ManageEngine

最も注意すべき8つの Windowsセキュリティ イベントID

ManageEngine

目次

Windowsセキュリティログ

イベントビューアーで確認できるWindowsセキュリティログには、ログオンとログオフ、アカウント管理、オブジェクトアクセスといった重要なユーザーアクションが記録されます。

Microsoftは、Windowsセキュリティログを「最も効果的な最後の防衛手段(your best and last defense)」と表現していますが、確かにそのとおりです。セキュリティログは、セキュリティ上の潜在的な問題の検出、ユーザーによる説明責任の遂行、セキュリティ侵害発生時のエビデンスとしての活用に役立てることができます。

注意すべきWindowsセキュリティイベントの見分け方

数多くあるWindowsセキュリティイベントのなかで特に重要と考えられるイベントは、大きく分けて次の2つのグループに分類できます。

1. 1回の発生によって悪意のあるアクティビティと認められるイベント。たとえば、標準的なエンドユーザーアカウントが機密性の高いセキュリティグループに突然追加された場合などです。

2. 許容される基準回数を超える連続した発生によって悪意のあるアクティビティと認められるイベント。たとえば、ログオンに失敗した回数が異常に多い場合などです。

最も注意すべき8つのWindowsセキュリティイベントID

通し番号	カテゴリ	イベントIDと説明	監視すべき理由 （すべてが網羅されているわけではありません）
(1)、(2)	**ログオンとログオフ**	**4624**（アカウントが正常にログオンしました。）	・部内者による不正の可能性が高い異常なアクティビティを見つけるため。たとえば、一定期間利用されていないアカウントまたは制限されたアカウントからのログオン、通常の就業時間外のユーザーログオン、多くのリソースへの同時ログオンなどのアクティビティが対象。 ・ユーザーの出勤状況や就業時間など、ユーザーの行動に関する情報を取得するため。
		4625（アカウントがログオンに失敗しました。）	・潜在的なブルートフォース攻撃、辞書攻撃、その他のパスワード類推攻撃を見つけるため。このような攻撃では、ログオンの失敗回数が突然、急上昇するという特徴がある。 ・アカウントロックアウトしきい値ポリシー設定のベンチマークを決定するため。
(3)、(4)、(5)	**アカウント管理**	**4728**（セキュリティが有効なグローバルグループにメンバーが追加されました。）	・大きな権限（keys to the kingdom）を持つ特権ユーザーのグループメンバーシップを確認し、定期的に精査するため。この確認作業はセキュリティグループにメンバーを追加する場合は特に重要である。 ・不正な追加の責任を負うユーザーによる特権の乱用を見つけるため。 ・不測の追加を見つけるため。
		4732（セキュリティが有効なローカルグループにメンバーが追加されました。）	
		4756（セキュリティが有効なユニバーサルグループにメンバーが追加されました。）	

(6)	**イベントログ**	**1102**（監査ログがクリアされました。）（イベントログサービスを無効にして、ログが記録されないように設定することも可能。この設定はシステム監査ポリシーで行いますが、この場合、イベント**4719**が記録される。）	・イベントログを改ざんするなどの悪意を持つユーザーを見分けるため。
(7)	**アカウント管理**	**4740**（ユーザーアカウントがロックアウトされました。）	・潜在的なブルートフォース攻撃、辞書攻撃、その他のパスワード類推攻撃を見つけるため。このような攻撃では、ログオンの失敗回数が突然、急上昇するという特徴がある。 ・正当なユーザーがロックアウトされて業務の遂行ができなくなるという影響を緩和するため。
(8)	**オブジェクトへのアクセス**	**4663**（オブジェクトにアクセスしようとしました。）	・ファイルやフォルダへの不正なアクセス試行を見つけるため。

ManageEngine

Active Directoryの保護

何より重要なこととして、Windowsでセキュリティログに関連イベントを記録できるようにするために、監査ポリシーを構成する必要があります。次に、収集されたログを集約して分析し、その結果をレポートやアラートなどの実用的な情報に変換します。ネイティブツールやPowerShellスクリプトを使用して、このような作業を行う場合は、専門的知識と多くの時間が必要になります。そのため、迅速かつ効率的に作業を行うには、サードパーティ製ツールの導入が不可欠です。

ADAudit Plusの詳細なレポート、リアルタイムのアラート、グラフィカルな表示などの機能を使用することで、Active Directoryおよび各サーバー、ワークステーションにおける**ログオンとログオフ**、**グループメンバーシップの変更**、**イベントログの消去**、**アカウントのロックアウト**、**ファイルサーバー**、その他のアクティビティの継続的な監視作業を簡素化できます。

ManageEngine
ADAudit Plus

ManageEngine ADAudit Plusは、ITのセキュリティとコンプライアンスに対応したソリューションです。200以上のイベント固有のレポートとリアルタイムのメールアラートにより、Active Directory、Microsoft Entra(旧Azure AD)、Windows Serversのコンテンツおよび構成に対して行われた変更の詳細な情報を取得できます。さらに、ワークステーションやファイルサーバー（NetApp、EMCなど）の詳細なアクセス情報を把握することも可能です。

お問合せ　**評価版ダウンロード**

最も注意すべき8つのWidowsセキュリティイベントID

2023年12月発行

■ 本製品に関するお問い合わせ
ゾーホージャパン株式会社ManageEngine事業部
〒222-0012 神奈川県横浜市西区みなとみらい三丁目6番1号 みなとみらいセンタービル 13階

ADAudit Plus製品ページ：https://www.manageengine.jp/products/ADAudit_Plus/
ホームページ：https://www.manageengine.jp/

■ 注意事項
本ガイドの内容は、改良のため、予告なく変更することがあります。
ゾーホージャパン株式会社は本ガイドに関しての一切の責任を負いかねます。
当社は、本ガイドを使用することにより引き起こされた偶発的もしくは間接的な損害についても責任を負いかねます。
本記事はグローバル本社のホワイトペーパーを翻訳し、加筆・修正したものです。原文はこちらをご参照ください。

ZJMP181218101 V2 231207