Active Directoryに対する攻撃検知のための管理者アカウント確認フロー

- ManageEngine対応製品とのマッピング -

ゾーホージャパン株式会社
ManageEngine

<Active Directoryの攻撃検知と対策>

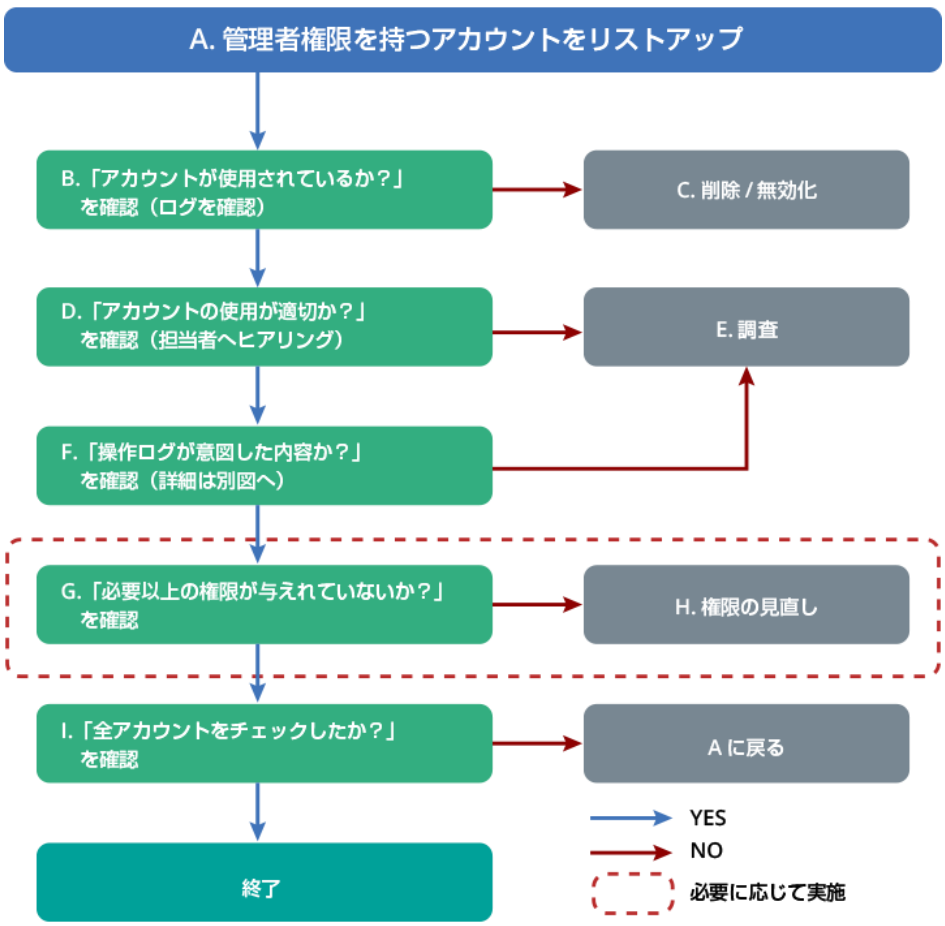
標的型攻撃が横行する昨今、企業内ネットワークに侵入した攻撃者によってActive Directoryのドメイン管理者アカウントが狙われるケースが多発しています。

攻撃者から重要情報を守るため、Active Directoryの管理者アカウントを防衛することはとても重要です。以下表は、JPCERT/CCが公開している「Active Directory のドメイン管理者アカウントの不正使用に関する注意喚起」から引用した「管理者アカウントについての確認内容」の一覧表です。

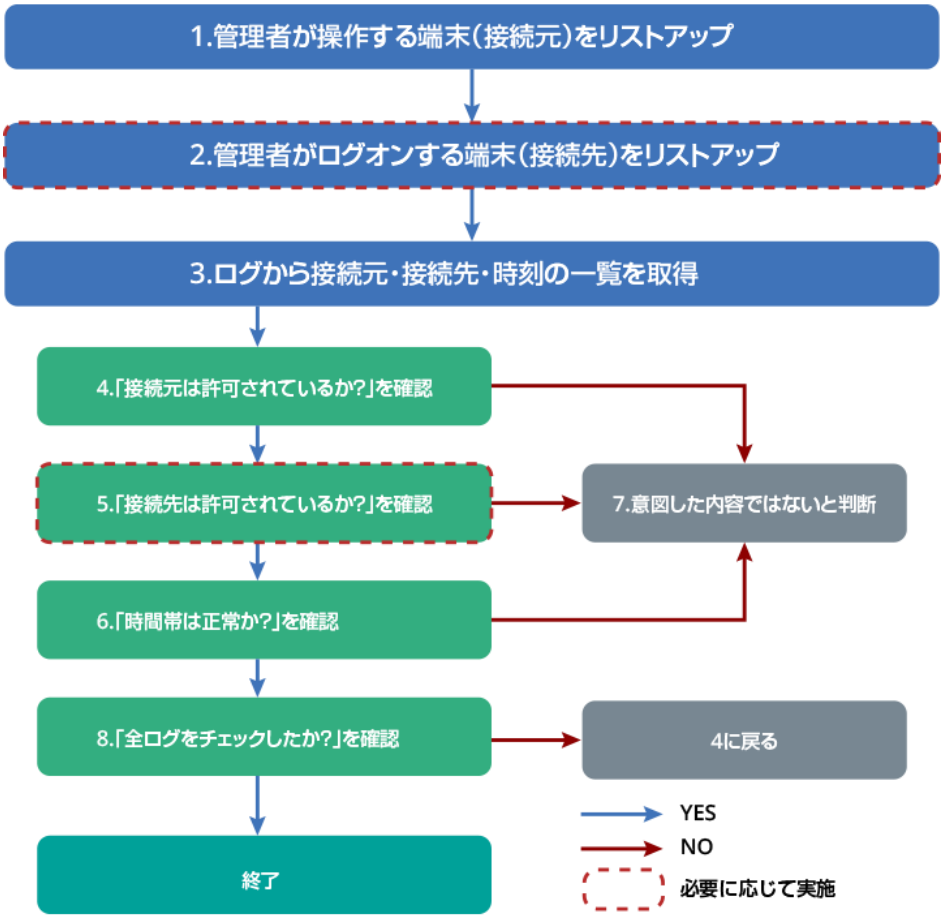
企業のセキュリティ対策の一環として、以下のような確認作業を独自に行うことが推奨されています。

管理者アカウントについての確認内容
・ログイン状況 - 使用していないはずのアカウントが使用されていないか
・接続先 - 管理者がログオンすることのないユーザ端末やサーバ、ドメインコントローラへのログオン・ログオン試行がないか
・接続元端末 - 管理者アカウントの運用を行うことのない端末での管理者アカウントの使用がないか
・使用している時間帯 - 休日や、業務時間外の深夜・早朝など業務で使用されていない期間のアクセスがないか
・操作内容 - 管理者アカウントの追加や、ポリシーの変更、イベントログの削除など想定していない操作が行われていないか

次の図は、具体的な確認作業をフローチャートで表現したものです（Active Directory のドメイン管理者アカウントの不正使用に関する注意喚起から引用の上、加筆・修正）。



前項の図の内、「F.操作ログが意図した内容か？」を洗い出すための確認作業をフローチャートとして表現したものが下図です（ Active Directory のドメイン管理者アカウントの不正使用に関する注意喚起　から引用の上、加筆・修正）。



A-Iおよび1-8のフローのそれぞれの項目に対して、すべて人力で行うにはリソース/工数が多分にかかります。ManageEngineが提供するソフトウェアと組み合わせて作業を行うことで、効率的かつ網羅的な確認が可能です。各項目と対応するManageEngine製品機能のマッピング表については、次項に掲載する表をご参照ください。

管理者アカウントについての確認作業

要件			ManageEngine対応製品		
No	作業内容	ツールへの必要要件	ADManager Plus	ADAudit Plus	Password Manager Pro
A	管理者権限を持つアカウントをリストアップ	管理者アカウントを判別する機能	グループに所属するアカウント一覧のレポート		
B	「アカウントが使用されているか？」を確認（ログを確認）	管理者アカウントのログイン状況と操作履歴をレポートする機能	未使用ADアカウントのレポート	ログオンレポート	
C	削除・無効化	削除・無効の操作と記録をする機能	未使用アカウントを個別もしくは一括で無効化		
D	「アカウントの使用が適切か？」を確認（担当者へヒアリング）	管理者アカウント利用時の申請内容を確認できる機能			ドメイン管理者利用時の申請内容の照会
E	調査	ツールで対応しない範囲			
F	「操作ログが意図した内容か？」を確認	不適切な操作を検出する機能		・認証失敗履歴のレポート ・特定のイベントIDの操作検出とアラート通知	ドメイン管理者利用時の申請内容の照会
G	「必要以上の権限が与えれていないか？」を確認	セキュリティグループの移動操作を記録する機能	グループに所属するアカウント一覧のレポート	適切な申請承認プロセスを得て変更されている権限がないか検出	ドメイン管理者利用時の申請内容の照会
H	権限の見直し	管理者アカウント利用時の申請内容を確認できる機能	・グループに所属するアカウント一覧のレポート ・グループメンバー変更の申請	グループの変更履歴のレポート	ドメイン管理者利用時の申請
I	「全アカウントをチェックしたか？」を確認	ADに関するログの記録と閲覧の機能	・ユーザー一覧レポート ・グループに所属するユーザー一覧のレポート	DCへのログオン/ログオフ、RDPセッション、ユーザー/グループ/OU/コンピューター/GPO、DNS、ADスキーマへの変更情報の記録と閲覧機能	ドメイン管理者利用時の申請内容の照会

意図しない操作ログについての確認作業

要件			ManageEngine対応製品		
No	作業内容	ツールへの必要要件	ADManager Plus	ADAudit Plus	Password Manager Pro
1	管理者が操作する端末（接続元）をリストアップ	管理者アカウントでの接続元を限定できる機能	踏み台アクセスにより、接続元を運用上固定化	管理者アカウント利用時にADManager PlusやPassoword Manager Pro以外からのアクセスの場合に検知しアラート通知	踏み台アクセスにより、接続元を運用上固定化
2	管理者がログオンする端末（接続先）をリストアップ	ツールで対応しない範囲			
3	ログから接続元・接続先・時刻の一覧を取得	接続元・接続先ドメインコントローラ・時刻の一覧が判別できるレポート機能	監査レポート	接続先DC毎に、接続元、時刻、ADに加えた変更レポート	監査レポート
4	「接続元は許可されているか？」を確認	手続き時の申請内容を確認する機能			ドメイン管理者利用時の申請内容の照会
5	「接続先は許可されているか？」を確認	手続き時の申請内容を確認する機能			ドメイン管理者利用時の申請内容の照会
6	「時間帯は正常か？」を確認	手続き時の申請内容を確認する機能			ドメイン管理者利用時の申請内容の照会（時間外申請があったか）
7	意図した操作でないと判断	ツールで対応しない範囲			
8	「全ログをチェックしたか？」を確認	ADに関するログの記録と閲覧の機能	・ユーザー一覧レポート ・グループに所属するユーザー一覧のレポート	DCへのログオン/ログオフ、RDPセッション、ユーザー/グループ/OU/コンピューター/GPO、DNS、ADスキーマへの変更情報の記録と閲覧機能	ドメイン管理者利用時の申請内容の照会

お問合せ

ご要件や検討状況をお聞きし、 ご相談やお見積りを承っております。
ご希望の方は以下へお問い合わせください。

ゾーホージャパン株式会社　ManageEngine 営業担当

電話：045-319-4612（平日9時 - 18時）
メール：jp-mesales@zohocorp.com