IBM Security QRadar
バージョン 7.2.6

Ariel 照会言語ガイド

注記

本書および本書で紹介する製品を使用する前に、 21 ページの『特記事項』に記載されている情報をお読みください。

この資料は、IBM QRadar Security Intelligence Platform V7.2.6 に適用されます。また、この資料の更新版が公開されない限り、これ以降のリリースにも適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： IBM Security QRadar
Version 7.2.6
Ariel Query Language Guide

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

このガイドについて

Ariel 照会言語 (AQL) ガイドは、AQL 拡張検索および API の使用に関する情報を提供します。

対象読者

Ariel データベースに保管されているイベント・データまたはフロー・データを確認するシステム管理者。

テクニカル・ドキュメント

IBM® Security QRadar® の製品資料を Web で入手するには、IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) にアクセスしてください。各言語に翻訳された資料もすべて用意されています。

QRadar 製品ライブラリー内のより技術的な資料にアクセスする方法については、Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644) を参照してください。

カスタマー・サポートへの連絡

お客様サポートへのお問い合わせについては、Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144) を参照してください。

適切なセキュリティーの実践に関する注意事項

IT システムのセキュリティーでは、企業内および企業外からの不適切なアクセスの防止、検出、およびそれらのアクセスへの対応により、システムおよび情報を保護する必要があります。不適切なアクセスにより、情報が改ざん、破壊、盗用、または悪用されたり、あるいはご使用のシステムの損傷または他のシステムへの攻撃のための利用を含む悪用につながる可能性があります。 完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービス、またはセキュリティー対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品およびサービスは、合法かつ包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

注意:

本プログラムの利用は、様々な法律または規制に関わる場合があります。これには、プライバシー、データ保護、雇用、電子通信、および電子保管に関連するものが含まれます。IBM Security QRadar は、合法的な目的のために合法的な手段を用いてのみ使用することができます。お客様は、適用される法律、規制、およびポリ

シーに従って本プログラムを使用することに同意し、かかる法律、規制、およびポリシーを遵守する全責任を負うものとします。ライセンシーは、IBM Security QRadar の合法的な使用に必要なすべての同意、許可、または使用権を取得するか、取得済みであることを表明するものとします。

Ariel 照会言語 (AQL)

Ariel 照会言語 (AQL) は、Ariel データベースと通信するために使用する構造化照会言語です。AQL を使用して、Ariel データベースからのイベント・データおよびフロー・データを管理します。

Ariel 照会言語 (AQL) の非推奨バージョン

Ariel 照会言語 (AQL) V1 および V2 は非推奨です。

コマンド・ライン・スクリプト **/opt/qradar/bin/arielClient** は非推奨です。結果が返される前後とも以下の警告メッセージが表示されます。

```
警告: AQL V1 および V2 は将来非推奨になります。
(WARNING: AQL V1 and V2 will be deprecated in the future.)
 AQL V3 の使用について詳しくは、製品資料を参照してください。
(For information about using AQL V3, see the product documentation.)
```

AQL V3 へのマイグレーション中、次のように入力すると警告メッセージを抑制できます。`/opt/qradar/bin/arielClient | grep -v WARNING`

Python クライアントおよび拡張検索オプションでは AQL V3 が使用されます。

AQL V3 で変更された AQL フィールド

Ariel 照会言語 (AQL) V2 は、QRadar V7.2.4 以降では非推奨です。一部の Ariel データベース・フィールドが AQL V3 では変更または削除されています。これらのフィールドを使用する照会がある場合、それらのフィールドを置換する必要があります。

以下の表は、新規の Ariel データベース・フィールドを示します。

表 1. AQL V3 で置換されたフィールド

フィールド名 (AQL V2)	置換関数名 (AQL V3)
destinationAssetName	AssetHostname
deviceGroup	LogSourceGroupName
sourceAssetName	AssetHostname
eventDescription	QidName
destinationNetwork	NetworkName
endDate	DateFormat
endDateFormatted	DateFormat
eventProcessor	Processorname
identityUsername	AssetUser
identityMAC	AssetProperty
identityHostName	AssetHostname
identityNetBiosName	AssetHostname
identityGroupName	AssetProperty
identityExtendedField	AssetProperty
deviceDate	DateFormat
payloadHex	UTF8

表 1. AQL V3 で置換されたフィールド (続き)

フィールド名 (AQL V2)	置換関数名 (AQL V3)
protocol	ProtocolName
sourceNetwork	NetworkName
startDate	DateFormat
startDateFormatted	DateFormat
destinationAssetName	AssetHostname
sourceAssetName	AssetHostname
destinationNetwork	NetworkName
sourceNetwork	NetworkName
application	ApplicationName
destinationPayloadHex	UTF8
firstPacketDate	DateFormat
eventProcessorId	ProcessorName

以下は、削除された Ariel データベース・フィールドのリストです。

- partialorMatchList
- qidNumber
- token
- destinationHost
- destinationIPSearch
- destinationPortNA
- sourceHost
- sourceIPSearch
- sourcePortNA
- destinationDscpOnly
- anyDestinationFlag
- smallDestinationPayload
- smallDestinationPayloadHex
- destinationPrecedanceOnly
- lastPacketDate
- localHost
- remoteHost
- sourceDscpOnly
- anySourceFlag
- sourcePayloadHex
- smallSourcePayload
- smallSourcePayloadHex
- sourcePrecedanceOnly
- sourceHostString
- destinationHostString
- destinationNetwork
- application

- sourceNetwork
- smallPayload
- smallPayloadHex
- quickSearchMatches
- bitsPerSecond
- srcBitsPerSecond
- dstBitsPerSecond
- bytesPerSecond
- bytesPerPacket
- srcBytesPerPacket
- dstBytesPerPacket
- destinationByteRatio
- destinationPacketRatio
- packetsPerSecond
- sourceByteRatio
- sourcePacketRatio
- totalBytes
- totalPackets
- retentionBucket
- properLastPacketTime
- properLastPacketDate

AQL 関数

Ariel 照会言語 (AQL) の組み込み関数を使用して、Ariel データベース内のデータを計算します。

表 2. 基本関数

演算子	説明	例
LONG	数値を表す値を長整数に変換します。	LONG('1234')
DOUBLE	数値を表す値を double 型に変換します。	DOUBLE('1234')
STR	任意のパラメーターをストリングに変換します。	STR(sourceIP)
STRLEN	このストリングの長さを返します。	STRLEN.(userName)
STRPOS	あるストリング内の別のストリングの位置 (インデックス - 先頭はゼロ) を返します。オプションで、特定のパターンの検索を開始する位置 (インデックス) を示す追加パラメーターを指定できます。	STRPOS(username, 'test'), STRPOS(username, 'test', 5)
SUBSTRING	文字の範囲をコピーして新しいストリングを作成します。	SUBSTRING(userName, 0, 3)
CONCAT	渡されたすべてのストリングを 1 つのストリングに連結します。	CONCAT(userName, STR(sourceIP))
PARSEDATETIME	1970 年 1 月 1 日の協定世界時 (UTC) 00:00:00 からの時間をミリ秒で表現した現在時刻を返します。	PARSEDATETIME('1 week ago')

表 2. 基本関数 (続き)

演算子	説明	例
DATEFORMAT	1970 年 1 月 1 日の協定世界時 (UTC) 00:00:00 からの時間をミリ秒で表現した時刻をユーザーが判読可能な形式にフォーマット設定します。	DATEFORMAT(startTime, 'YYYY-MM-DD HH:mm:ss') as StartTime
NOW	1970 年 1 月 1 日の協定世界時 (UTC) 00:00:00 からの時間をミリ秒で表現した現在時刻を返します。	NOW()
UTF8	バイト配列の UTF8 ストリングを返します。	UTF8(payload)
UPPER	ストリングをすべて大文字にして返します。	UPPER(username)
LOWER	ストリングをすべて小文字にして返します。	LOWER(username)
REPLACEFIRST	正規表現と突き合わせ、最初の一致をテキストで置換します。	REPLACEFIRST('¥d{16}', username, 'censored')
REPLACEALL	正規表現と突き合わせ、すべての一致をテキストで置換します。	REPLACEALL('¥d{16}', username, 'censored')

表 3. 集約関数

演算子	情報	例
GROUP BY	1 つ以上の列の集約を作成します。	SELECT sourceIP, COUNT(*) from events group by sourceIP, destinationIP
COUNT	集約内の行の数を返します。	SELECT sourceIP, COUNT(*) from events group by sourceIP
UNIQUECOUNT	集約内の値の固有カウントを返します。	SELECT sourceIP, UNIQUECOUNT (category) from events group by sourceIP
FIRST	集約内の行の最初の項目を返します。	SELECT sourceIP, FIRST(magnitude) from events group by sourceIP
LAST	集約内の行の最後の項目を返します。	SELECT sourceIP, LAST(magnitude) from events group by sourceIP
SUM	集約内の行の合計を返します。	SELECT sourceIP, SUM(sourceBytes) from flows group by sourceIP
AVG	集約内の行の平均値を返します。	SELECT sourceIP, AVG(magnitude) from events group by sourceIP
MIN	集約内の行の最小値を返します。	SELECT sourceIP, MIN(magnitude) from events group by sourceIP
MAX	集約内の行の最大値を返します。	SELECT sourceIP, MAX(magnitude) from events group by sourceIP
STDEV	集約内の行のサンプル標準偏差値を返します。	SELECT sourceIP, STDEV(magnitude) from events group by sourceIP
STDEVP	集約内の行の母集団標準偏差値を返します。	SELECT sourceIP, STDEVP(magnitude) from events group by sourceIP
HAVING	グループ列の結果について演算子を許可します。	SELECT sourceIP, MAX(magnitude) as MAG from events group by sourceIP HAVING MAG > 5

表 4. 外部関数

名前	説明	引数のタイプ	説明
HostName	ログ・ソース ID またはフロー・ソース ID を検索します。	NUMERIC	ログ・ソース ID またはフロー・ソース ID。

表 4. 外部関数 (続き)

名前	説明	引数のタイプ	説明
AssetHostname	ある時点でのアセットのホスト名を検索します。 特定のドメイン内のアセットをターゲットにするために、オプションでドメインを指定できます。	VARCHAR DOUBLE BIGINT	IP アドレス、タイム・スタンプ オプション: 指定されない場合は NOW() を使用します。 オプション: ドメイン ID
AssetProperty	アセットのプロパティーを検索します。 特定のドメイン内のアセットをターゲットにするために、オプションでドメインを指定できます。	VARCHAR OTHER BIGINT	IP アドレス、プロパティー名 オプション: ドメイン ID
AssetUser	ある時点でのアセットのユーザーを検索します。 特定のドメイン内のアセットをターゲットにするために、オプションでドメインを指定できます。	VARCHAR DOUBLE BIGINT	IP アドレス、タイム・スタンプ オプション: 指定されない場合は NOW() を使用します。オプション: ドメイン ID
MatchesAsset Search	アセットの保存済み検索の結果にアセットが含まれている場合、true を返します。	VARCHAR VARCHAR	IP アドレス、保存済み検索名
ReferenceMap	リファレンス・マップ内のキーの値を検索します。	JAVA_OBJECT JAVA_OBJECT	ストリング、ストリング **例:** ReferenceMap ('IPLookup', 'userName')
ReferenceTable	特定のリファレンス・テーブル収集内のテーブル・キーによって識別されるテーブル内の列キーの値を参照します。	VARCHAR JAVA_OBJECT JAVA_OBJECT	ストリング、ストリング、ストリング (または IP アドレス) **例:** ReferenceTable ('testTable', 'numKey', '100.10.10.1') or ReferenceTable ('testTable', 'numKey', sourceIP)
Reference MapSet Contains	特定のセットのリファレンス・マップ内のキーによって識別されるリファレンス・セットに値が含まれている場合、true を返します。	VARCHAR JAVA_OBJECT JAVA_OBJECT	ストリング、ストリング、ストリング **例:** ReferenceMap SetContains('RiskyUsersForIps', 'sourceIP', 'userName')
ReferenceSet Contains	特定のリファレンス・セットに値が含まれている場合、true を返します。	VARCHAR JAVA_OBJECT	ストリング、ストリング **例:** ReferenceSetContains ('MySet', 'SourceIP')
CategoryName	カテゴリーの名前をカテゴリー ID で検索します。	NUMERIC	カテゴリー ID
LogSource Group Name	ログ・ソース・グループの名前をログ・ソース・グループ ID で検索します。	NUMERIC	デバイス・グループ・リスト **例:** LogSourceGroupName(deviceGroupList)

表 4. 外部関数 (続き)

名前	説明	引数のタイプ	説明
QidDescription	QID の説明を QID で検索します。	NUMERIC	QID
QidName	QID の名前を QID で検索します。	NUMERIC	QID
Application Name	フロー・アプリケーションの名前を返します。	NUMERIC	アプリケーション・アイデンティティー
LogSource Name	ログ・ソースの名前をログ・ソース ID で検索します。	NUMERIC	ログ・ソース ID **例:** LogSourceName(logSourceId)
LogSource Type Name	ログ・ソース・タイプの名前をデバイス・タイプで検索します。	Types .NUMERIC	デバイス・タイプ **例:** LogSourceTypeName(deviceType)
UTF-8	UTF-8 ストリングを返します。	VARBINARY	バイト配列 **例:** Payload
StrLen	このストリングの長さを返します。	VARCHAR	ストリング
Str	パラメーターをストリングに変換します。	JAVA_OBJECT	ストリング
SubString	文字の範囲をコピーして新しいストリングを作成します。	VARCHAR NUMERIC NUMERIC	ストリング、開始の相対位置、および長さ
Concat	渡されたすべてのストリングを 1 つのストリングに連結します。	VARCHAR NUMERIC NUMERIC	ストリングのリスト
ParseDate time	2014 年 1 月 1 日の協定世界時 (UTC) 00:00:00 からの時間をミリ秒で表現した現在時刻を返します。	VARCHAR	日時を表すストリング
Now	2014 年 1 月 1 日の協定世界時 (UTC) 00:00:00 からの時間をミリ秒で表現した現在時刻を返します。	NULL	なし
ProtocolName	プロトコル ID 番号に基づいてプロトコルの名前を返します。	NUMERIC	プロトコル ID 番号
InOffense	イベントまたはフローが指定されたオフェンスに属する場合、true を返します。	NUMERIC	オフェンス ID **例:** SELECT * FROM events WHERE InOffense(123) SELECT * FROM flows WHERE InOffense(123)
InCIDR	指定された IP/列が、指定された IP/CIDR に含まれるか、これと等しい場合、true を返します。	VARCHAR, OTHER	IP/CIDR、IP アドレス **例:** ...WHERE InCIDR('172.16.0.0/16', sourceip) AND ...
NetworkName	渡された Host について、ネットワーク階層からネットワーク名を検索します。	OTHER	ホスト・プロパティー **例:** NetworkName(sourceip)
RuleName	渡された 1 つ以上のルール ID に基づいて 1 つ以上のルール名を返します。	INTEGER	単一のルール ID、またはルール ID のリスト。 **例:** RuleName(creEventList), RuleName(1033)

表 4. 外部関数 (続き)

名前	説明	引数のタイプ	説明
Long	数値を表すストリングを Long (整数) データ型に解析します。	VARCHAR	数値を表すストリング。 **例:** Long('1234')
Double	数値を表すストリングを Double (整数) データ型に解析します。	VARCHAR	数値を表すストリング。 **例:** Double('1234')
DomainName	ドメイン ID に基づいてドメイン名を検索します。	NUMERIC	ドメイン ID **例:** DomainName(domainID)

論理演算子および比較演算子

論理演算子は、値が同等か異なるかを判別するために AQL ステートメント内で使用されます。AQL ステートメントの WHERE 節で論理演算子を使用することで、返される結果は WHERE 節の条件に一致するものに制限/フィルター処理されます。次の表に、サポートされる演算子をリストします。

表 5. Ariel API の演算子

演算子	情報	例
=	2 つの値を比較し、等しければ true を返します。	...WHERE sourceIP = destinationIP
!=	2 つの値を比較し、等しくなければ true を返します。	...WHERE sourceIP != desintationIP)
(および)	複雑なブール式を作成する場合、括弧を使用して、 WHERE 節または HAVING 節の構成要素をネストします。	...WHERE (sourceIP = destinationIP) AND (sourcePort = destinationPort)
< および <=	2 つの値を比較し、左の値が右の値より小さいか等しければ true を返します。	...WHERE sourceBytes < 64 and destinationBytes <= 64
> および >=	2 つの値を比較し、左の値が右の値より大きいか等しければ true を返します。	...WHERE sourceBytes > 64 and destinationBytes >= 64
*	2 つの値を乗算し、結果を返します。	...WHERE sourceBytes * 1024 < 1
/	2 つの値を除算し、結果を返します。	...WHERE sourceBytes / 8 > 64
+	2 つの値を加算し、結果を返します。	...WHERE sourceBytes + destinationBytes < 64
-	1 つの値をもう一方の値から減算し、結果を返します。	...WHERE sourceBytes - destinationBytes > 0
^	1 つの値を指定し、指定されたべき乗計算を行って結果を返します。	...WHERE sourceBytes ^ 2 < 256
%	値のモジュロを指定し、結果を返します。	...WHERE sourceBytes % 8 == 7

表 5. Ariel API の演算子 (続き)

演算子	情報	例
AND	ステートメントの左側とステートメントの右側を指定し、両方が true の場合に true を返します。	...WHERE (sourceIP = destinationIP) AND (sourcePort = destinationPort)
OR	ステートメントの左側とステートメントの右側を指定し、いずれかが true の場合に true を返します。	...WHERE (sourceIP = destinationIP) または (sourcePort = destinationPort)
NOT	ステートメントを指定し、ステートメントが false に評価された場合に true を返します。	...WHERE NOT (sourceIP = destinationIP)
IS NULL	値を指定し、値が null の場合に true を返します。	...WHERE userName IS NULL
NOT NULL	値を指定し、値が null でない場合に true を返します。	...WHERE userName IS NOT NULL
BETWEEN (X,Y)	左側と 2 つの値を指定し、左側がその 2 つの値の間にある場合に true を返します。	...WHERE magnitude BETWEEN 1 AND 5
LIMIT	結果の数を、指定した数に制限します。	...WHERE magnitude > 5 LIMIT 10
ORDER BY (ASC,DESC)	指定した列で結果セットを並べ替えます。	SELECT * FROM EVENTS ORDER BY sourceIP DESC
COLLATE	BCP47 言語タグで照合できるようにする ORDER BY のパラメーター。	SELECT * FROM EVENTS ORDER BY sourceIP DESC COLLATE 'de-CH'
INTO	別の時間での照会が可能な結果を含む名前付きカーソルを作成します。	SELECT * FROM EVENTS INTO 'MyCursor' WHERE....
START	データの選択を START する時間 (開始時刻) を以下の形式で渡すことができます。 yyyy-MM-dd HH:mm yyyy-MM-dd HH:mm:ss yyyy/MM/dd HH:mm:ss yyyy/MM/dd-HH:mm:ss yyyy:MM:dd-HH:mm:ss タイム・ゾーン は、以下の形式で z または Z により表現されます。 yyyy-MM-dd HH:mm'Z' yyyy-MM-dd HH:mm'z' STOP と組み合わせて使用してください。	例 1 ...WHERE userName IS NULL START '2014-04-25 15:51' STOP '2014-04-25 17:00' 例 1 から返される結果は '2014-04-25 15:51:00' to '2014-04-25 16:59:59' です。 例 2 ...WHERE userName IS NULL START '2014-04-25 15:51:20' STOP '2014-04-25 17:00:20' 例 2 から返される結果は '2014-04-25 15:51:00' to '2014-04-25 17:00:59' です。 PARSEDATETIME 関数では任意の形式を使用できます。以下に例を示します。 Select * from events START PARSEDATETIME('1 hour ago') STOP PARSEDATETIME('now') STOP はオプションです。これを照会に含めない場合、STOP 時刻は now() になります。

表 5. Ariel API の演算子 (続き)

演算子	情報	例
STOP	データの選択を STOP する時間 (終了時刻) を以下の形式で渡すことができます。 yyyy-MM-dd HH:mm yyyy-MM-dd HH:mm:ss yyyy/MM/dd HH:mm:ss yyyy/MM/dd-HH:mm:ss yyyy:MM:dd-HH:mm:ss タイム・ゾーン は、以下の形式で z または Z により表現されます。 yyyy-MM-dd HH:mm'Z' yyyy-MM-dd HH:mm'z' START と組み合わせて使用してください。	...WHERE userName IS NULL START '2014-04-25 14:00' STOP '2014-04-25 16:00' ...WHERE userName IS NULL START '2014-04-25 15:00:30' STOP '2014-04-25 15:02:30' PARSEDATETIME 関数では任意の形式を使用できます。以下に例を示します。 Select * from events START PARSEDATETIME('1 day ago') この照会に STOP は含まれていませんが、STOP 時刻は now() になります。
LAST	データを選択する時間間隔を渡すことができます。有効な間隔は、分、時間、および日です。	...WHERE userName IS NULL LAST 6 HOURS
LIKE	渡されたストリングが、渡された値と LIKE の関係にあるかどうかを照合します。% はワイルドカードです。	...WHERE userName LIKE '%bob%'
ILIKE	大/小文字を区別しない場合に、渡されたストリングが、渡された値と LIKE の関係にあるかどうかを照合します。 % はワイルドカードです。	...WHERE userName ILIKE '%bob%'
MATCHES	ストリングが、指定された正規表現と一致するかどうかを照合します。	...WHERE userName MATCHES '^.bob.$'
IMATCHES	大/小文字を区別しない場合に、ストリングが、指定された正規表現と一致するかどうかを照合します。	...WHERE userName IMATCHES '^.bob.$'

表 5. Ariel API の演算子 (続き)

演算子	情報	例
TEXT SEARCH	渡された値での全文検索。 「TEXT SEARCH」は、AND 演算子とともに使用できます。「TEXT SEARCH」は、OR 演算子および他の演算子とともに使用することはできません。使用した場合は構文エラーが発生します。 TEXT SEARCH は、WHERE 節の最初の位置に配置してください。TEXT SEARCH を WHERE 節の他の位置に配置すると、エラーが発生します。正しい順序を示す WHERE TEXT SEARCH の例を参照してください。 QRadar ユーザー・インターフェースのクイック・フィルターを使用することでも全文検索を実行できます。クイック・フィルターの機能については、「*IBM Security QRadar SIEM ユーザーズ・ガイド*」を参照してください。	...WHERE TEXT SEARCH 'firewall' AND ... SELECT sourceip,url from events WHERE TEXT SEARCH 'download.cdn.mozilla.net' AND sourceip='192.168.1.1' START '2015-01-30 16:10:12' STOP '2015-02-22 17:10:22'

論理演算子および比較演算子の例

- 解析されていないイベントをソートするには、以下の照会を入力します。

```
SELECT * FROM events WHERE payload = 'false'
```

- オフェンスが存在する特定の送信元 IP アドレスを検出するためにイベントをソートするには、以下の照会を入力します。

```
SELECT * FROM events WHERE sourceIP = '231.12.37.17' AND
hasOffense = 'true'
```

- AQL で「**クイック・フィルター**」検索を実行できます。「ファイアウォール」のイベントをソートするには、以下の照会を入力します。

```
SELECT QIDNAME(qid) AS EventName, * from events where TEXT SEARCH 'firewall'
```

AQL 照会のイベント、フロー、および simarc フィールド

Ariel 照会言語 (AQL) を使用して、Ariel データベースのイベント、フロー、および simarc 表から特定のフィールドを取得します。

AQL 照会でサポートされるフロー・フィールド

照会可能なフロー・フィールドを以下の表に示します。

表 6. AQL 照会でサポートされるフロー・フィールド

フィールド名	説明
applicationId	アプリケーション・アイデンティティー
category	カテゴリー
credibility	信頼性
destinationASN	宛先 ASN
destinationBytes	宛先バイト数
destinationDSCP	宛先の DSCP
destinationFlags	宛先のフラグ
destinationIP	宛先 IP
destinationIfIndex	宛先の If 索引
destinationPackets	宛先のパケット数
destinationPayload	宛先のペイロード
destinationPort	宛先ポート
destinationPrecedence	宛先の優先順位
destinationTOS	宛先の QoS
destinationv6	IPv6 宛先
processorID	イベント・プロセッサー ID
fullMatchList	完全一致のリスト
firstPacketTime	最初のパケットの時刻
flowBias	フロー・バイアス
flowDirection	フローの向き **ローカルからローカル (L2L)** **ローカルからリモート (L2R)** **リモートからローカル (R2L)** **リモートからリモート (R2R)**
flowInterfaceID	フロー・インターフェース ID
flowSource	フロー・ソース
flowType	フロー・タイプ
geographic	地理的位置に一致する
hasDestinationPayload	宛先ペイロードあり
hasOffense	オフェンス・ペイロードあり
hasSourcePayload	送信元ペイロードあり
icmpCode	ICMP コード
icmpType	ICMP タイプまたはコード
flowInterface	フロー・インターフェース
intervalId	間隔 ID

表 6. AQL 照会でサポートされるフロー・フィールド (続き)

フィールド名	説明
isDuplicate	重複イベント
lastPacketTime	最後のパケットの時刻
partialMatchList	部分一致のリスト
protocol	プロトコル
protocolId	プロトコル ID
qid	Qid
relevance	関連性
retentionBucket	保存バケットのダミー
severity	重大度
sourceASN	送信元 ASN
sourceBytes	送信元バイト数
sourceDSCP	送信元の DSCP
sourceFlags	送信元のフラグ
sourceIP	送信元 IP
sourceIfIndex	送信元の If 索引
sourcePackets	送信元のパケット数
sourcePayload	送信元のペイロード
sourcePort	送信元ポート
sourcePrecedence	送信元の優先順位
sourcev6	IPv6 送信元
startTime	開始時刻
viewObjectPair	ビュー・オブジェクト・ペア

AQL 照会でサポートされるイベント・フィールド

照会可能なイベント・フィールドを以下の表に示します。

表 7. AQL 照会でサポートされるイベント・フィールド

フィールド名	説明
category	下位カテゴリー
creEventList	一致したカスタム・ルール
credibility	信頼性
destinationMAC	宛先 MAC
destinationPort	宛先ポート
destinationv6	IPv6 宛先
deviceTime	ログ・ソースの時刻
deviceType	ログ・ソース・タイプ
domainID	ドメイン ID **注:** QRadar Log Manager のみ
duration	期間

表 7. AQL 照会でサポートされるイベント・フィールド (続き)

フィールド名	説明
endTime	終了時刻
eventCount	イベント数
eventDirection	イベントの方向: **ローカルからローカル (L2L)** **ローカルからリモート (L2R)** **リモートからローカル (R2L)** **リモートからリモート (R2R)**
processorId	イベント・プロセッサー ID
hasIdentity	アイデンティティーあり
hasOffense	オフェンスとの関連
highLevelCategory	上位カテゴリー
isCREEvent	カスタム・ルール・イベント
magnitude	マグニチュード
payload	ペイロード
postNatDestinationIP	NAT 後の宛先 IP
postNatDestinationPort	NAT 後の宛先ポート
postNatSourceIP	NAT 後の送信元 IP
postNatSourcePort	NAT 後の送信元ポート
preNatDestinationIP	NAT 前の宛先 IP
preNatDestinationPort	NAT 前の宛先ポート
preNatSourceIP	NAT 前の送信元 IP
preNatSourcePort	NAT 前の送信元ポート
protocolID	プロトコル
qid	イベント名 ID
relevance	関連性
severity	重大度
sourceIP	送信元 IP
sourceMAC	送信元 MAC
sourcePort	送信元ポート
sourcev6	IPv6 送信元
startTime	開始時刻
isunparsed	未解析のイベント
userName	ユーザー名

AQL 照会でサポートされる simarc フィールド

照会可能な simarc フィールドを以下の表に示します。

表 8. AQL 照会でサポートされる simarc フィールド

フィールド名	説明
destinationPort	宛先ポート・キー作成者
destinationType	宛先タイプ・キー作成者
deviceId	デバイス・キー作成者
direction	方向キー作成者
eventCount	イベント数キー作成者
eventFlag	フラグ・キー作成者
applicationId	アプリケーション・アイデンティティー・キー作成者
flowCount	フロー数キー作成者
destinationBytes	宛先バイト数キー作成者
flowSource	フロー・ソース・キー作成者
sourceBytes	送信元バイト数キー作成者
lastPacketTime	時刻キー作成者
protocolId	プロトコル・キー作成者
source	送信元キー作成者
sourceType	送信元タイプ・キー作成者
sourceRemoteNetwork	送信元リモート・ネットワーク・キー作成者
destinationRemoteNetwork	宛先リモート・ネットワーク・キー作成者
sourceCountry	送信元地理キー作成者
destinationCountry	宛先地理キー作成者
destination	宛先キー作成者
creEventList	正規化イベント・プロパティー CRE イベント・リスト
partialMatchList	正規化イベント・プロパティー部分一致リスト

SELECT ステートメント

SELECT ステートメントを使用して、Ariel データベース内のイベント表またはフロー表から特定のデータを取得します。SELECT 操作は、*問合せ* と呼ばれます。

構文

```
SELECT selectList
     FROM joinClauses
     [WHERE searchCondition]
     [GROUP BY groupClause]
     [ORDER BY orderClause]
```

使用

SELECT ステートメントには、フロー表またはイベント表から 1 つ以上のフィールドを含めることができます。すべての列を示すには、アスタリスク * を使用します。すべてのフィールド名は大/小文字の区別があります。ただし、 SELECT ステートメントおよび FROM ステートメントでは大/小文字の区別はありません。

AQL 照会に渡される時間設定のオーバーライド

SELECT ステートメントは、時間設定をオーバーライドする arieltime オプションをサポートします。

AQL 照会が評価される期間をユーザーが制限することができます。

START および STOP キーワードを使用することができます。

例:

```
SELECT sourceIP FROM events START '2014-05-02 09:25' stop '2014-05-02 09:30'
```

また、LAST キーワードを使用することもできます。

例:

```
SELECT * FROM events LAST 15 MINUTES
SELECT * FROM events LAST 1 HOUR
SLECT * FROM events LAST 2 DAYS
```

CIDR 範囲を使用する SELECT ステートメントの例

SELECT ステートメントを CIDR ベースの照会で使用することもできます。送信元 IP アドレス sourceIP または宛先 IP アドレス destinationIP で照会するには、以下の形式を使用します。

```
SELECT <query item> FROM <flows|events> WHERE
<sourceCIDR|destinationCIDR> = '<CIDR Range>'
```

例:

```
SELECT * FROM flows WHERE sourceCIDR = '10.100.100/24'
```

10.100.100 サブネットから着信するすべてのフローを返すか、このサブネットから着信するフローとこのサブネットに送信するフローをキャプチャーするには、通常の OR 式を使用します。

例:

```
SELECT * FROM flows WHERE sourceCIDR = '10.100.100/24' OR
destinationCIDR = '10.100.100/24'
```

送信元 IP が 192.168.222.0/24 の範囲に含まれていることについて照会するには、以下の形式を使用します。

```
SELECT <query item> FROM <events> WHERE
<INCIDR> = '<INCIDR Range>'
```

例:

```
SELECT * FROM events WHERE INCIDR('192.168.222.0/24, sourceIP)
```

source IP が 192.168.222.0/24 の範囲に含まれていないことについて照会するには、以下の形式を使用します。

```
SELECT <query item> FROM <events> WHERE
<INCIDR> != '<INCIDR Range>'
```

例:

```
SELECT * FROM events WHERE NOT INCIDR('192.168.222.0/24, sourceIP)
```

WHERE 節

WHERE 節を使用して AQL 照会を制限します。WHERE 節は、照会に適用するフィルター条件を記述し、指定された条件を満たすイベントまたはフローのみ受け入れるように結果のビューをフィルター処理します。

構文

```
WHERE searchCondition
```

searchCondition は、論理演算子および比較演算子の組み合わせです。この組み合わせで 1 つのテストを形成します。テストに合格した入力行のみが結果に含められます。

WHERE 節の例

以下の照会では、カテゴリーから選択された、重大度レベルが 9 より大きいイベントが表示されます。

```
SELECT sourceIP, category, credibility FROM events WHERE
severity > 9 AND category = 5013
```

評価の順序は括弧を使用することで変更できます。括弧で囲んだ検索条件が最初に評価されます。

```
SELECT sourceIP, category, credibility FROM events WHERE
(severity > 9 AND category = 5013) OR (severity < 5 and
credibility > 8)
```

GROUP BY 節

データを集約するには、GROUP BY 節を使用します。集約から意味のある結果を得るために、データ集約は通常、他の列の算術関数と結合されます。

構文

```
GROUP BY groupClause
```

Ariel 照会言語 (AQL) 照会で集約関数を使用して、複数行の情報を要約できます。以下の表に、サポートされる集約関数を示します。

表 9. 集約関数

機能	説明
GROUP BY	1 つ以上の列の集約を作成します。
COUNT	集約内の行の数を返します。
UNIQUECOUNT	集約内の値の固有カウントを返します。

表 9. 集約関数 (続き)

機能	説明
FIRST	集約内の行の最初の項目を返します。
SUM	数値データに対して使用される場合は、値の合計を返します。カテゴリー・データに対して使用される場合は、カテゴリー値の和集合を返します。
AVG	集約内の行の平均値を返します。
MIN(expr)	集約内の行の最も低い値を返します。
MAX(expr)	集約内の行の最も高い値を返します。
HAVING	グループ列の結果について演算子を許可します。

GROUP BY 節の例

以下の照会の例は、特定の時間におけるすべてのフロー内で 100 万バイトを超えるデータを送信した IP アドレスを示しています。

```
select sourceIP, SUM(sourceBytes) from flows where sourceBytes >
1000000 group by sourceIP
```

結果は以下の出力と同様になります。

```
----------------------------------
| sourceIP | SUM_sourceBytes |
----------------------------------
| 64.124.201.151 | 4282590.0 |
| 10.105.2.10 | 4902509.0 |
| 10.103.70.243 | 2802715.0 |
| 10.103.77.143 | 3313370.0 |
| 10.105.32.29 | 2467183.0 |
| 10.105.96.148 | 8325356.0 |
| 10.103.73.206 | 1629768.0 |
----------------------------------
```

ただし、この情報を非集約照会と比較した場合、以下の出力に示すように、すべての IP アドレスは一意的に表示されます。

```
------------------------------
| sourceIP | sourceBytes |
------------------------------
| 64.124.201.151 | 1448629 |
| 10.105.2.10 | 2412426 |
| 10.103.70.243 | 1793095 |
| 10.103.77.143 | 1449148 |
| 10.105.32.29 | 1097523 |
| 10.105.96.148 | 4096834 |
| 64.124.201.151 | 2833961 |
| 10.105.2.10 | 2490083 |
| 10.103.73.206 | 1629768 |
| 10.103.70.243 | 1009620 |
| 10.105.32.29 | 1369660 |
| 10.103.77.143 | 1864222 |
| 10.105.96.148 | 4228522 |
------------------------------
```

最大イベント数を表示するには、以下の構文を使用します。

```
SELECT MAX(eventCount) FROM events
```

送信元 IP からの平均イベント数を表示するには、以下の構文を使用します。

```
SELECT AVG(eventCount) FROM events GROUP BY sourceIP
```

出力に、以下の結果が表示されます。

```
---------------------------------
| sourceIP | protocol |
---------------------------------
| 64.124.201.151 | TCP.tcp.ip |
| 10.105.2.10 | UDP.udp.ip |
| 10.103.70.243 | UDP.udp.ip |
| 10.103.77.143 | UDP.udp.ip |
| 10.105.32.29 | TCP.tcp.ip |
| 10.105.96.148 | TCP.tcp.ip |
| 64.124.201.151 | TCP.tcp.ip |
| 10.105.2.10 | ICMP.icmp.ip |
---------------------------------
```

ORDER BY 節

ORDER BY 節を使用して、式の結果に基づいて得られたビューをソートします。ソート順は昇順または降順です。

構文

```
ORDER BY orderClause
```

ORDER BY 節では 1 つのフィールドのみ使用できます。ORDER BY 節に ASC または DESC キーワードを追加することによって、ソートを昇順または降順に切り換えることができます。

GROUP BY 節と ORDER BY 節の組み合わせによるデータの作成

上位の異常イベントまたは帯域幅を最も多く消費する IP アドレスを判別するために、GROUP BY 節と ORDER BY 節を単一の照会で組み合わせることができます。これらの節を組み合わせて、上位 N リストなどのデータを作成します。例えば、以下の照会は、トラフィックが最も多い IP アドレスを降順に表示します。

```
SELECT sourceIP, SUM(sourceBytes) FROM flows GROUP sourceIP
ORDER BY SUM(sourceBytes) DESC
```

ORDER BY 節の例

結果を降順で返すように AQL を照会するには、以下の構文を使用します。

```
SELECT sourceBytes, sourceIP FROM flows WHERE sourceBytes >
1000000 ORDER BY sourceBytes
```

結果を昇順に表示するには、以下の構文を使用します。

```
SELECT sourceBytes, sourceIP FROM flows WHERE sourceBytes >
1000000 ORDER BY sourceBytes ASC
```

LIKE 節

LIKE 節を使用して、Ariel データベース内で部分的なストリングの一致を取得します。

構文

```
ORDER BY orderClause
```

LIKE 節を使用してフィールドを検索することができます。

Ariel 照会言語 (AQL) では、以下のワイルドカード・オプションがサポートされます。

表 10. LIKE 節でサポートされるワイルドカード・オプション

ワイルドカード文字	説明
%	ゼロ以上の文字のストリングの照合を行います。
_	任意の単一文字の照合を行います。

LIKE 節の例

Joe、Joanne、Joseph など、Jo で始まるすべての名前を照合するには、以下の照会を入力します。

```
SELECT * FROM events WHERE userName LIKE 'jo%'
```

Jo で始まり、Joe、Jon などの 3 文字の長さの名前を照合するには、以下の照会を入力します。

```
SELECT * FROM events WHERE userName LIKE 'Jo_'
```

以下の例のように、コマンドのあらゆる場所でワイルドカード・オプションを入力することができます。

```
SELECT * FROM flows WHERE sourcePayload LIKE '%xyz'
SELECT * FROM events WHERE payload LIKE '%xyz%'
SELECT * FROM events WHERE payload LIKE '_yz'
```

ストリングの突き合わせキーワードの例

キーワード ILIKE および IMATCHES は、LIKE および MATCHES の大/小文字を区別しないバージョンです。

```
SELECT qidname(qid) as test FROM events WHERE test LIKE 'Information%'
SELECT qidname(qid) as test FROM events WHERE test ILIKE 'inForMatiOn%'

SELECT qidname(qid) as test FROM events WHERE test MATCHES '.*Information.*'
SELECT qidname(qid) as test FROM events WHERE test IMATCHES '.*Information.*'
```

COUNT 関数

COUNT 関数は、SELECT 文の WHERE 節を満たす行数を返します。

SELECT 文に WHERE 節が指定されていない場合、COUNT 関数により、表に含まれる行の総数が返されます。

構文

```
COUNT
```

例

信頼性が 9 以上のすべてのイベントをカウントするには、以下の照会を入力します。

```
SELECT COUNT() FROM events WHERE credibility >= 9
```

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資 料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

IBM、IBM ロゴおよび ibm.com® は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

以下は、それぞれ各社の商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

このソフトウェア・オファリングは、展開される構成に応じて、セッション管理および認証の目的のために、それぞれのお客様のセッション ID を、セッションごとの Cookie を使用して収集する場合があります。これらの Cookie は無効にできますが、その場合、これらを有効にした場合の機能を活用することはできません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、 お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』および『IBM Software Products and Software-as-a-Service Privacy Statement』(http://www.ibm.com/software/info/product-privacy) を参照してください。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。