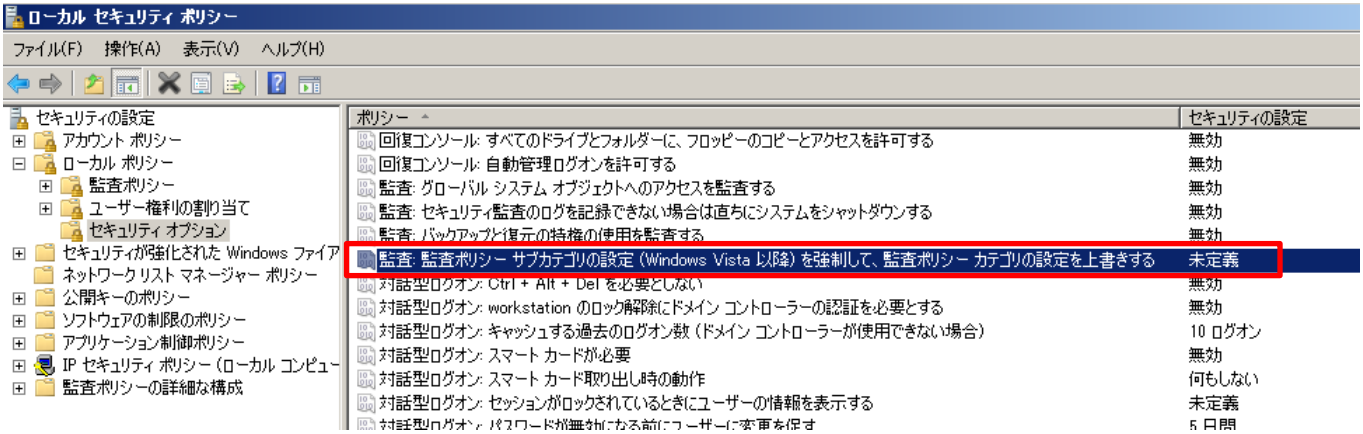
イベントログ大量出力の抑止（Windows Server 2008R2 以降）

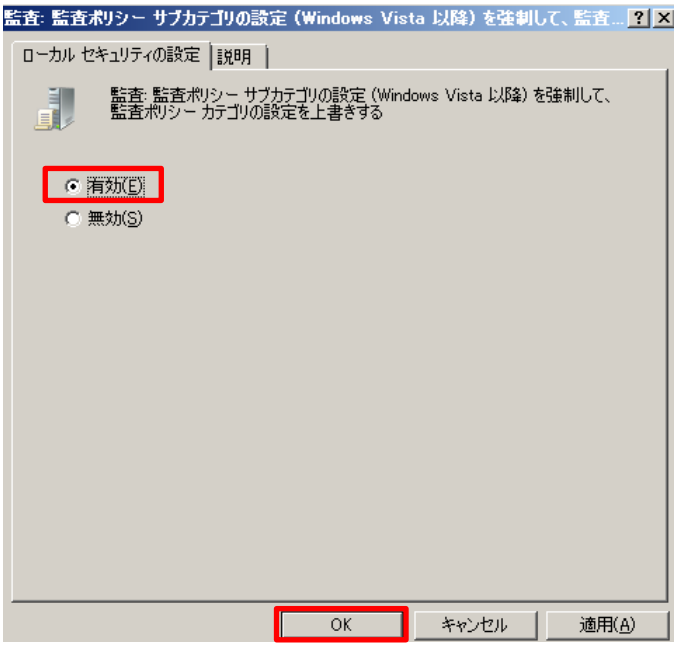
対象サーバの OS バージョンが Windows Server 2008R2 以降の場合、イベントログ（セキュリティ）のレコードが大量出力される事象を確認しております。
イベントログ（セキュリティ）の設定で、「イベントを上書きしないでログをアーカイブする」方式を選択している場合、イベントログのロスト（収集漏れ）は防止することが出来ますが、不要なイベントログの大量出力自体を抑止したい場合は、Windows に対して下記設定を行なうことで、イベントログの大量出力を抑止することが出来ます。

注意	グループポリシーを適用している環境では、ローカルセキュリティポリシーの設定はグループポリシーによって上書きされます。そのため本設定はグループポリシー側で行う必要があります。

1） 管理者権限をもつアカウントでログオンします。
2） スタートメニューの[管理ツール]から[ローカル セキュリティ ポリシー]をダブルクリックします。
3） [ローカルセキュリティポリシー]画面が開きますので[セキュリティの設定]、[ローカルポリシー] 、[セキュリティオプション]と展開し、[監査: 監査ポリシー サブカテゴリの設定 (Windows Vista 以降) を強制して、監査ポリシー カテゴリの設定を上書きする]を開きます。

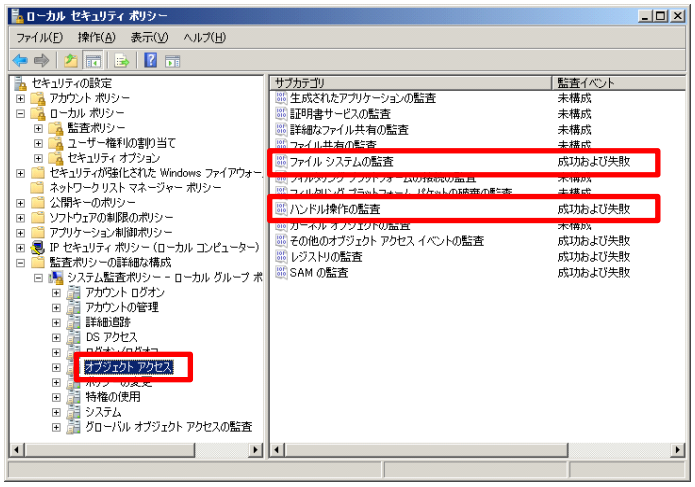


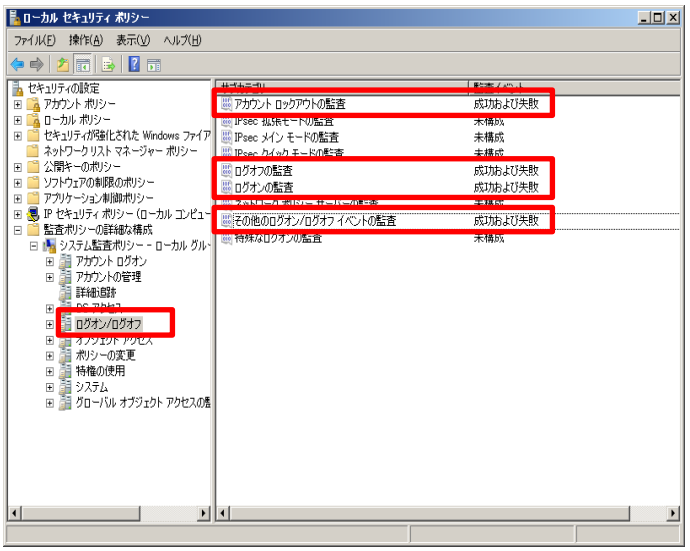
4） [有効]にチェックを入れて、「OK」ボタンをクリックします。



5）[ローカルセキュリティポリシー]画面が開きますので[セキュリティの設定]、[監査ポリシーの詳細な構成]と展開し、[システム監査ポリシー--ローカルグループポリシーオブジェクト]をクリックします。
6）ALog で取得するログに対応する項目に[成功]、[失敗]チェックを入れて[OK]ボタンをクリックし終了します。

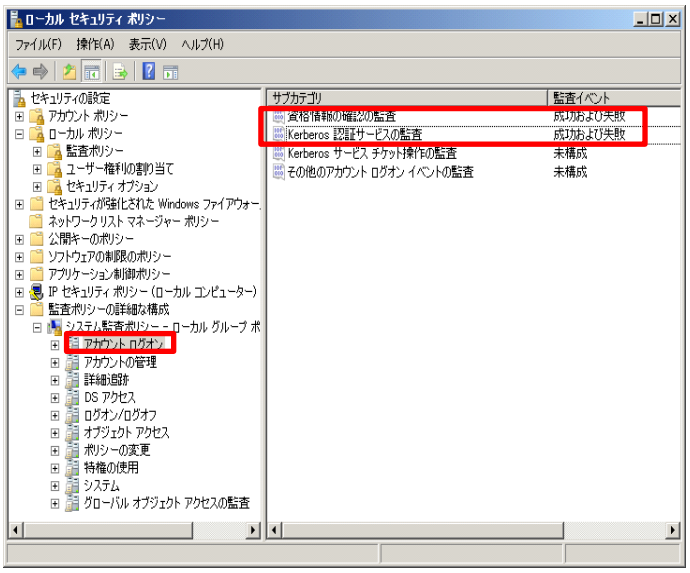
◆ファイルアクセスログ/アクセス権変更ログ

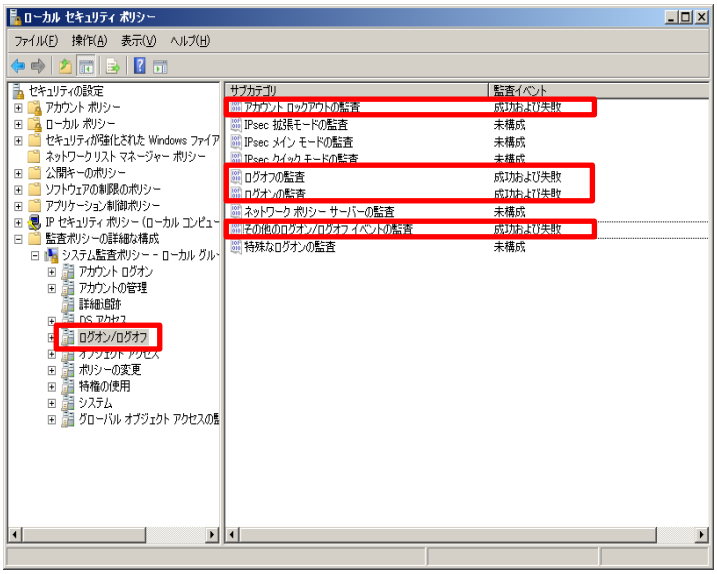




No	カテゴリ	サブカテゴリ	セキュリティの設定	対応バージョン
1	オブジェクト アクセス	生成されたアプリケーションの監査	未構成（監査なし）	Windows Server 2008R2
2		証明書サービスの監査	未構成（監査なし）	
3		詳細なファイル共有の監査	未構成（監査なし）	
4		ファイル共有の監査	未構成（監査なし）	
5		**ファイルシステムの監査**	**成功および失敗**	
6		フィルタリングプラットフォームの接続の監査	未構成（監査なし）	
7		フィルタリングプラットフォームパケットの破棄の監査	未構成（監査なし）	
8		**ハンドル操作の監査**	**成功および失敗**	
9		カーネルオブジェクトの監査	未構成（監査なし）	
10		その他のオブジェクトアクセスイベントの監査	未構成（監査なし）	
11		レジストリの監査	未構成（監査なし）	
12		SAM の監査	未構成（監査なし）	
13		リムーバブル記憶域の監査	未構成（監査なし）	Windows Server 2012
14		集約型アクセスポリシーステージングの監査	未構成（監査なし）	
15	ログオン/ログオフ	**アカウントロックアウトの監査**	**成功および失敗**	Windows Server 2008R2
16		IPsec 拡張モードの監査	未構成（監査なし）	
17		IPsec メインモードの監査	未構成（監査なし）	
18		IPsec クイックモードの監査	未構成（監査なし）	
19		**ログオフの監査**	**成功および失敗**	
20		**ログオンの監査**	**成功および失敗**	
21		ネットワークポリシーサーバの監査	未構成（監査なし）	
22		**その他のログオン/ログオフイベントの監査**	**成功および失敗**	
23		特殊なログオンの監査	未構成（監査なし）	
24		ユーザー要求/デバイスの信頼性情報の監査	未構成（監査なし）	Windows Server 2012

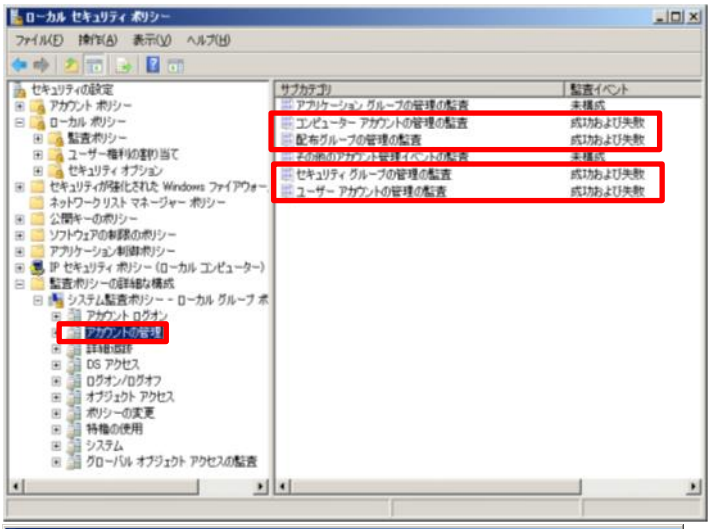
◆ログオン

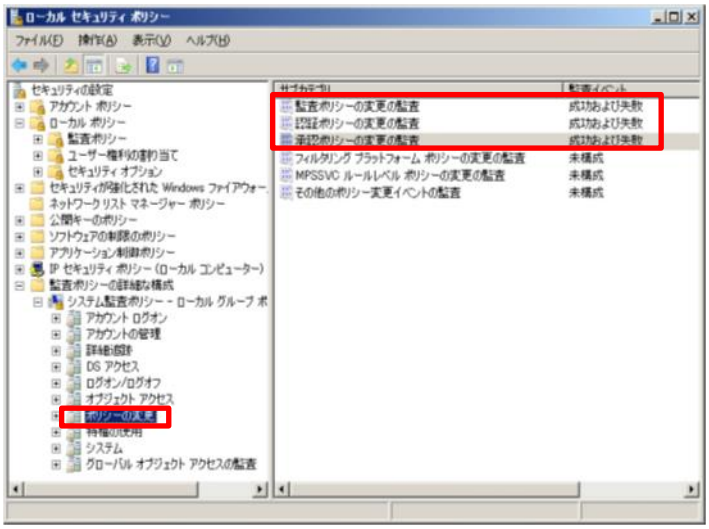


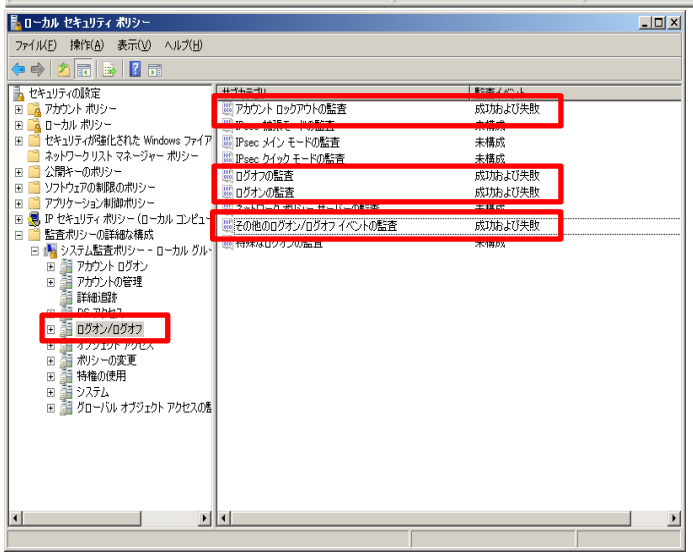


No	カテゴリ	サブカテゴリ	セキュリティの設定	対応バージョン
1	アカウント　ログオン	**資格情報の確認の監査**	**成功および失敗**	Windows Server 2008R2
2		**Kerberos 認証サービスの監査**	**成功および失敗**	
3		Kerberos サービスチケット操作の監査	未構成（監査なし）	
4		その他のアカウントログオンイベントの監査	未構成（監査なし）	
5	ログオン/ログオフ	**アカウントロックアウトの監査**	**成功および失敗**	
6		IPsec 拡張モードの監査	未構成（監査なし）	
7		IPsec メインモードの監査	未構成（監査なし）	
8		IPsec クイックモードの監査	未構成（監査なし）	
9		**ログオフの監査**	**成功および失敗**	
10		**ログオンの監査**	**成功および失敗**	
11		ネットワークポリシーサーバの監査	未構成（監査なし）	
12		**その他のログオン/ログオフイベントの監査**	**成功および失敗**	
13		特殊なログオンの監査	未構成（監査なし）	
14		ユーザー要求/デバイスの信頼性情報の監査	未構成（監査なし）	Windows Server 2012

◆管理者操作ログ

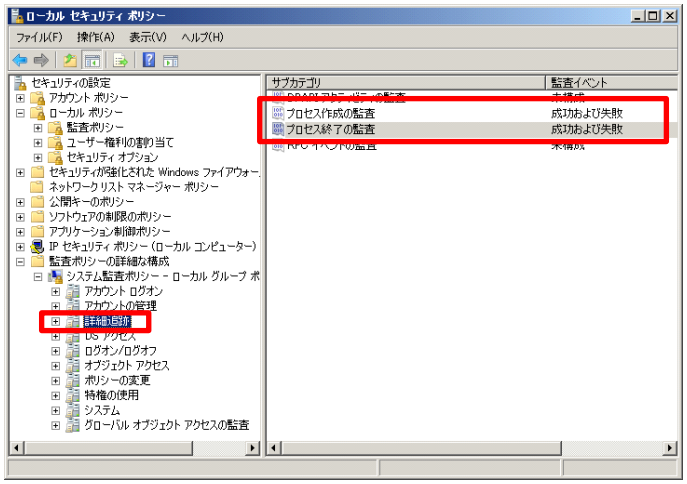


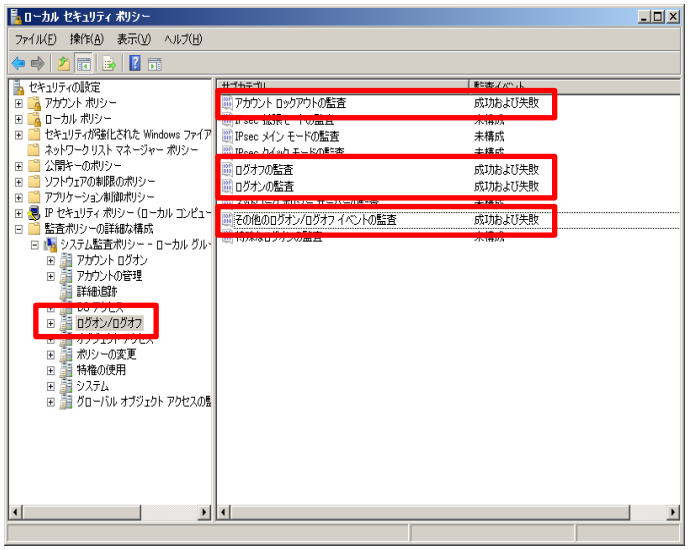




No	カテゴリ	サブカテゴリ	セキュリティの設定	セキュリティの設定
1	アカウントの管理	アプリケーショングループの管理の監査	未構成（監査なし）	Windows Server 2008R2
2		**コンピューターアカウントの管理の監査**	**成功および失敗**	
3		**配布グループの管理の監査**	**成功および失敗**	
4		その他のアカウント管理イベントの監査	未構成（監査なし）	
5		**セキュリティグループの管理の監査**	**成功および失敗**	
6		**ユーザーアカウントの管理の監査**	**成功および失敗**	
7	ポリシーの変更	**監査ポリシーの変更の監査**	**成功および失敗**	
8		**認証ポリシーの変更の監査**	**成功および失敗**	
9		**承認ポリシーの変更の監査**	**成功および失敗**	
10		フィルタリングプラットフォームのポリシーの変更の監査	未構成（監査なし）	
11		MPSSVC ルールレベルポリシーの変更の監査	未構成（監査なし）	
12		その他のポリシー変更イベントの監査	未構成（監査なし）	
13	ログオン/ログオフ	**アカウントロックアウトの監査**	**成功および失敗**	
14		IPsec 拡張モードの監査	未構成（監査なし）	
15		IPsec メインモードの監査	未構成（監査なし）	
16		IPsec クイックモードの監査	未構成（監査なし）	
17		**ログオフの監査**	**成功および失敗**	
18		**ログオンの監査**	**成功および失敗**	
19		ネットワークポリシーサーバの監査	未構成（監査なし）	
20		**その他のログオン/ログオフイベントの監査**	**成功および失敗**	
21		特殊なログオンの監査	未構成（監査なし）	
22		ユーザー要求/デバイスの信頼性情報の監査	未構成（監査なし）	Windows Server 2012

◆アプリケーション起動ログ





No	カテゴリ	サブカテゴリ	セキュリティの設定	セキュリティの設定
1	詳細追跡	DPAPI アクティビティの監査	未構成（監査なし）	Windows Server 2008R2
2		**プロセス作成の監査**	**成功および失敗**	
3		**プロセス終了の監査**	**成功および失敗**	
4		RPC イベントの監査	未構成（監査なし）	
5	ログオン/ログオフ	**アカウントロックアウトの監査**	**成功および失敗**	
6		IPsec 拡張モードの監査	未構成（監査なし）	
7		IPsec メインモードの監査	未構成（監査なし）	
8		IPsec クイックモードの監査	未構成（監査なし）	
9		**ログオフの監査**	**成功および失敗**	
10		**ログオンの監査**	**成功および失敗**	
11		ネットワークポリシーサーバの監査	未構成（監査なし）	
12		**その他のログオン/ログオフイベントの監査**	**成功および失敗**	
13		特殊なログオンの監査	未構成（監査なし）	
14		ユーザー要求/デバイスの信頼性情報の監査	未構成（監査なし）	Windows Server 2012