00 00
36	24		その他のログオン/ログオフ イベント	00 00	00 00
38	26		ネットワーク ポリシー サーバー	03 00	03 00
40	28		ユーザー要求/デバイスの信頼性情報	00 00	00 00
42	2A	監査グループのメンバーシップ	00 00	00 00	
44	2C	オブジェクト アクセス	ファイル システム	00 00	00 00
46	2E		レジストリ	00 00	00 00
48	30		カーネル オブジェクト	00 00	00 00
50	32		SAM	00 00	00 00
52	34		その他のオブジェクト アクセス イベント	00 00	00 00
54	36		証明書サービス	00 00	00 00
56	38		生成されたアプリケーション	00 00	00 00
58	3A		ハンドル操作	00 00	00 00
60	3C		ファイルの共有	00 00	00 00
62	3E		フィルタリング プラットフォーム パケットのドロップ	00 00	00 00
64	40		フィルタリング プラットフォームの接続	00 00	00 00
66	42	詳細なファイル共有	00 00	00 00	
68	44	リムーバブル記憶域	00 00	00 00	
70	46	集約型ポリシー ステージング	00 00	00 00	
72	48	特権の使用	重要な特権の使用	00 00	00 00
74	4A		重要でない特権の使用	00 00	00 00
76	4C		その他の特権の使用イベント	00 00	00 00
78	4E	詳細追跡	プロセス作成	00 00	00 00
80	50		プロセス終了	00 00	00 00
82	52		DPAPI アクティビティ	00 00	00 00
84	54		RPC イベント	00 00	00 00
86	56		ブラグ アンド プレイ イベント	00 00	00 00
88	58		<b>Token Right Adjusted Events</b>	00 00	00 00
90	5A	ポリシーの変更	ポリシーの変更の監査	01 00	01 00
92	5C		ポリシーの変更の認証	01 00	01 00
94	5E		ポリシーの変更の承認	00 00	00 00
96	60		MPSSVC ルールレベル ポリシーの変更	00 00	00 00
98	62		フィルタリング プラットフォームのポリシーの変更	00 00	00 00
100	64		その他のポリシー変更イベント	00 00	00 00
102	66	アカウント管理	ユーザー アカウント管理	01 00	01 00
104	68		コンピューター アカウント管理	<b>00 00</b>	<b>01 00</b>
106	6A		セキュリティ グループ管理	01 00	01 00
108	6C		配布グループの管理	00 00	00 00
110	6E		アプリケーション グループの管理	00 00	00 00
112	70		その他のアカウント管理イベント	00 00	00 00
114	72	DS アクセス	ディレクトリ サービス アクセス	<b>00 00</b>	<b>01 00</b>
116	74		ディレクトリ サービスの変更	00 00	00 00
118	76		ディレクトリ サービスのレプリケーション	00 00	00 00
120	78		詳細なディレクトリ サービス レプリケーション	00 00	00 00
122	7A	アカウント ログオン	資格情報の確認	<b>00 00</b>	<b>01 00</b>
124	7C		Kerberos サービス チケット操作	<b>00 00</b>	<b>01 00</b>
126	7E		その他のアカウント ログオン イベント	00 00	00 00
128	80		Kerberos 認証サービス	<b>00 00</b>	<b>01 00</b>
130	82	フッタ	不明	<b>0C DB</b>	<b>33 CC</b>
132	<b>84</b>		システム カテゴリのサブカテゴリ数	05 00	05 00
134	86		ログオン/ログオフ カテゴリのサブカテゴリ数	0B 00	0B 00
136	88		オブジェクト アクセス カテゴリのサブカテゴリ数	0E 00	0E 00
138	8A		特権の使用 カテゴリのサブカテゴリ数	03 00	03 00
140	8C		詳細追跡 カテゴリのサブカテゴリ数	<b>06 00</b>	<b>06 00</b>
142	8E		ポリシーの変更 カテゴリのサブカテゴリ数	06 00	06 00
144	90		アカウント管理 カテゴリのサブカテゴリ数	06 00	06 00
146	92		DS アクセス カテゴリのサブカテゴリ数	04 00	04 00
148	94		アカウント ログオン カテゴリのサブカテゴリ数	04 00	04 00