自動DDoS Mitigationサービス

北川 直哉

国立情報学研究所

自動DDoS Mitigationサービス

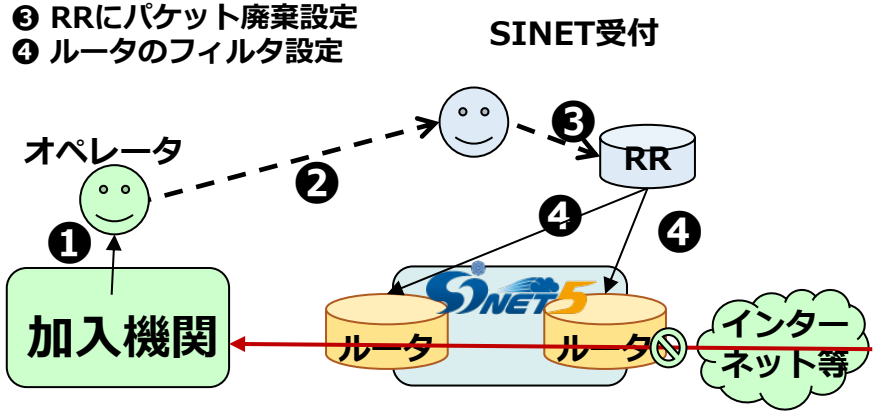
- DDoS攻撃を自動的に検出・防御を行うための新サービスの提供を開始
  - 2023年1月より正式サービスとして運用を開始
  - SINET内にDDoS攻撃検知機能を配備
  - 事前にサービス申請に基づき検知対象IPアドレスを設定
  - DDoS攻撃をリアルタイムに検出・アラートを発出
    - 検知後10秒程度でパケットフィルタを自動設定（2023年11月より提供開始）

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

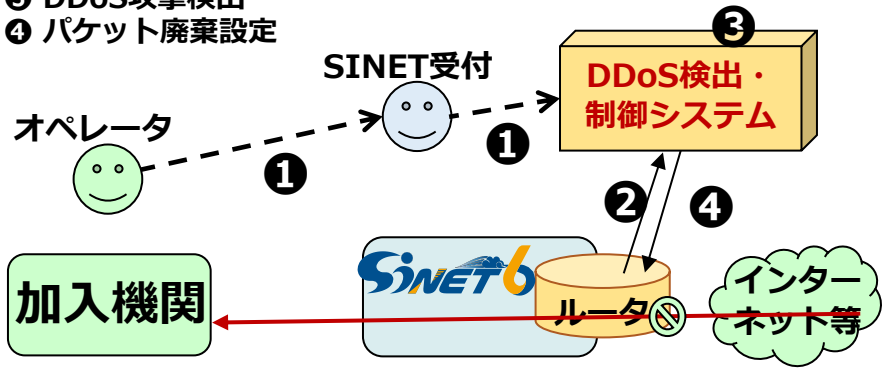
❶ DDoS検出
❷ ミティゲーション申請
❸ RRにパケット廃棄設定
❹ ルータのフィルタ設定



自動DDoS Mitigationサービス

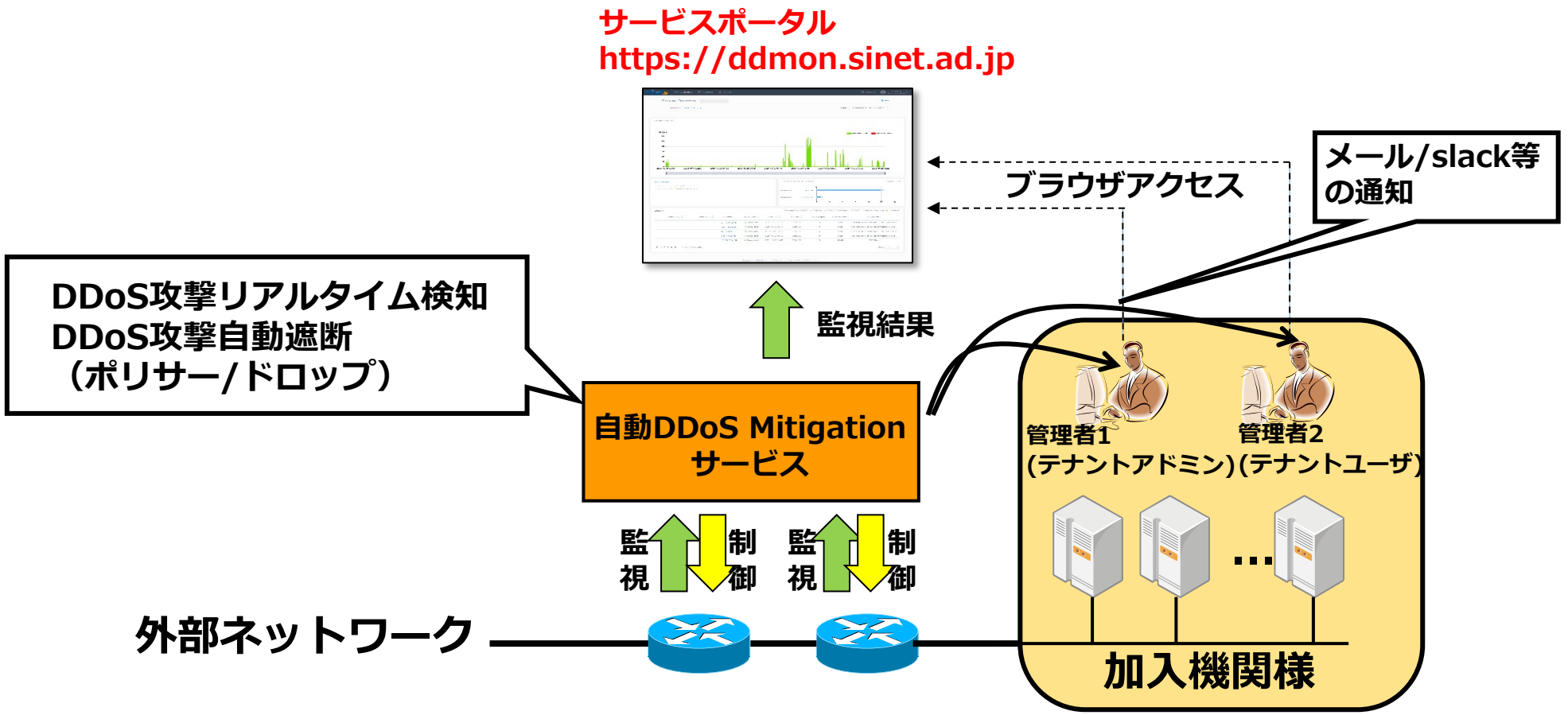
検出から廃棄設定完了まで10秒程度

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



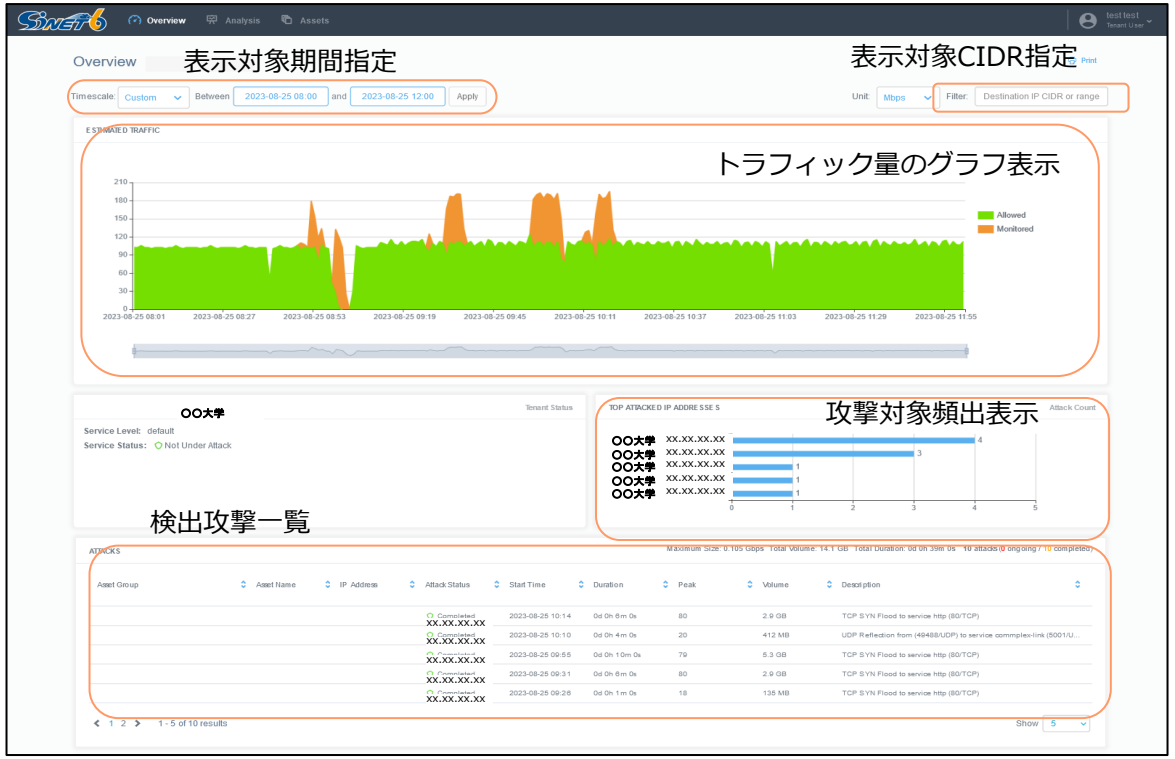
システム概要

- SINETが提供する自動DDoS Mitigationサービスによる攻撃検知結果を、ブラウザにてリアルタイムに確認いただくことが可能です



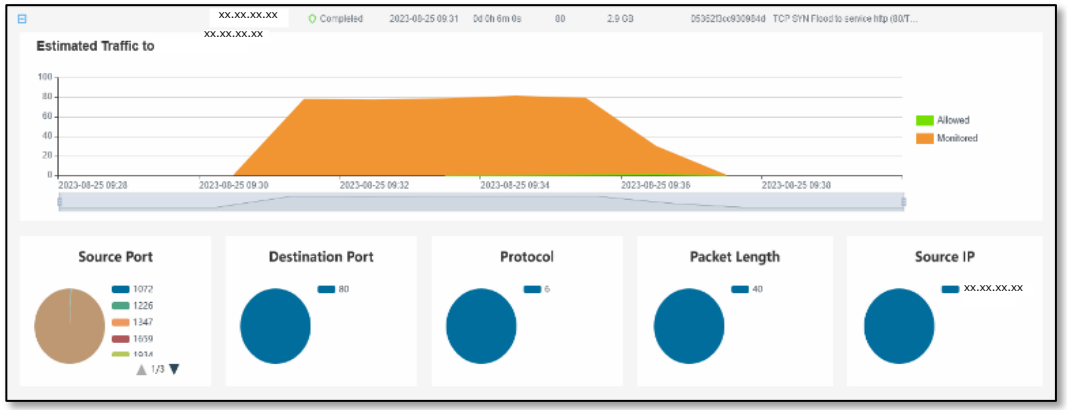
ポータルサイトで確認できる情報

- 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
  - 検知したDDoS攻撃トラフィック量、遮断したトラフィック量のグラフを表示
- 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



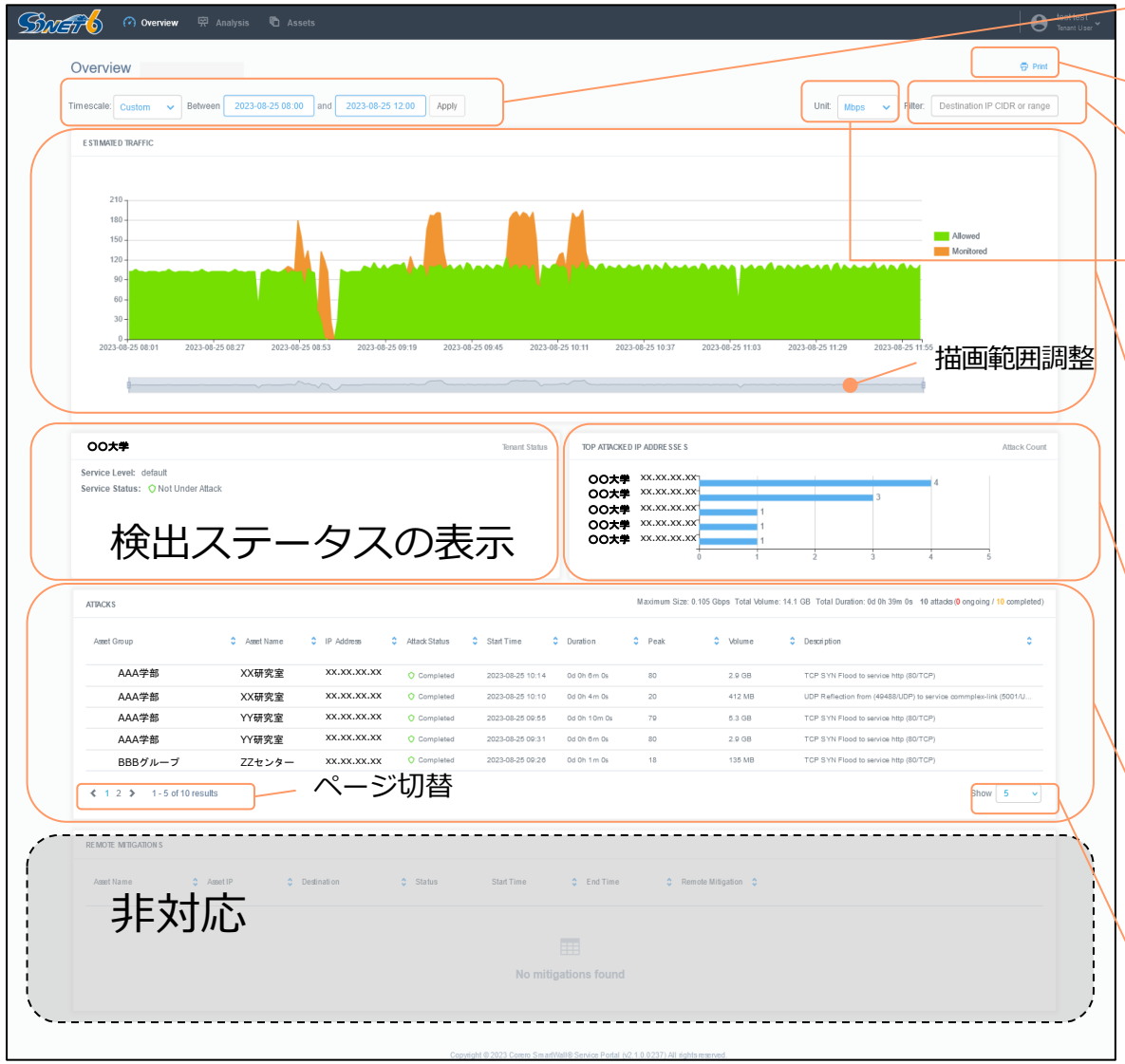
- ブラウザ表示
- メールレポート機能（一部提供中）
- Slack, Microsoft teams 連携機能
- ログインユーザ管理

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、攻撃検知一覧を表示**



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)

ブラウザ機能による印刷

CIDRで表示対象絞り込み可能

グラフ表記切替(bps/pps)

加入機関様登録CIDRのトラフィックボリュームグラフ
・通常トラフィック
・攻撃検知トラフィック（遮断なし）
・攻撃検知トラフィック（遮断あり）

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

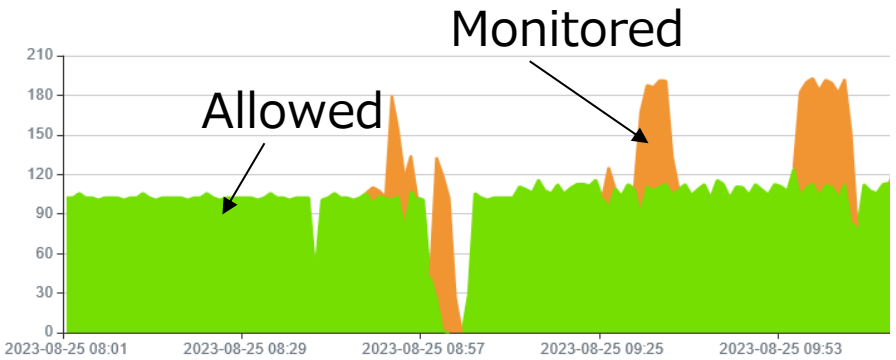
検出攻撃一覧
(ターゲットIP,発生日時,検出理由等)
項目名クリックにより当該項目のソートが可能

表示数選択/ページ

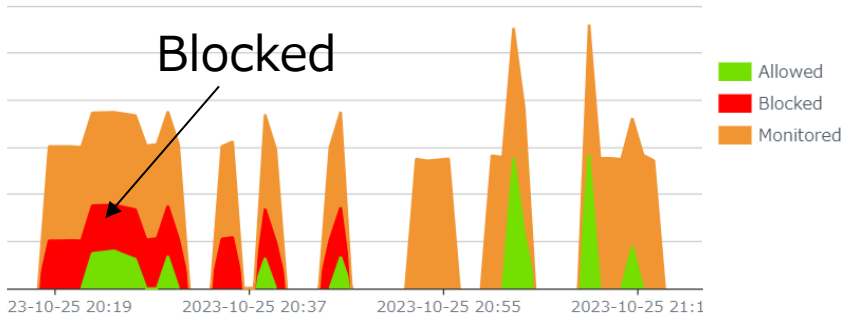
概要画面(Overview)グラフ表示

- **トラフィックグラフの表示色の違いにより攻撃検知結果を示します**

（緑）	**Allowed**	攻撃とみなされなかった通常トラフィックのボリューム
（橙）	**Monitored**	攻撃とみなされた被疑トラフィック（遮断せず通過状態を維持）のボリューム
（赤）	**Blocked**	攻撃とみなされた被疑トラフィック（本システムにより遮断中）のボリューム



・・・



新バージョン(2023/9/08以降)は旧バージョンとグラフの見え方が異なりますのでご注意ください

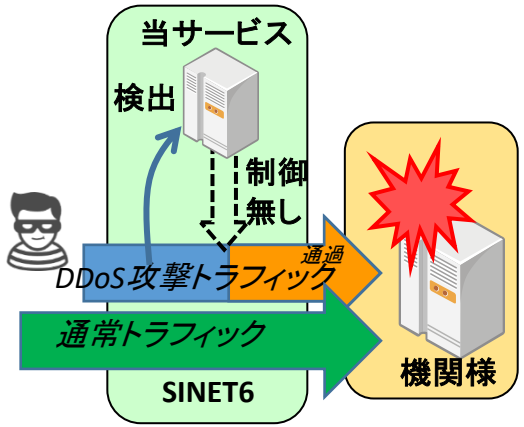
（旧バージョンでは攻撃検知有無にかかわらずAllowed(緑)表示されていたものが新バージョンではAllowed/Monitoredで明示的に区別）

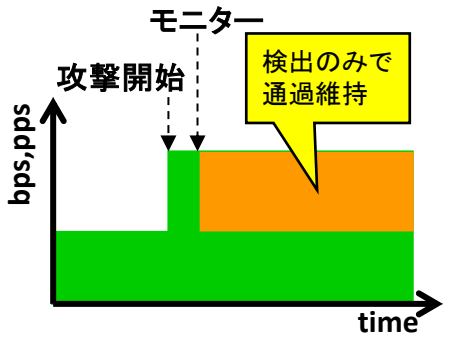
	旧バージョンでの見え方 (2023/9/07以前)	新バージョンでの見え方 (2023/9/08以降)	ドロップ/ポリサー機能 提供以降(2023/11/01以降)
通常トラフィック	Allowed	Allowed	Allowed
攻撃とみなされた被疑トラフィック （遮断せず通過状態を維持）	Allowed	Monitored	Monitored
攻撃とみなされた被疑トラフィック （本システムにより遮断中）	非対応	非対応	Blocked

アクション発動時のグラフの見え方

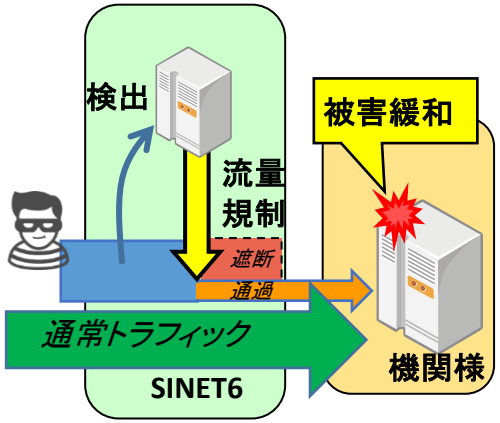
- 攻撃検出時の制御はCIDR毎にご指定いただくアクションによって異なり、グラフの見え方と発動アクションの対応は以下の通りとなります。

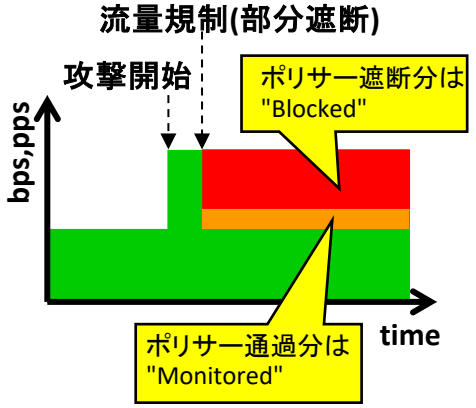
アクション：モニターを指定した
CIDR宛のトラフィック



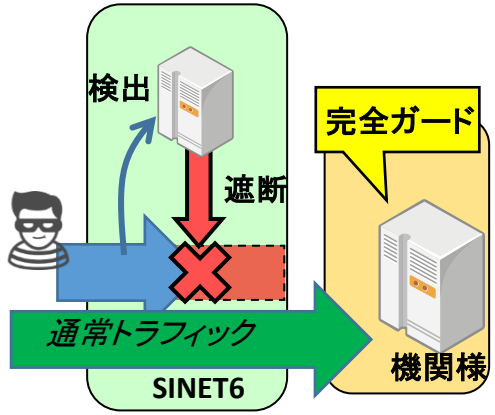


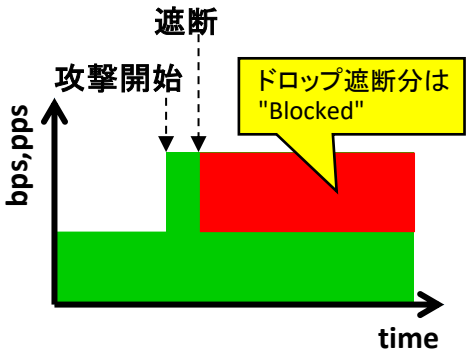
アクション：ポリサーを指定した
CIDR宛のトラフィック





アクション：ドロップを指定した
CIDR宛のトラフィック





（緑）Allowed （橙）Monitored （赤）Blocked

FAQ

- 当サービスの利用による通信遅延等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。なお、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。
- 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。
- アクション変更申請を行なった場合（例: モニタ→ドロップ）、変更後のアクションはいつ適用されますか？
  - システムの仕様上、攻撃検出状態が進行中のものには適用されません。
    当該アドレスに対する次回検出時に、変更申請いただいた新しいアクションが適用されます。
- 攻撃検出とアクション（ドロップ等）適用のイメージを知りたい
  - 単純なトラフィック量の超過だけではなく、送信元/送信先のアドレスおよびポート番号、パケットサイズ、TCPフラグ等、様々な要素の組合せ条件により攻撃検出が行われます。
    その後、事前に指定したアクションが適用され、当該条件の攻撃終了後にそのアクションが自動的に解除されます。

おわりに

- 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
  - ドロップ/ポリサを利用の際は注意事項をよくお読みの上ご申請ください

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！