



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

ネットワークセキュリティの会社です。

ジェイズ・コミュニケーション株式会社

文書管理番号 : EX-PS17-053

Copyright © 2017 J's Communication Co., Ltd. All rights reserved.

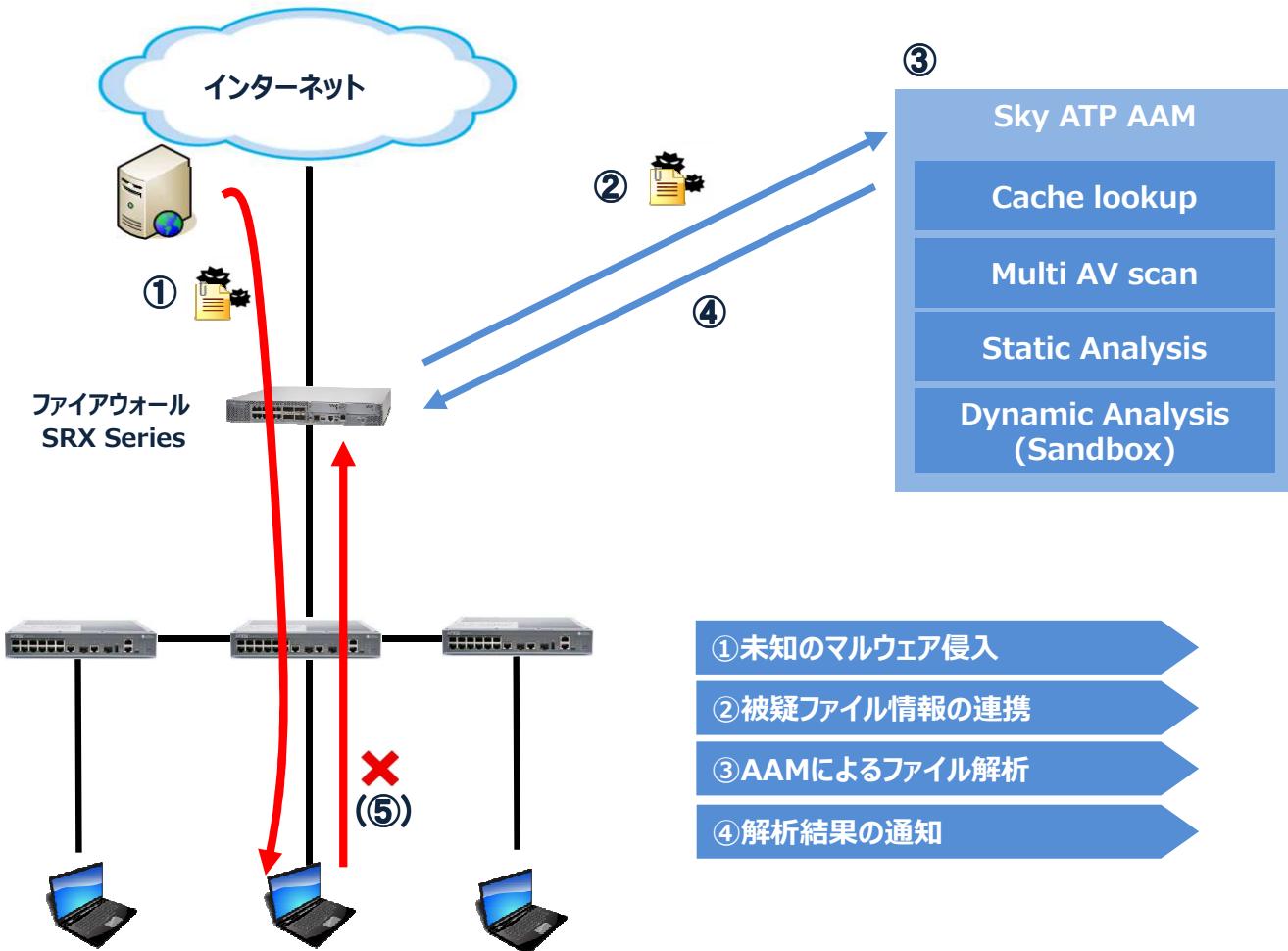
Sky Advanced Threat Prevention

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

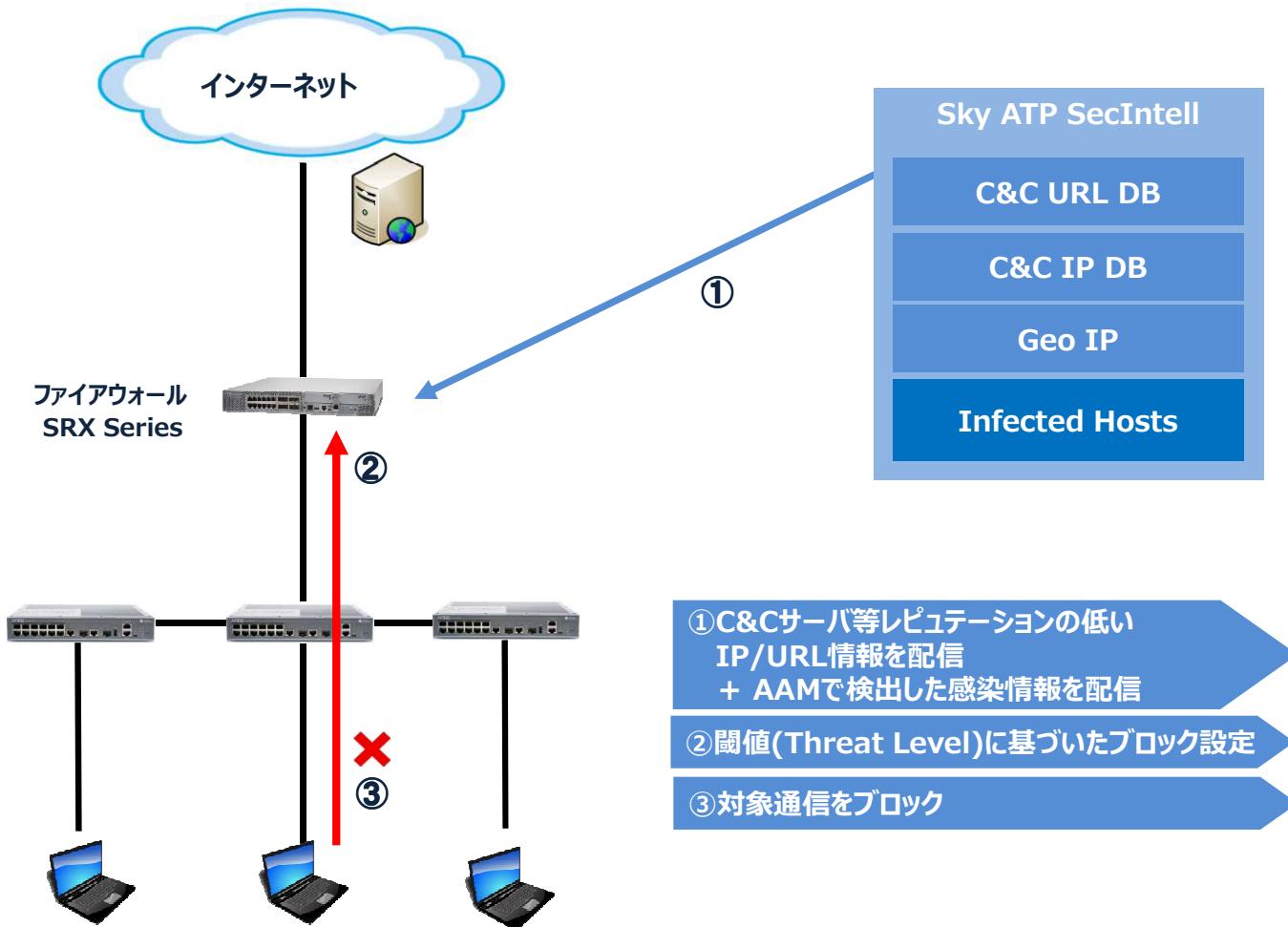
The screenshot displays the Sky ATP dashboard interface. At the top, there are navigation tabs: Dashboard, Monitor, Devices, Configure, and Admin/Status. The main area is titled "Sky ATP". It features several data visualizations and tables:

- C&C Server and Malware Source Locations:** A world map showing threat counts by region. A legend indicates threat counts: 1-49 (green), 50-99 (yellow), and 100+ (red).
- Top Compromised Hosts:** A table listing hosts based on threat count. The table includes columns: IP Address, Threat Count, Blocked Status, and Name of Investigator.
- Top Scanned File Categories:** A bar chart showing the number of files scanned across various categories.
- Top Malware Identified:** A table listing malware types and their count.
- Malware Analysis Table:** A detailed table showing individual malware entries with columns: Hash, Device ID, Date/Time, URL, Category, and Status.

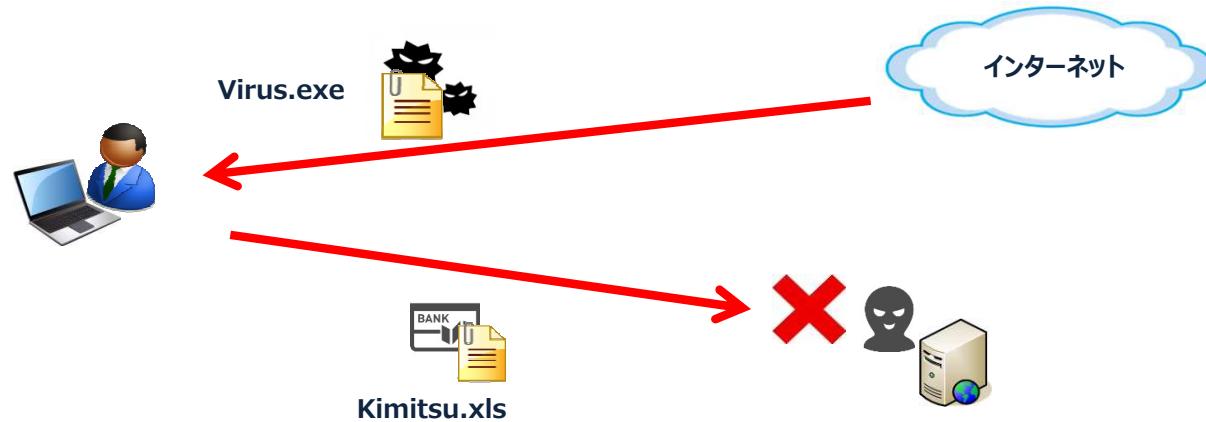
Sky ATP Advanced Anti-Malware機能



Sky ATP Security Intelligence機能



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

The screenshot shows a table of threat levels for various files. The columns are labeled 'File Signature', 'Threat Level', and 'Malware Name'. The threat levels are represented by icons: a red circle with a white exclamation mark for high risk, a yellow square for medium risk, and a green circle for low risk.

File Signature	Threat Level	Malware Name
eg. 123, 456	🔍	
2ca7c919fd097c49d8...	⚠️ 9	Win32:Trojan:Rozena.J
2ca7c919fd097c49d8...	⚠️ 9	Win32:Trojan:Rozena.J
8b34c4cbf598706320...	⚠️ 10	Tr:Xls:1404661
b69458054cd20cffac...	⚠️ 6	Generic malware

The screenshot shows the VirusTotal logo and a summary of the analysis. It includes the SHA256 hash of the file, the detection rate (11/57), and the date of the analysis (2016-10-21). On the right, there is a small graphic showing a red sad face, a green happy face, and a blue neutral face, each with a count of 0.

virustotal

SHA256: 7e194a04ddec0387c271411f49bdc42bc5bdb0177bac4337d3e7bd4e8c1777b1

検出率: 11 / 57

分析日時: 2016-10-21 19:46:46 UTC (10ヶ月, 1週間前)

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

Host 10.131.208.158

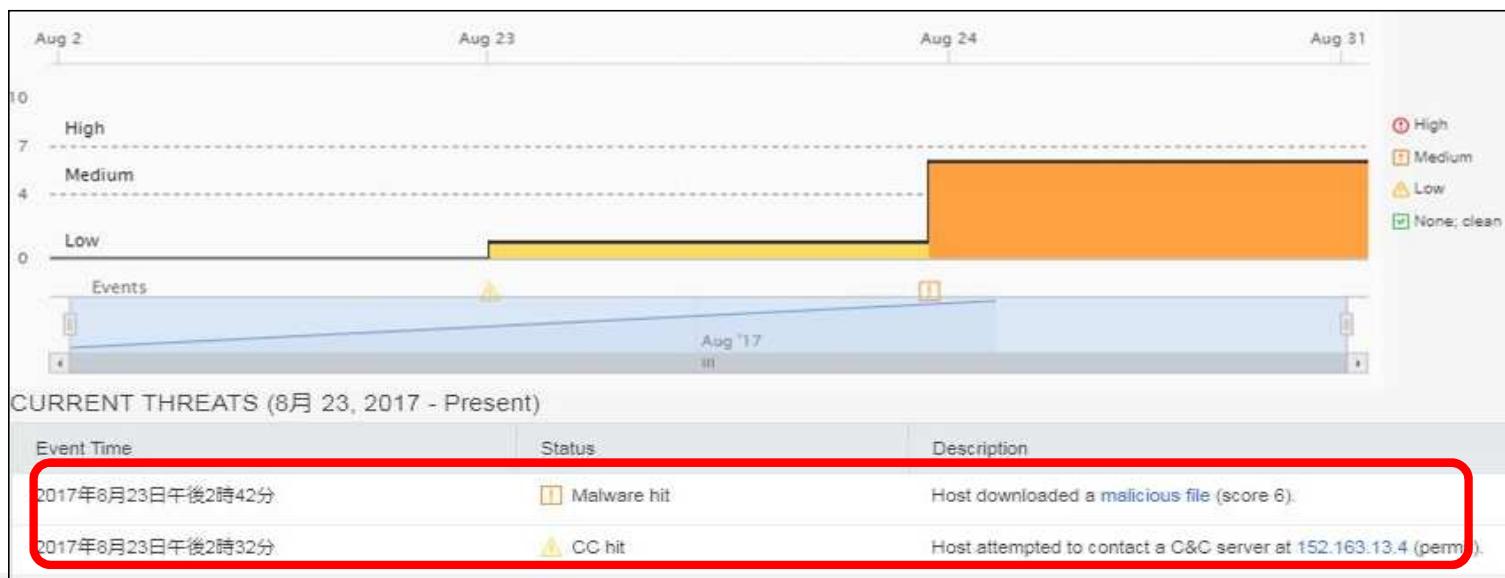
General

Host Identifier ⑦ 10.131.208.158
Save Reset

Host IP 10.131.208.158

MAC Address Not available – Policy Enforcer required

Host Status ⑦ High threat level, recommend blocking host and investigating further



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**する事で効果を發揮



ネットワークセキュリティの会社です。

ジェイズ・コミュニケーション株式会社

文書管理番号：EX-PS17-053