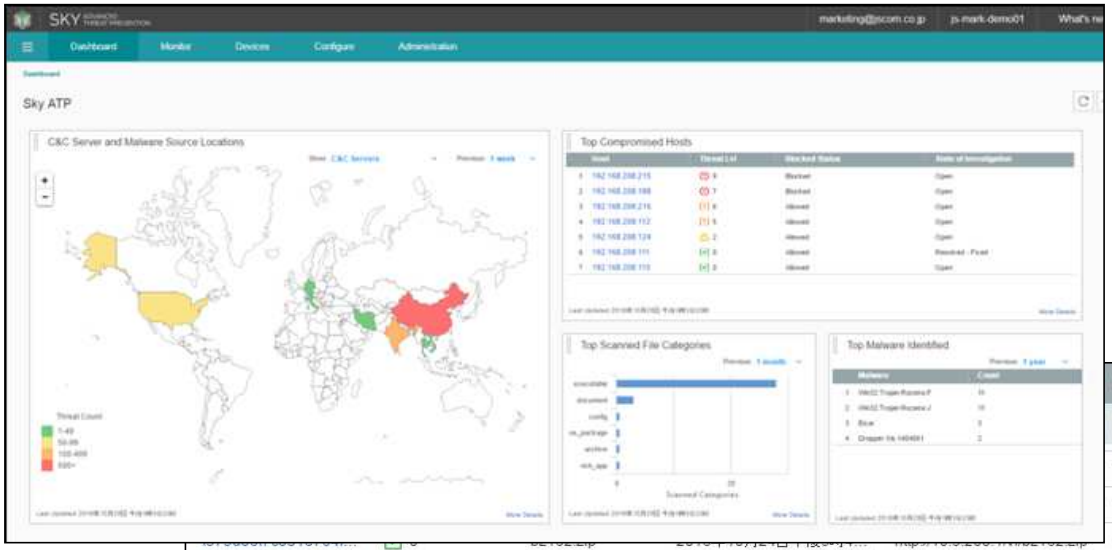
# Juniper SRXシリーズ
# Sky ATP機能

ジェイズ・コミュニケーション株式会社
プロダクト・ソリューション技術部

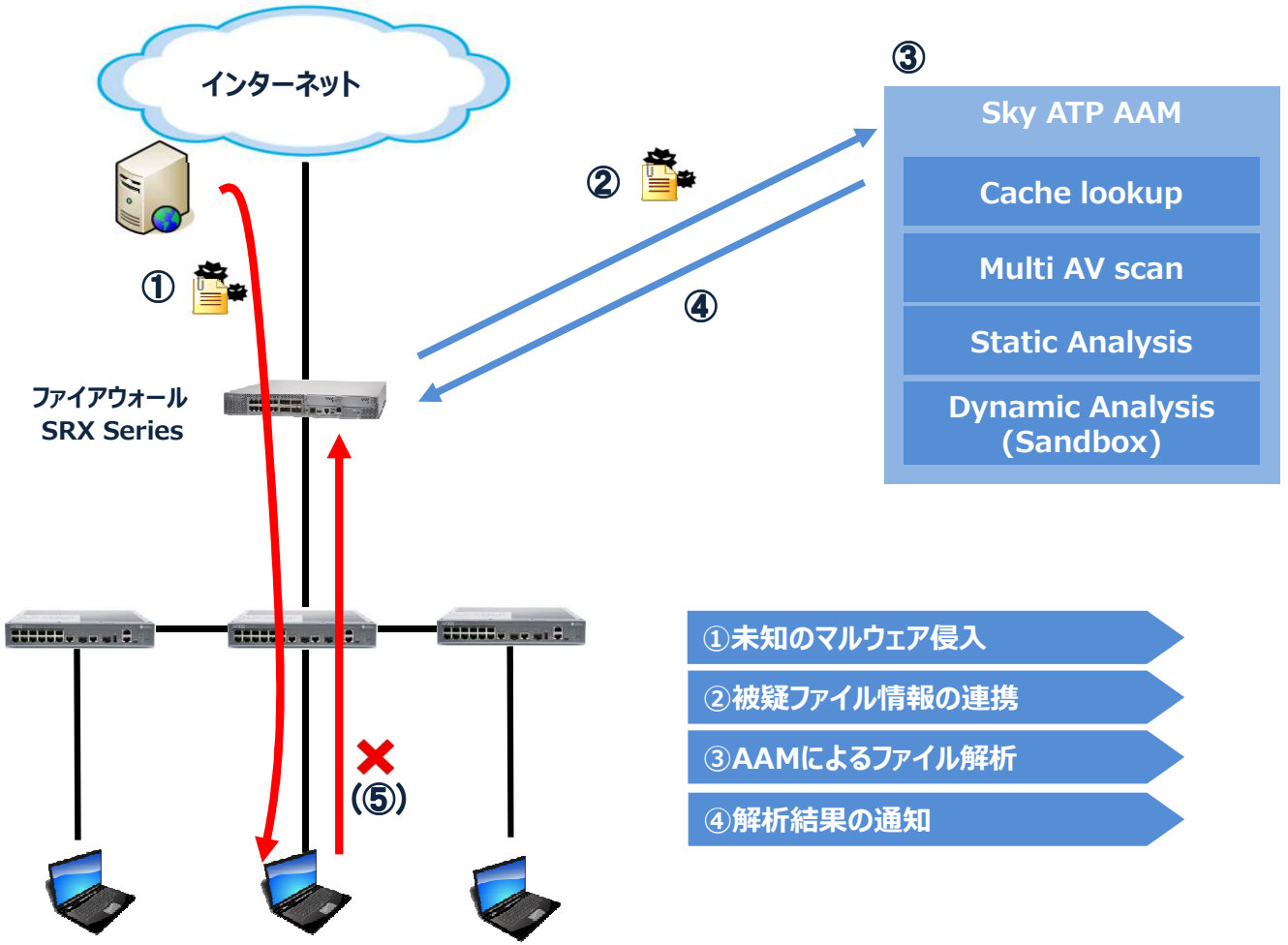
# Sky Advanced Threat Prevention

・未知の脅威を検出するAdvanced Anti-Malware
・感染行動を防ぐSecurity Intelligence



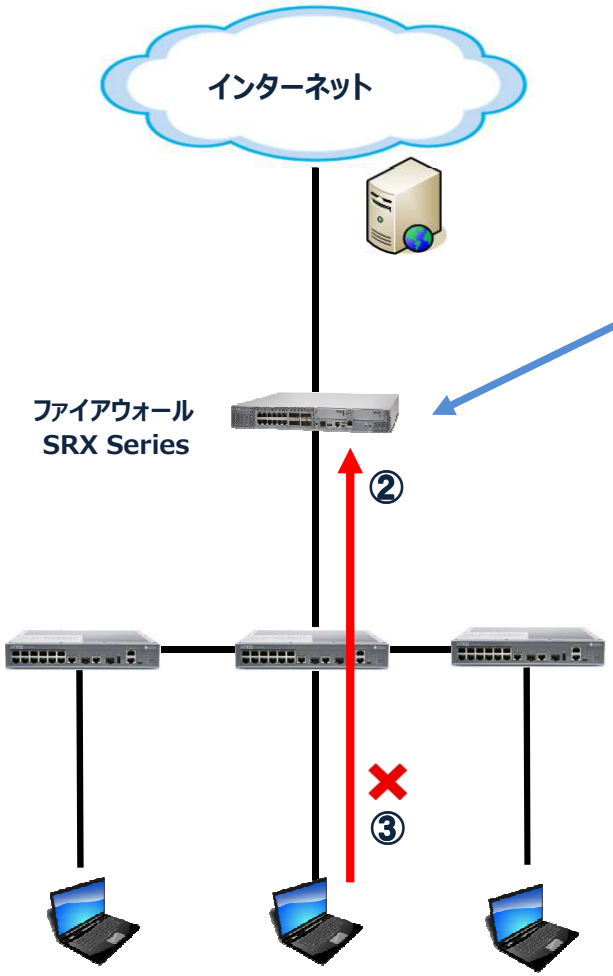

| | | | | | Malware Name | Category |
|---|---|---|---|---|---|---|
| | | | | | Win32:Trojan:Rozena:F | executable |
| | | | | | Win32:Trojan:Rozena:F | executable |
| | | | | | Clean | archive |
| 52ae7ed6d362ce8cc... | 0 | NARAClient_V1... | 2016年10月24日午後5時4... | http://10.3.208.1/vi/NARAC... | Clean | archive |
| 781f9c0635019de9f7... | 0 | swfupload.swf | 2016年10月24日午後5時3... | http://jscom.cybermail.jp/ex... | Clean | rich_app |
| 7e194a04ddec0387c... | 7 | payload-x86_64... | 2016年10月24日午後3時8分 | http://10.3.208.1/vi/payload... | Generic malware | executable |
| b69458054cd20cfffac... | 4 | C2Test.exe | 2016年10月24日午後3時6分 | http://10.3.208.1/vi/C2Test.... | Generic malware | executable |
| 4d6fe9c2643abf6483... | 0 | SumLinksLPv1.... | 2016年10月24日午後3時4分 | http://chat.kongregate.com/... | Clean | rich_app |
| 8c739cde224935a6d... | 0 | moatwrapper.swf | 2016年10月24日午後3時4分 | http://v.adsrvr.org/moatwra... | Clean | rich_app |

# Sky ATP Advanced Anti-Malware機能




①未知のマルウェア侵入
②被疑ファイル情報の連携
③AAMによるファイル解析
④解析結果の通知

# Sky ATP Security Intelligence機能




Sky ATP SecIntell

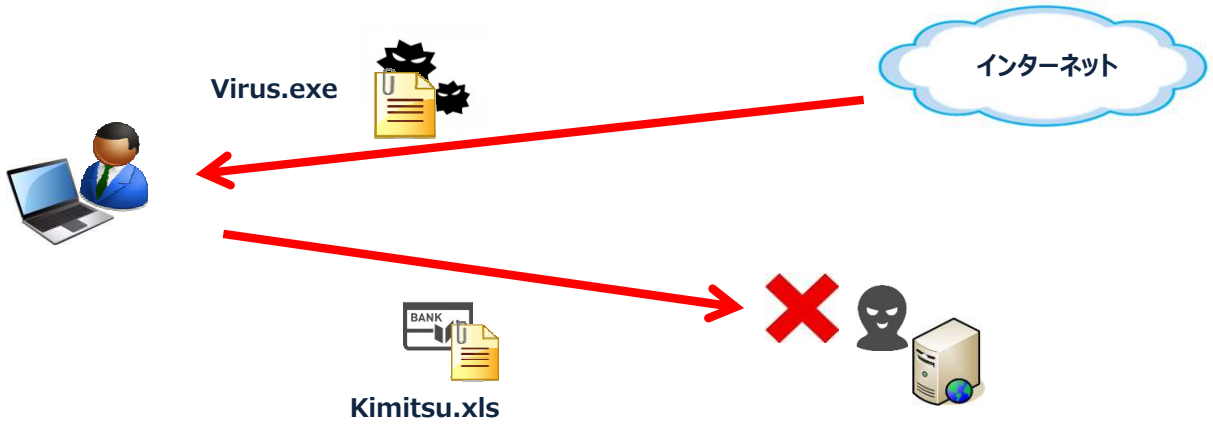
- C&C URL DB
- C&C IP DB
- Geo IP
- Infected Hosts

①C&Cサーバ等レピュテーションの低い
IP/URL情報を配信
＋ AAMで検出した感染情報を配信

②閾値(Threat Level)に基づいたブロック設定

③対象通信をブロック

# Sky ATPの特長




**本当に止めなければいけないのは、ダウンロードしたファイルそのものだけではなく、**
**そのファイルを実行してしまって感染行動を行っている端末です。**

**Sky ATPは検査済みファイルのブロックと合わせて**
**感染端末のブロックが可能**

# Advanced Anti-Malware 検証

## 弊社ASチームから提供された複数の検体で検出精度を検証

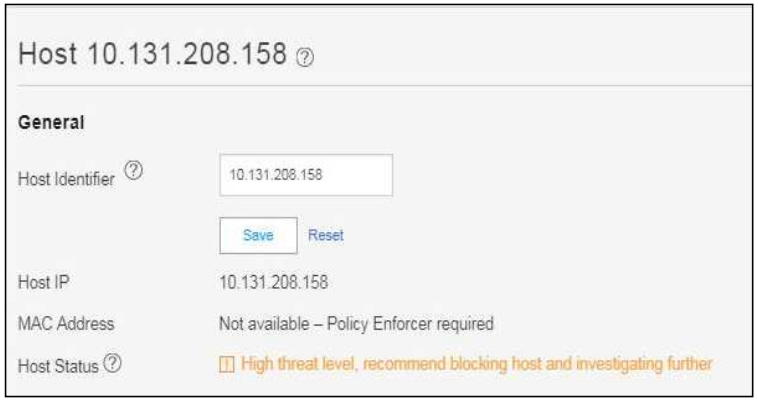
| 検体 | A | B | C | D | E |
|---|---|---|---|---|---|
| 某Anti-Virus製品　検出結果 | × | ○ | ○ | × | × |
| virus total　検出結果 | ○ | ○ | ○ | ○ | ○ |
| 検出率 | 11/57 | 12/64 | 27/64 | 12/59 | 1/42 |
| Sky ATP　検出結果 | ○ | ○ | ○ | ○ | ○ |
| threat level | 10 | 7 | 10 | 9 | 6 |

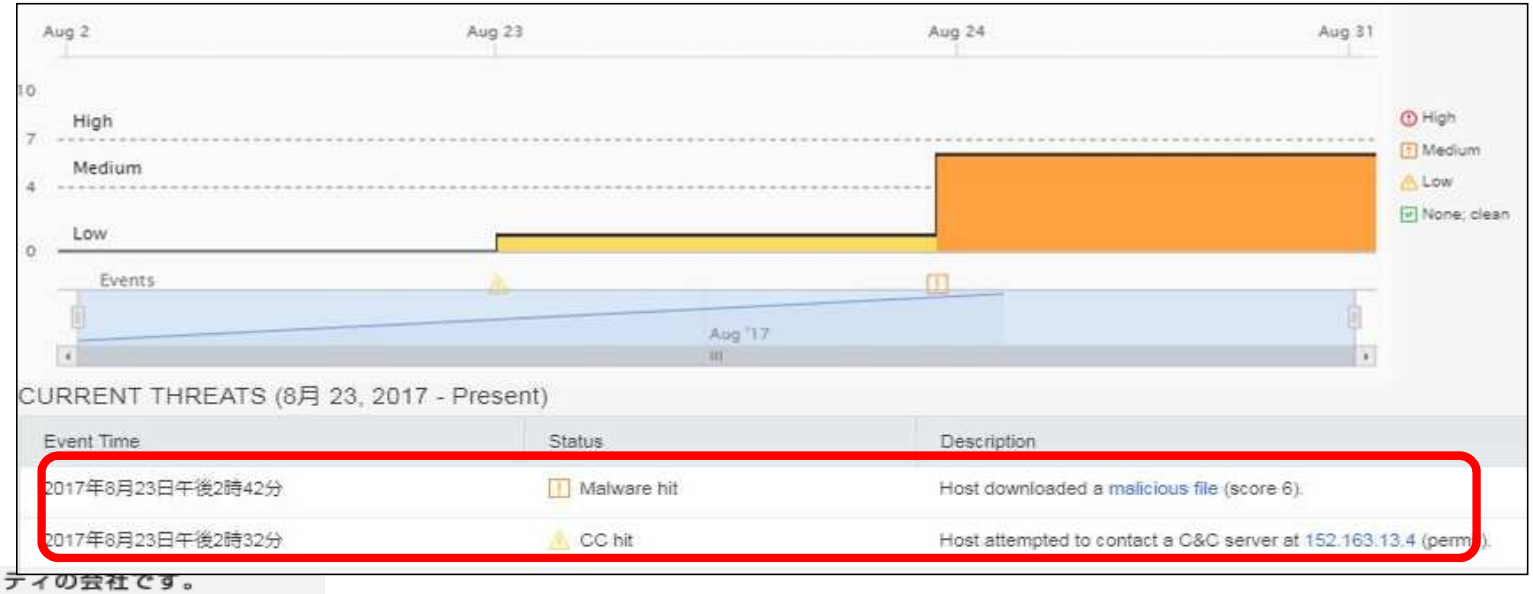

# AAM / SecIntell 連携

**疑わしい通信と被疑ファイル検出**

↓

**双方の観点から”感染ホスト”と判断**



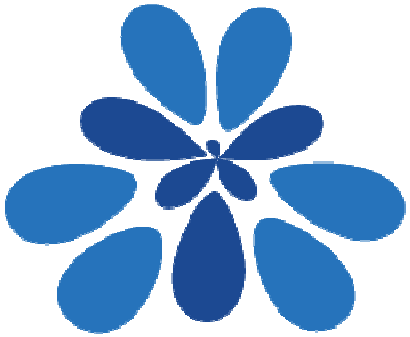



# Sky ATP 総括

ファイルを止める、だけでなく
ファイルをダウンロードした端末を防御

Advanced Anti-Malware検出精度は上々の結果

Advanced Anti-Malwareだけでなく、
Security Intelligenceを併用する事で効果を発揮



J's Communication