自動DDoS Mitigationサービス

2023年5月29日
国立情報学研究所

自動DDoS Mitigationサービス

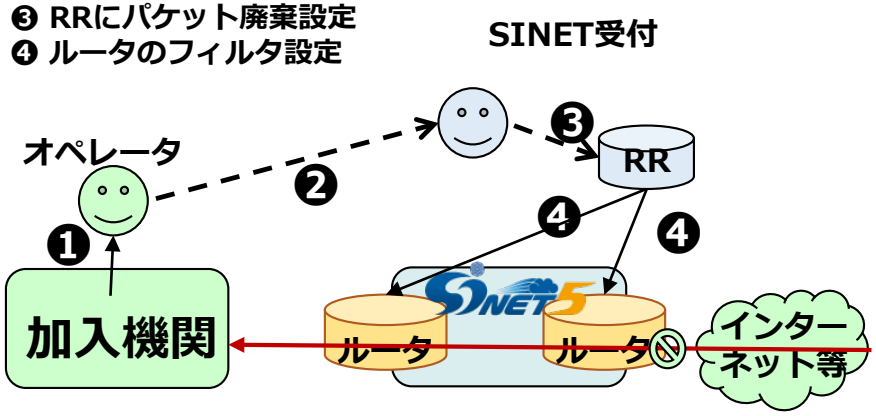
- DDoS攻撃を自動的に検出・防御を行うための新サービスの提供を開始
  - 2023年1月より正式サービスとして運用を開始
  - SINET内にDDoS攻撃検知機能を配備
  - サービス申請に基づき検知対象IPアドレスを設定
  - DDoS攻撃をリアルタイムに検出・アラートを発出
    - 検知後10秒程度でパケットフィルタを自動設定（後日提供予定）

NEW！

従来のDDoSミティゲーションサービス

申し込みから廃棄設定完了まで数時間以上

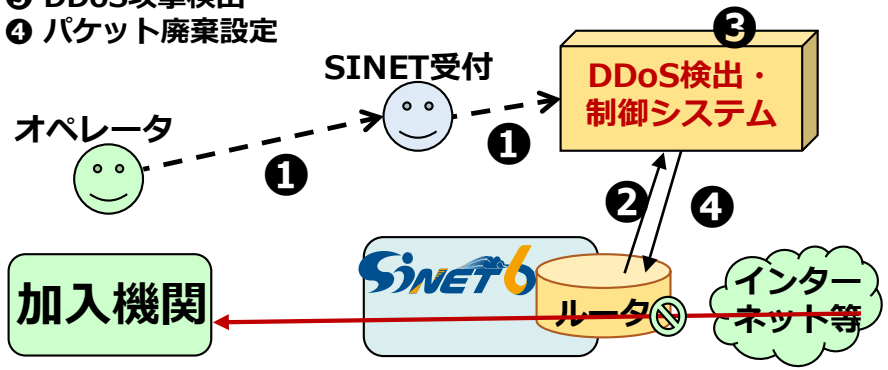
❶ DDoS検出
❷ ミティゲーション申請
❸ RRにパケット廃棄設定
❹ ルータのフィルタ設定



自動DDoS Mitigationサービス

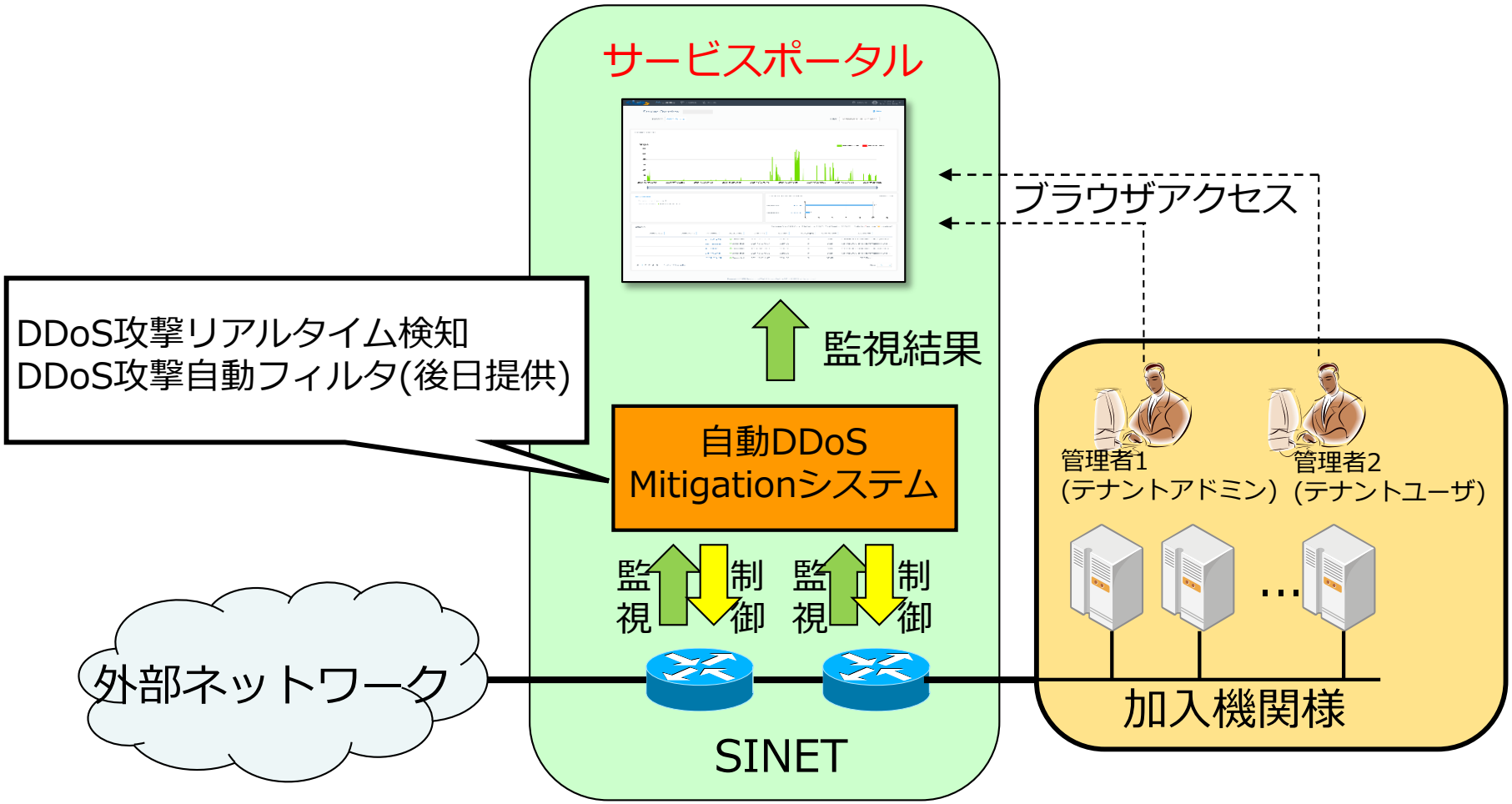
検出から廃棄設定完了まで10秒程度

❶ サービス申請（DDoS対象アドレス登録）
❷ 情報収集
❸ DDoS攻撃検出
❹ パケット廃棄設定



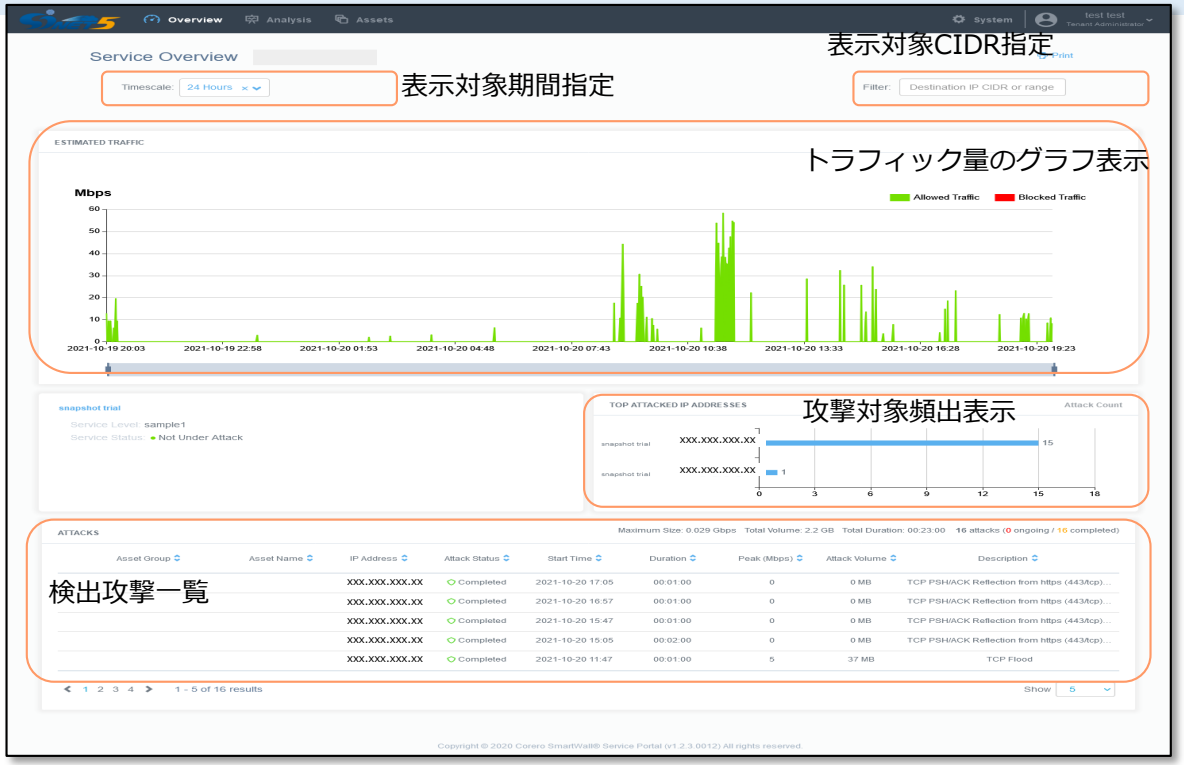
攻撃検知結果の確認について

- **サービスポータルにアクセスすることで、自動DDoS Mitigationサービスによる攻撃検知結果をお手元のブラウザにてリアルタイムにご確認いただけます**



ポータルサイトで確認できる情報

- トラフィック量のグラフ表示
  - 加入機関様ネットワークに入力するトラフィック量の時間推移グラフを表示
  - 破棄したDDoS攻撃トラフィック量のグラフ表示も対応
- 攻撃対象IPアドレス頻出表示
  - 加入機関様ネットワークで攻撃対象となったIPアドレスの頻出ランキングを表示
- 検出攻撃一覧
  - 加入機関様ネットワークに対する攻撃検知の一覧を表示
    - 攻撃対象IPアドレス、検知期間、検知トラフィック量等

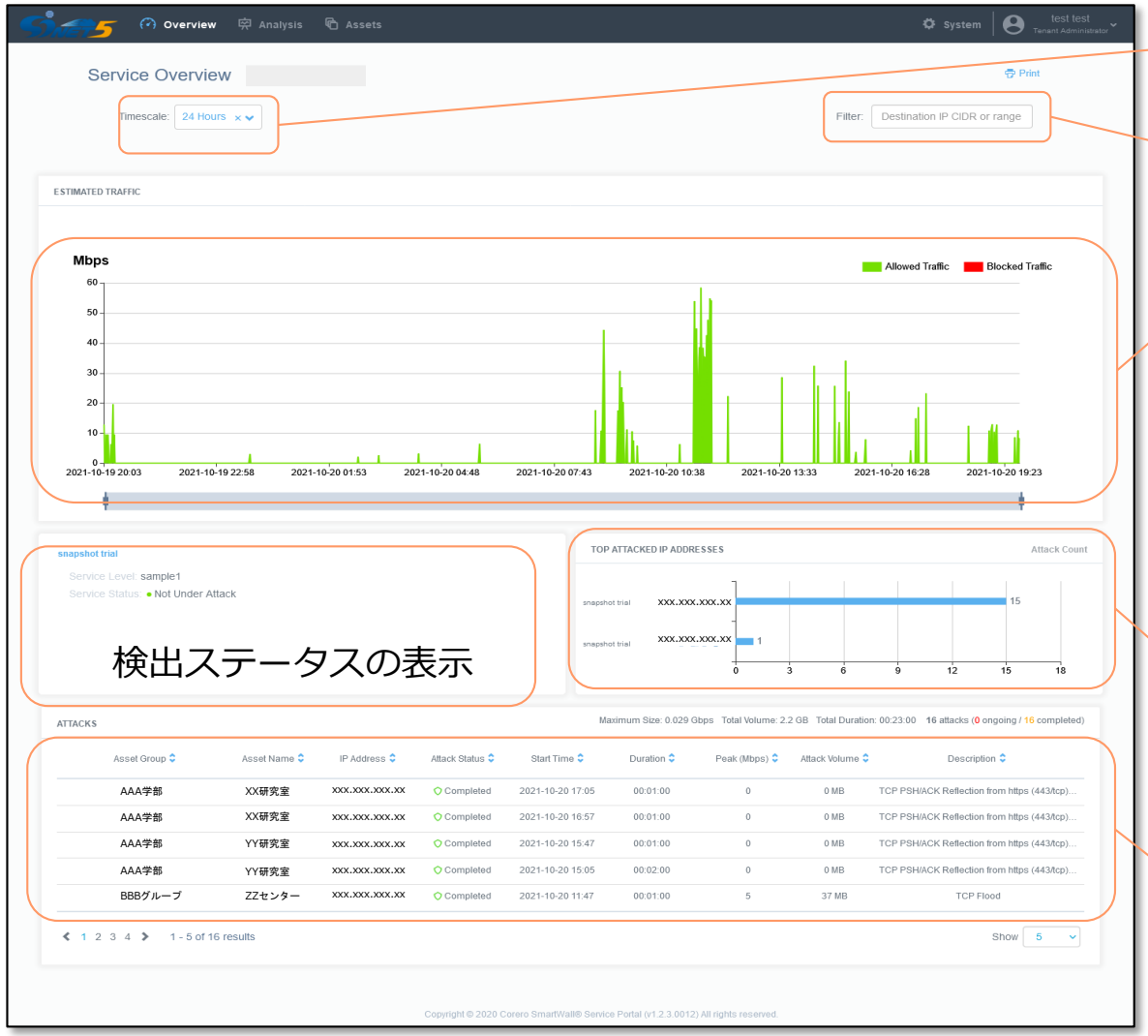


- ブラウザ表示
- メールレポート機能
- ログインユーザ管理

検出攻撃毎のグラフ表示

概要画面 (Overview)

- トラフィックグラフ、攻撃検知一覧を閲覧できます



日時指定(From,To)で
表示期間絞り込み可能
(※デフォルトは直近24時間指定)

CIDRで表示対象絞り込み可能

加入期間様登録CIDRの
トラフィックボリュームグラフ表示

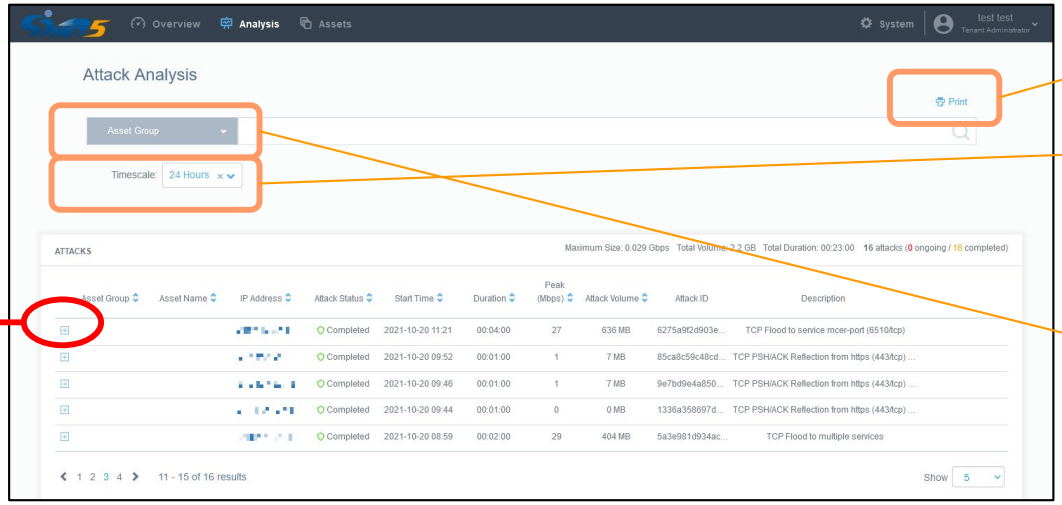
自動遮断(※)中の
攻撃トラフィックボリュームも
表示可能
(※自動遮断制御は後日提供予定)

攻撃ターゲットIPアドレスと
その検出数ランキング表示

検出攻撃一覧
(ターゲットIPアドレス,
発生日時,検出理由等)
項目名クリックにより
当該項目のソートが可能

分析画面 (Analysis)

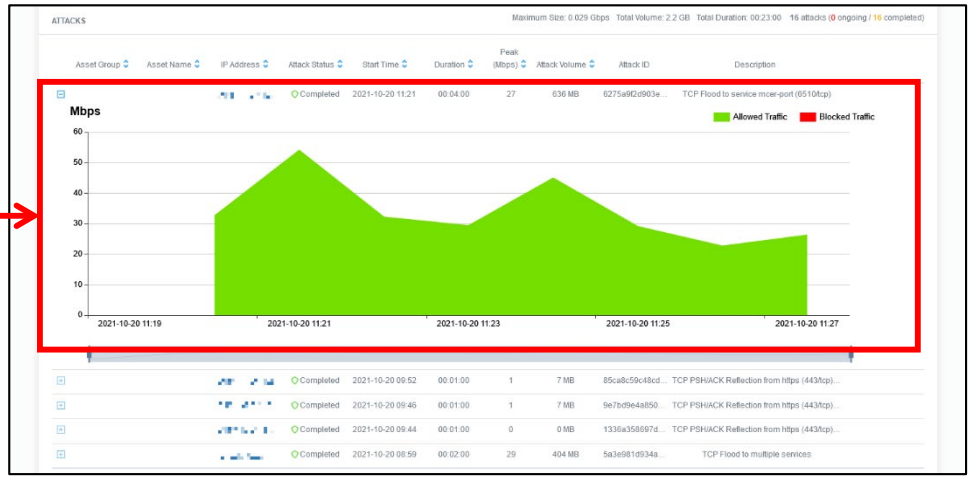
- 検知された攻撃の一覧を閲覧できます
- 攻撃トラフィック個々についてトラフィックグラフを閲覧できます



ブラウザ機能による印刷を実行

攻撃検知結果の表示期間絞り込み
（デフォルトは直近24時間指定）

攻撃一覧から「＋」アイコンをマウスクリックでトラフィックグラフ表示



攻撃検知結果絞り込み

・IPアドレス
　攻撃ターゲットとなったIPアドレス
・Attack ID
　システムが自動付与する攻撃識別用のID
・Asset Name
　加入機関様にて定義したサブネット名称
・Asset Group
　加入機関様にて定義したサブネットグループ名称

攻撃検出一覧について

- **ご登録いただいたIPアドレス帯に対する攻撃情報を抽出しリスト化**
  ①攻撃対象となった加入機関様IPアドレス
  ②攻撃概要（TCP PSH/ACK Flood, UDP Reflection等）
  ③攻撃対象となった加入機関様サービス（プロトコル、ポート番号等）

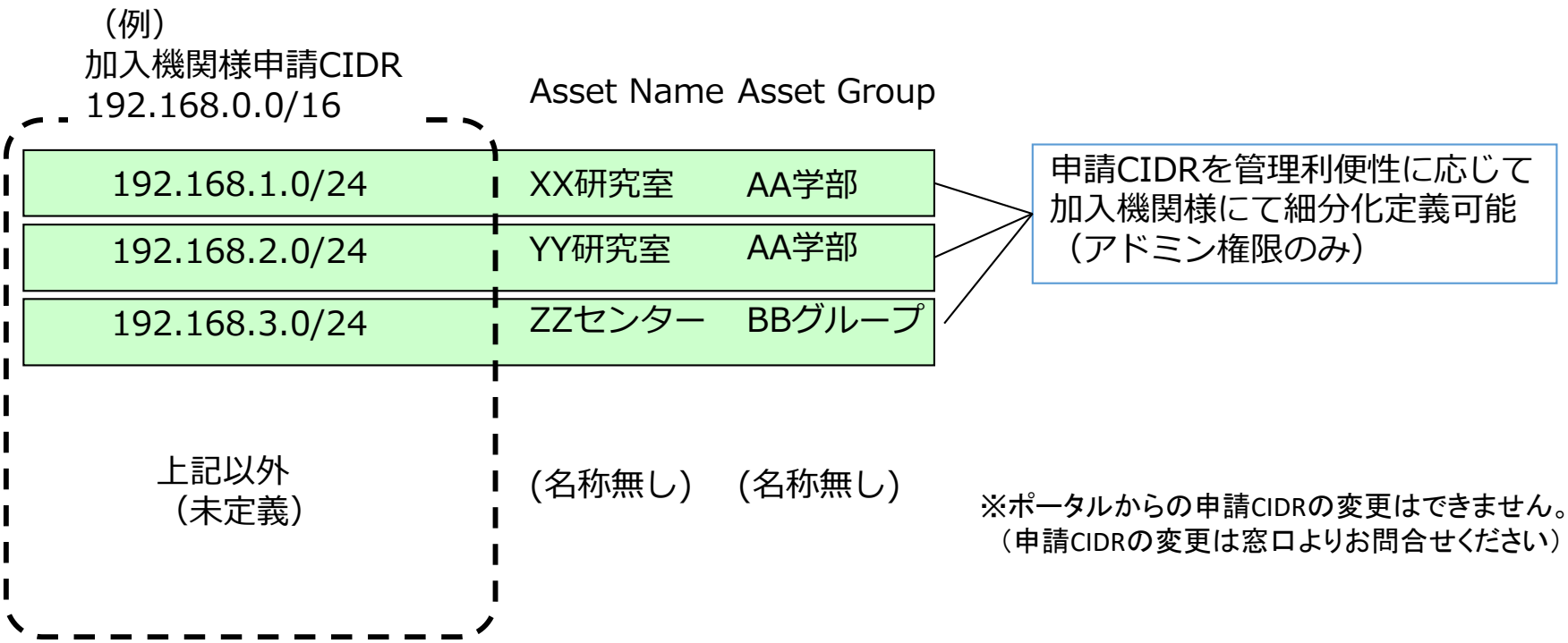
所属サブネットグループ名（Asset Group）	所属サブネット名（Asset Name）	対象IP（Target IP）	ステータス（Attack Status）	攻撃開始時（Start time）	攻撃期間（Duration）	攻撃ピーク[Mbps]（Peak）	攻撃総量（Attack Volume）	攻撃情報（Description）
AAA学部	XX研究室	130.xx.xx.xx	Ongoing	06/15/21 14:25:38	00:02:00	9	74MB	UDP Reflection from https (443/udp) to service 56xxx 57xxx
BBBグループ	ZZセンター	130.xx.xx.xx	Completed	06/15/21 11:10:05	00:01:00	8	60MB	TCP PSH/ACK Flood to service http-alt (8080/tcp)

1 2 3

加入機関様にて監視対象CIDR名称（Asset Name）、同グループ名称（Asset Group）を定義されている場合、識別、ソート、検索の利便性のため攻撃対象IPが所属するCIDR名とCIDRグループ名で表示できます。

監視対象CIDR管理 (Assets)

- **本システムによる監視対象CIDRの名称管理機能です**
- **加入機関様からの事前申請いただいたネットワークアドレスを更に細分化して、名称をつけて管理、グループ管理することができます**
- **OverviewまたはAnalysis画面にて、攻撃対象IPアドレスが属するネットワークセグメントを定義した名称での表示・ソートが可能となります**
  - **Analysis画面では検索も可能です**



おわりに (FAQ)

- **当サービスの利用による通信遅延の影響はありますか？**
  - 当サービスの導入および提供においては通信遅延の増大や転送速度の低下などの影響が無いことを確認して進めてきておりますが、 これまでにそのような影響の発生は確認されておりません。
- **ドロップ（パケットフィルタ）機能の提供開始時期はいつですか？**
  - 大変申し訳ございませんが鋭意準備中です。
    準備が整い次第SINET Webページにてご案内いたします。
- **SINET利用機関であれば無償で利用可能ですか？**
  - はい、無償にてご利用いただけます。

- **ご利用にあたって**
  - 本サービスはIPv4/IPv6 dualサービスを利用されている機関様向けサービスです
  - 利用申請にあたっては，加入機関内の合意を得た上で、機関の長、最高情報システム責任者または最高情報セキュリティ責任者の承諾を得た上でご申請ください

自動DDoS Mitigationサービスをぜひご利用ください！

共考共創

ご清聴ありがとうございました！