APPENDIX A

システム セキュリティ イベント

次の表に、Cisco ANA EventVision の [Security] タブで表示されるシステム セキュリティ イベントの一覧を示します。システム セキュリティ イベントは、システムと環境を管理する場合のクライアント ログインおよびユーザ アクティビティに関連しています。

セキュリティ イベントの説明で使用される用語と変数は、次のとおりです。

用語	定義
avmid	AVM ID
avmkey	AVM キー
BOS	ANA
DNA	ANA
MC	ユニット（Metro Central）
VNE	仮想ネットワーク要素

表 A-1　　セキュリティ イベント

イベント名	発信元 OID	簡単な説明	重大度	原因	処理
カテゴリ：管理者による処理					
avm-added	IAvm	AVM <ip>:<avmid>（<avmkey>）が追加されました	CLEARED	管理者による処理	不要
avm-classesjar-changed	IAvm	AVM <ip>:<avmid>（<avmkey>）のクラス JAR リストが <classesjar> に変更されました	CLEARED	管理者による処理	不要
avm-disabled	IAvm	AVM <ip>:<avmid>（<avmkey>）がディセーブルにされました	CLEARED	管理者による処理	不要
avm-enabled	IAvm	AVM <ip>:<avmid>（<avmkey>）がイネーブルにされました	CLEARED	管理者による処理	不要
avm-high-availability-disabled	IAvm	AVM <ip>:<avmid>（<avmkey>）のハイ アベイラビリティがディセーブルにされました	CLEARED	管理者による処理	不要
avm-high-availability-enabled	IAvm	AVM <ip>:<avmid>（<avmkey>）のハイ アベイラビリティがイネーブルにされました	CLEARED	管理者による処理	不要

表 A-1　セキュリティ イベント （続き）

イベント名	発信元 OID	簡単な説明	重大度	原因	処理
avm-key-changed	IAvm	AVM <ip>:<avmid>（<avmkey>）のキーが <newkey> に変更されました	CLEARED	管理者による処理	不要
avm-maxmem-changed	IAvm	AVM <ip>:<avmid>（<avmkey>）の最大ヒープ サイズが <maxmem> に変更されました	CLEARED	管理者による処理	不要
avm-moved	IAvm	AVM <ip>:<avmid>（<avmkey>）が <newip> に移動されました	CLEARED	管理者による処理	不要
avm-patchjar-changed	IAvm	AVM <ip>:<avmid>（<avmkey>）のパッチ JAR リストが <patchjar> に変更されました	CLEARED	管理者による処理	不要
avm-removed	IAvm	AVM <ip>:<avmid>（<avmkey>）が削除されました	CLEARED	管理者による処理	不要
avm-restarted	IAvm	AVM <ip>:<avmid>（<avmkey>）が再起動されました	CLEARED	管理者による処理	不要
client-license-added	IClientLicenseManagement	クライアント ライセンス <key> が追加されました	CLEARED	管理者による処理	不要
client-license-removed	IClientLicenseManagement	クライアント ライセンス <key> が削除されました	CLEARED	管理者による処理	不要
element-added	IElementManagement	要素 <key> が AVM <unitip>:<avmid> に追加されました	CLEARED	管理者による処理	不要
element-alias-added	IElementManagement	エイリアス <alias> が（AVM <unitip>:<avmid> 中の）要素 <key> に追加されました	CLEARED	管理者による処理	不要
element-alias-removed	IElementManagement	エイリアス <alias> が（AVM <unitip>:<avmid> 中の）要素 <key> から削除されました	CLEARED	管理者による処理	不要
element-disabled	IElementManagement	（AVM <unitip>:<avmid> 中の）要素 <key> がディセーブルにされました	CLEARED	管理者による処理	不要
element-enabled	IElementManagement	（AVM <unitip>:<avmid> 中の）要素 <key> がイネーブルにされました	CLEARED	管理者による処理	不要
element-moved	IElementManagement	要素 <key> が AVM <unitip>:<avmid> から AVM <newip>:<newavmid> に移動されました	CLEARED	管理者による処理	不要
element-removed	IElementManagement	要素 <key> が AVM <unitip>:<avmid> から削除されました	CLEARED	管理者による処理	不要

表 A-1　セキュリティ イベント （続き）

イベント名	発信元 OID	簡単な説明	重大度	原因	処理
mc-network-high-availability-disabled	IMCNetwork	BOS ネットワークのハイ アベイラビリティがディセーブルになりました	CLEARED	管理者による処理	不要
mc-network-high-availability-enabled	IMCNetwork	BOS ネットワークのハイ アベイラビリティがイネーブルになりました	CLEARED	管理者による処理	不要
permission-added	IPermission	ユーザ <username> にロール <role> を持つスコープ <scope> へのアクセス権が与えられました	CLEARED	管理者がユーザへのアクセス権限付与コマンドを実行しました。	不要
permission-deleted	IPermission	ユーザ <username> のスコープ <scope> へのアクセス権限が抹消されました（以前のロール：<role>）	CLEARED	管理者がユーザへのアクセス権限抹消コマンドを実行しました。	不要
permission-role-changed	IPermission	スコープ <scope> のユーザ <username> のロールが <role> に変更されました	CLEARED	管理者がユーザへのロール変更コマンドを実行しました。	不要
polling-group-added	IPollingGroupManagement	ポーリング グループ <name> （説明：<description>）が追加されました	CLEARED	管理者による処理	不要
polling-group-description-changed	IPollingGroupManagement	ポーリング グループ <name> の説明が <description> に変更されました	CLEARED	管理者による処理	不要
polling-group-removed	IPollingGroupManagement	ポーリング グループ <name> （説明：<description>）が削除されました	CLEARED	管理者による処理	不要
polling-interval-added	IPollingInterval	ポーリング間隔 <group>/<name> （間隔：<interval>）が追加されました	CLEARED	管理者による処理	不要
polling-interval-changed	IPollingInterval	ポーリング間隔 <group>/<name> が <interval> に変更されました	CLEARED	管理者による処理	不要
polling-interval-removed	IPollingInterval	ポーリング間隔 <group>/<name> （間隔：<interval>）が削除されました	CLEARED	管理者による処理	不要
protection-group-added	IProtectionGroup	保護グループ <key>（説明：<description>）が追加されました	CLEARED	管理者による処理	不要
protection-group-description-changed	IProtectionGroup	保護グループ <key> の説明が <description> に変更されました	CLEARED	管理者による処理	不要
protection-group-removed	IProtectionGroup	保護グループ <key>（説明：<description>）が削除されました	CLEARED	管理者による処理	不要

表 A-1　セキュリティ イベント （続き）

イベント名	発信元 OID	簡単な説明	重大度	原因	処理
redundant-unit-added	IMC	DNA Redundant Unit <ip> が追加されました	CLEARED	管理者による処理	不要
scope-created	IScope	スコープ <scope> が作成されました	CLEARED	管理者がスコープ作成コマンドを実行しました。	不要
scope-deleted	IScope	スコープ <scope> が削除されました	CLEARED	管理者がスコープ削除コマンドを実行しました。	不要
scope-elements-added	IScope	次の要素がスコープ <scope>: <elements> に追加されました	CLEARED	管理者がスコープへの要素追加コマンドを実行しました。	不要
scope-elements-removed	IScope	次の要素がスコープ <scope>: <elements> から削除されました	CLEARED	管理者がスコープからの要素削除コマンドを実行しました。	不要
static-link-added	IStaticTopologyManagement	<source> から <destination> への静的トポロジ リンクが追加されました	CLEARED	管理者による処理	不要
static-link-removed	IStaticTopologyManagement	<source> から <destination> への静的トポロジ リンクが削除されました	CLEARED	管理者による処理	不要
transport-uplink-added	IMCNetwork	<sourceaddress>（ローカル名：<sourcename>）と <destinationaddress>（ローカル名：<destinationname>）の間のトランスポート アップリンクが追加されました	CLEARED	管理者による処理	不要
transport-uplink-disabled	IMCNetwork	<sourceaddress>（ローカル名：<sourcename>）と <destinationaddress>（ローカル名：<destinationname>）の間のトランスポート アップリンクがディセーブルにされました	CLEARED	管理者による処理	不要
transport-uplink-enabled	IMCNetwork	<sourceaddress>（ローカル名：<sourcename>）と <destinationaddress>（ローカル名：<destinationname>）の間のトランスポート アップリンクがイネーブルにされました	CLEARED	管理者による処理	不要

表 A-1　セキュリティ イベント （続き）

イベント名	発信元 OID	簡単な説明	重大度	原因	処理
transport-uplink-removed	IMCNetwork	<sourceaddress>（ローカル名：<sourcename>）と <destinationaddress>（ローカル名：<destinationname>）の間のトランスポート アップリンクが削除されました	CLEARED	管理者による処理	不要
unit-added	IMC	DNA Unit <ip> が追加されました	CLEARED	管理者による処理	不要
unit-high-availability-disabled	IMC	BOS Unit <ip> のハイ アベイラビリティがディセーブルにされました	CLEARED	管理者による処理	不要
unit-high-availability-enabled	IMC	BOS Unit <ip> のハイ アベイラビリティがイネーブルにされました	CLEARED	管理者による処理	不要
unit-manual-failover	IMC	手動フェールオーバーが BOS Unit <ip> で開始されました	CLEARED	管理者による処理	不要
unit-protection-group-changed	IMC	BOS Unit <ip> の保護グループが <protectiongroup> に変更されました	CLEARED	管理者による処理	不要
unit-removed	IMC	BOS Unit <ip> が削除されました	CLEARED	管理者による処理	不要
unit-restart	IMC	BOS Unit <ip> が再起動されました	CLEARED	管理者による処理	不要
unit-restarted	IMC	BOS Unit <ip> が再起動されました	CLEARED	管理者による処理	不要
user-created	IBOSUser	ユーザ <username> が作成されました	CLEARED	管理者がユーザ作成コマンドを実行しました。	不要
user-deleted	IBOSUser	ユーザ <username> が削除されました	CLEARED	管理者がユーザ削除コマンドを実行しました。	不要
user-map-added	IBOSUser	ユーザ <username> がマップ <map> の使用権限を与えられました	CLEARED	管理者による処理	不要
user-map-removed	IBOSUser	マップ <map> を使用するユーザ <username> の権限が抹消されました	CLEARED	管理者による処理	不要
user-password-changed	IBOSUser	ユーザ <username> のパスワードが変更されました	CLEARED	管理者がパスワード変更コマンドを実行しました。	不要

表 A-1　セキュリティ イベント （続き）

イベント名	発信元 OID	簡単な説明	重大度	原因	処理
user-property-changed	IBOSUser	ユーザ <username> のプロパティ <property> が <value> に変更されました	CLEARED	管理者がユーザ プロパティの変更コマンドを実行しました。	不要
カテゴリ：不十分な権限					
execute command	IAvm	ユーザ <username> にはコマンド <command name> の実行に必要な権限がありません	MAJOR	ユーザが不十分な権限でコマンドを実行しました。セキュリティ攻撃の可能性があります。	ログを検査し、ユーザおよびコマンドを特定してください。組織のセキュリティ ポリシーにしたがって適切な処置を行います。
カテゴリ：ライセンス					
license_cap_exceeded	IAvm	ユーザ = <username>、ip = <ip> に対するライセンスがキャパシティを超えました	MAJOR	ユーザがログインしようとしましたが、すでに接続数が最大数に達しています。	アプリケーションへのユーザ接続をいくつか閉じてください。
license_expired	IAvm	ユーザ = <username>、ip = <ip> に対するライセンスの期限が切れました	MAJOR	ユーザのライセンスの期限が切れました。	ライセンスを購入するか、別ユーザとしてログインしてください。
no_license	IAvm	ユーザ = <username>、ip = <ip> のライセンスがありません	MAJOR	ユーザにはアプリケーションを使用するライセンスがありません。	ライセンスを購入してください。
カテゴリ：ログイン					
invalid password	IAvm	パスワードが無効です。ユーザ <username> を認証できません	MINOR	ユーザが無効なパスワードを入力しました。	パスワードを正しく入力してください。
invalid user	IAvm	ログインが無効です。未知のユーザ <username>	MINOR	ユーザが無効なログイン名を入力しました。	ログイン名を正しく入力してください。

表 A-1　セキュリティ イベント （続き）

イベント名	発信元 OID	簡単な説明	重大度	原因	処理
session number exceeded	IAvm	ユーザ <username> が開いているセッション数が許可されている数を超過しました	MINOR	ユーザが許可されている数より多くのセッションを開きました。	このユーザに許可するセッションの数を増やすか、指定の数より多いセッションを開かないでください。
success	IAvm	<username> のログインが成功しました	CLEARED	ユーザが正しいログイン情報を入力しました。	不要
total number session exceeded	IAvm	開いているセッションの最大数が超過しました（<maxOpenSessions>）	MINOR	システムのユーザが開いた接続数が多すぎます。	システムへの接続をいくつか閉じてください。
user disabled	IAvm	ユーザ <username> がディセーブルになっています	MINOR	ユーザが何度も不正なパスワードでログインしようとしたため、アカウントがディセーブルになりました。	アカウントをイネーブルにしてください。
カテゴリ：ログオフ					
user logoff	IAvm	ユーザ <username> がログオフしました	CLEARED	ユーザがシステムに接続されていたアプリケーションを閉じました。	不要
カテゴリ：パスワード変更					
password changed	IAvm	ユーザ <username> がパスワードを変更しました	CLEARED	ユーザがパスワードを変更しました。	不要
カテゴリ：パスワード期限切れ					
authenticate	IAvm	パスワードの期限が切れました。ユーザ <username> を認証できません	MINOR	ユーザ パスワードの期限になりました。	ユーザ パスワードを更新してください。
disabled	IAvm	アカウントの無活動タイムアウトの期限が切れました。アカウントがディセーブルになりました。ユーザ <username> を認証できません	MINOR	ユーザが指定時間内にログインしなかったため、アカウントがディセーブルになりました。	ユーザ アカウントをイネーブルにしてください。