IBM Security QRadar Incident Forensics
バージョン 7.2.8

IBM QRadar Network Packet Capture API ガイド

注記

本書および本書で紹介する製品をご使用になる前に、 9 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。

本書は、本書の更新版に置き換えられない限り、IBM QRadar Security Intelligence Platform V7.2.8 および以降のリリースに適用されます。

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 Incident Forensics
Version 7.2.8
IBM QRadar Network Packet Capture API 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

QRadar Network Packet Capture API の概要

本書では IBM® QRadar® Network Packet Capture の RESTful API について説明します。

対象読者

このガイドは、コーディングの経験がある開発者を対象としています。このガイドは、QRadar へのアクセス権限とご使用の企業ネットワークとネットワーキング・テクノロジーに関する知識をお持ちの方を想定して記述されています。

テクニカル・ドキュメント

QRadar 製品ライブラリーで IBM Security QRadar 製品資料を見つけるには、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。

お客様サポートへのお問い合わせ

お客様サポートへのお問い合わせ方法については、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、企業の内部と外部からの不正なアクセスの防止、検出、対応により、システムと情報を保護する必要があります。不正なアクセスにより、情報の改ざん、破壊、盗用、悪用が発生したり、使用しているシステムの損傷や、他のシステムに対する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。

第 1 章 RESTful API の概要

IBM QRadar Network Packet Capture の REST API には、プログラムでパケット・キャプチャー・データを処理するための方法が用意されています。この API は REST アーキテクチャーに準拠しています。

現在の API バージョンは 1.0 です。

開発者が REST API の対話式資料を使用して情報を入力して「テスト」をクリックすると、適切にフォーマットされた HTTPS URL、応答、GET ヘッダー、エラー、スキーマ情報、および PUT、GET、POST、または DELETE の各コマンドの詳細情報を取得できます。

対話式 API 資料ページへのアクセス

対話式 API 資料ページを使用して、RESTful API の技術的詳細を参照したり、ご使用のサーバーへの API 要求の実行をテストしたりします。

手順

1. 対話式 API 資料にアクセスするには、Web ブラウザーで `https://<IP アドレス>/api/` という URL を入力します。QRadar Network Packet Capture アプライアンスの *<IP アドレス>* を使用してください。
2. アクセスするエンドポイントに移動します。
3. エンドポイントの資料を参照して、要求のパラメーターを入力します。
4. 「試用」をクリックします。これにより、コンソールに API 要求が送信され、適切な形式の HTTPS 応答が得られます。

第 2 章 cURL の例

IBM QRadar Network Packet Capture の REST API を照会するには **cURL** コマンド・ライン・ツールを使用します。

アプライアンスに関するアイデンティティー情報の取得

以下の例は Linux で実行します。

この例では、/1/self REST endpoint に対する **HTTP GET** を発行して、QRadar Network Packet Capture アプライアンスに関する識別情報を取得します。

```
$ curl -k https://<IP_address>:443/1/self
> {
   "uuid": "4c4c4544-0032-3210-804c-c7c04f4a3332",
   "version": "1.0.0",
   "type": "QRadar Network Packet Capture",
   "location": "New York",
   "fqdn": "ibm.example.com"
}
```

-k オプションを使用するときは、**cURL** の組み込みの認証局に対する HTTPS 接続に使用する SSL 証明書が使用されません。QRadar Network Packet Capture アプライアンスに付属する SSL 鍵は既知の認証局によって署名されていません。API を通じて、ユーザー自身の鍵および証明書をアップロードできます。この例では認証が不要です。出力は QRadar Network Packet Capture アプライアンスの連絡先情報、バージョン、ロケーション、および UUID です。

管理特権が必要なアカウントのリスト

管理特権が必要な QRadar Network Packet Capture アプライアンスのアカウントをリストするには、GET /1/accounts という REST エンドポイント要求を実行します。

```
$ curl -k https://admin:ibm@<IP_address>:443/1/accounts
> {
   "accounts": {
     "admin": {
       "password":"d28ef5d0e38a783662e74eda9fd2df316846585484",
       "level": "admin"
     }
   }
}
```

出力は QRadar Network Packet Capture アプライアンスに存在するアカウントのリストです。ユーザー名およびパスワードは **cURL** によって HTTPS ヘッダーで送信されます。

詳細コマンドを使用した詳細情報の取得

ご使用の端末と QRadar Network Packet Capture アプライアンスの間で送受信される cURL コマンドの詳細を表示させる場合は、以下のように -v フラグを追加します。

```
$ curl -vk https://admin:pandion@<IP_address>:443/1/accounts
```

最初の例では、QRadar Network Packet Capture アプライアンスの UUID が取得されています。UUID は、他の多くの QRadar Network Packet Capture REST API 呼び出しで使用します。

ロケーションおよび連絡先のオプションの設定

REST API を通じてロケーションおよび連絡先のオプションを構成するには、`POST /1/configuration/` 要求を実行します。

```
$ curl -X POST -H "Accept: Application/json" ¥
           -H "Content-Type: application/json" ¥
           -d '{ ¥
                    "general": { ¥
                      "location": "New York", ¥
                      "contact": "info@ibm.com" ¥
                    } \
                  }' ¥
           -k https://admin:ibm@localhost:443¥
                  /1/configure/4c4c4544-0032-3210-804c-c7c04f4a8149
> {
    "success": "Configuration applied"
}
```

この例の UUID は、必ず自身の QRadar Network Packet Capture アプライアンスの UUID で置き換えてください。QRadar Network Packet Capture アプライアンスの UUID は、ほとんどの API エンドポイントで必要になるほか、API 呼び出しをグループの他のメンバーに転送するためにも使用します。

ヘッダーの送信

REST API エンドポイントがアプリケーションおよび json のデータを取り込んだり生成したりするときに、HTTP ヘッダーを送信するために -H が設定されます。

前記の例では、JSON オブジェクトを使用して `/1/configure/` エンドポイントに対する POST 要求を実行しています。

```
{"general": {"location": "New York",
             "contact": info@ibm.com
            }
}
```

第 3 章 HTTPLIB を使用した Python の例

IBM QRadar Network Packet Capture の REST API を照会するには Python を使用します。

前提条件

Python バージョン 2.7.9 以降をインストールしておく必要があります。

アプライアンスに関するアイデンティティー情報の取得

```
GET /1/me
```

以下の例では、基本ライブラリーをインポートし、セキュア接続を作成し、認証を要求し、ID 要求を実行します。許可ヘッダーおよび結果は標準出力に出力されます。以下の例における QRadar Network Packet Capture アプライアンスの IP アドレスは、いずれも 10.10.10.11 です。

```
import httplib
import base64
import ssl

conn = httplib.HTTPSConnection('10.10.10.11', 443)
conn._context.check_hostname = False
conn._context.verify_mode = ssl.CERT_NONE

headers = {}
headers['Authorization'] = ¥
    "Basic %s" % base64.standard_b64encode("admin:ibm")

req = conn.request('GET', '/1/me', headers=headers)
res = conn.getresponse()

print res.read()
```

表 *1.* インポートする基本ライブラリーのリスト。

ライブラリー名	説明
httplib	基本的な HTTP 接続に使用
base64	基本 HTTP 許可が Base64 エンコードされているため
ssl	SSL 証明書の信頼性を検査しないように HTTPLIB に指示する必要があるため

この例では、インポートした HTTPSConnection モジュールを使用してセキュア HTTPS 接続を作成します。この接続は、QRadar Network Packet Capture アプライアンスの REST API インターフェースの IP アドレスおよびポートを指します。

HTTPS 要求の許可ヘッダーは base64 という Python モジュールを使用して作成します。このヘッダーを使用してユーザー名およびパスワードを送信します。

この許可ヘッダーを使用して `/1/me API` の呼び出しを実行し、結果を読み取ります。

ロケーション情報および連絡先情報の構成

```
POST /1/configure
```

以下の例では、POST /1/configure という REST API エンドポイントを使用して QRadar Network Packet Capture アプライアンスのロケーション情報および連絡先情報を構成します。

```
import httplib
import base64
import ssl
import json

# Create SSL connection while certificates are ignored
conn = httplib.HTTPSConnection("10.10.10.11", 443)
conn._context.check_hostname = False conn._context.verify_mode = ssl.CERT_NONE

# HTTP headers
headers = {'Authorization':
           "Basic %s" % base64.standard_b64encode(
               "admin:ibm"),
           'Accept': "application/json",
           'Content-Type': "application/json"}

# Configuration to be sent to ibm
config_post = {'general':
               {'location': 'New York',
                'contact': 'info@ibm.com'
               }
              }

# Get the UUID (required for POST to /1/configure)
conn.request('GET', '/1/self', headers=headers)
res = conn.getresponse()
assert(res.status == 200)

resp = json.loads(res.read())
uuid = resp['uuid']

# Post the new configuration to ibm
conn.request('POST', '/1/configure/%s' % uuid,
             headers=headers, body=json.dumps(config_post))
res = conn.getresponse()
assert(res.status == 200)

print res.read()
```

必要なライブラリーをインポートした後、REST API を通じて QRadar Network Packet Capture アプライアンスと通信するために必要なセキュア接続 (HTTPSConnection) を作成します。

HTTP ヘッダーを作成します。Authorization は、管理者のユーザー名およびパスワード資格情報を指定するために必要です。また、POST する Content-Type が JSON であることを QRadar Network Packet Capture アプライアンスに指定する必要もあります。さもなければ、QRadar Network Packet Capture REST エンドポイントで要求が拒否されます。

最初の conn.request 要求で QRadar Network Packet Capture アプライアンスの UUID を取得します。UUID は、/1/configure の REST API 呼び出しを完了するために必要です。この UUID は変数 *uuid* に格納します。

この UUID を使用して、/1/configure エンドポイントに対する POST 要求を作成できます。json.dumps 関数を使用して、config_post という JSON オブジェクトを config_post という Python 辞書からテキスト表現に変換して送信します。最後に、この要求を HTTP POST 要求の本体 (コンテンツ) として送信します。

POST からの応答を、HTTPSConnection オブジェクトを通じて読み取って画面に表示します。QRadar Network Packet Capture アプライアンスの連絡先情報およびロケーション情報が正常に変更されたことが応答によって示されます。

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

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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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。

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。

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。

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。

製品資料に関するご使用条件

これらの資料は、以下のご使用条件に同意していただける場合に限りご使用いただけます。

適用度

IBM Web サイトの「ご利用条件」に加えて、以下のご使用条件が適用されます。

個人使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

権限

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入 関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、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なしで提供されます。

IBM オンラインでのプライバシー・ステートメント

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。

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21