ORIZON

導入事例

Flowmon
Driving Network Visibility

国立研究開発法人 理化学研究所 様

全国各地の全拠点をカバーする ネットワーク可視化システムを構築し 迅速なインシデント対応体制を確立

今年で創立100周年を迎える理化学研究所（以下 理研）は、各時代の要請に応えて、施設、拠点を拡充しながら発展してきました。
現在、和光地区を中核拠点として、仙台、筑波、横浜、大阪、兵庫などに多数の拠点を擁する理研のネットワーク運用において、Flowmonがどのように活用されているのか、全拠点のITシステムの運用管理を統括する情報システム部のお2人にお話しをうかがいました。

COMPANY PROFILE

RIKEN

国立研究開発法人 理化学研究所

http://www.riken.jp/

〒351-0198
埼玉県和光市広沢2-1

理化学研究所（理研）は、1917年（大正6年）に、産業の発展のために基礎研究と応用研究を行なう財団法人として創立。その後、株式会社、特殊法人などを経て2015年に国立研究開発法人となりました。現在、日本唯一の自然科学総合研究所として、物理学、工学、化学、数理・情報科学、計算科学、生物学、医科学など幅広い分野で先導的な研究を進め、国内外の関係機関とも連携しつつ、豊かな国民生活の実現に寄与するとともに、世界のRIKENとして国際社会にも貢献しています。

導入前の課題

セキュリティインシデント発生時に備えて 端末・サーバ通信のトレーサビリティを確保

サイバー攻撃が横行する昨今、インシデント発生時の対応として重要なことは、該当するサーバや端末を迅速に特定し、システム全体への影響を俯瞰的に把握することです。理研は、これまで、各地の拠点ごとにITシステムを構築して運用していたため、全ての拠点の通信状況を一元的に可視化して、端末やサーバ通信のトレーサビリティを確保することが課題でした。

「セッション単位で分析する内製ツールを一部では使っていましたが、データ量が膨大になる点やメンテナンスの問題で、全事業所を対象に集中管理することはしていませんでした。セキュリティに関する危機感が高まる中、事業所毎での対応ではなく、集中管理できる体制を確立し、全拠点のトラフィック情報のログをインシデント対応に活用できるシステムを構築することになりました。フローベースのシステムにしたのは、セッション単位でのログ収集に比べて、フローとして集約された情報を分析する方がデータ量や時間を節約できるからです。」（黒川氏）

Flowmonにより構築された新しいネットワーク可視化システムでは、複数ある10GbEの光ファイバ回線からトラフィックデータをミラー取得してフロー情報へ変換する「Flowmon Probe」が、物理アプライアンスで全国6カ所（和光地区、筑波地区、横浜地区、大阪地区、神戸第1、第2地区、播磨地区）に合計7台配備されています。その内、理研の最大拠点であり、大容量のトラフィックが流れる和光地区では、処理性能の高いハードウェアアクセラレートモデル「Flowmon Probe Pro」が導入されて、仙台、東京の拠点もカバーしており、理研の全事業所が網羅されています。7台の「Flowmon Probe」から生成されたフローログは、和光地区の「Flowmon Collector」（フロー収集／解析専用アプライアンス機）に収集され一元管理されます。（裏面地図参照）

導入効果

問題のある事象を一発で特定 ネットワーク全体の最適化にも期待

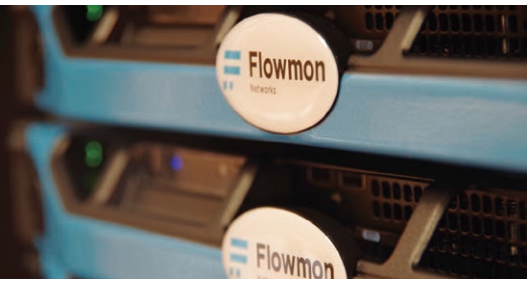
Flowmon Probeは、スイッチのミラーポートやTAPに接続するだけで、取り込んだネットワークパケットデータからフロー情報（NetFlow）を生成できます。

“インシデント発生時に、一発で事象を特定可能な仕組みが必要でした。担当者の負荷は大幅に軽減されています”

情報システム部 次長
博士（情報科学）
黒川 原佳 氏

インシデント対応のためのフロー取得に加えてネットワークの障害対応など新たな使い方も検討しています

情報システム部
情報化戦略・基盤課
技師
本多 英晴 氏



導入システム概要

● Flowmon Collector R6-24000 Pro　1台
（物理アプライアンス）
フロー最大処理数 250,000フロー/秒
ストレージ容量 24TB
（HW RAID6、冗長電源付）

● Flowmon Probe 20000 SFP+　6台
（物理アプライアンス）
1ポート当たりのパケット処理性能 1.5 Mp/s
モニタリングインタフェース 2x 10GbE
ストレージ容量 500GB

● Flowmon Probe 20000 Pro SFP+　1台
（ハードウェアアクセラレートモデル/物理アプライアンス）
1ポート当たりのパケット処理性能 14.8 Mp/s
モニタリングインタフェース 2x 10GbE
ストレージ容量 500GB

導入はいたって容易で、理研でも、導入後1カ月で本格稼働を開始しました。和光地区においてネットワークを担当する本多氏はFlowmonの活用方法を次のように語っています。「セキュリティ監視は、既存のシステムで行っていますが、そこからアラートが上がった場合に、Flowmonで取得するフロー情報を使用します。Flowmon Probeから生成されたフロー情報は、Flowmon Collectorにいったん集められた後、高速なログ解析専用システムに送られます。他システムからのインシデントログと相関分析をかけることで、事象の特定や全体像を把握するという使い方ができます。」

また、本多氏は、Flowmonの当初システム要件でなかった機能にも注目しています。それは、Flowmon Probeで生成したフローデータを基に、非SSL通信においてURLを解析する機能です。Flowmon Probeで生成したフローデータは、拡張フィールドを用いて一部L7レベルの情報を解析することができます。マルウェア感染などのインシデント対応に有益な機能として、今後活用していきたいと述べています。

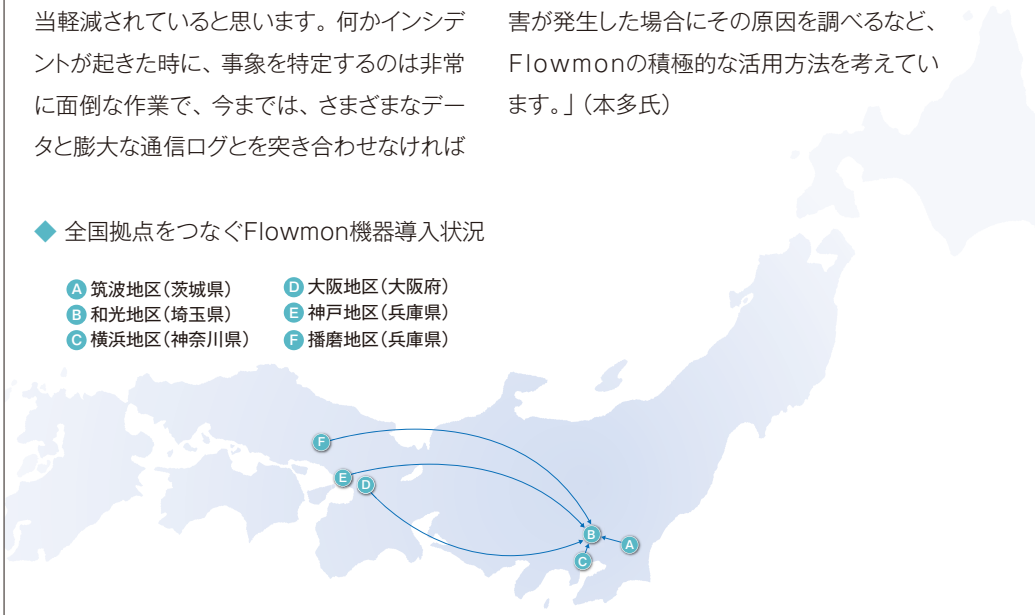
「Flowmon導入により、実際にインシデント対応をしている担当者たちの負荷は相当軽減されていると思います。何かインシデントが起きた時に、事象を特定するのは非常に面倒な作業で、今までは、さまざまなデータと膨大な通信ログとを突き合わせなければなりませんでしたが、Flowmonで収集したネットワーク全体のフロー情報を相関分析的に利用することで、一発で特定できるようになります。」（黒川氏）

さらに黒川氏は、Flowmon自体のトラフィック分析機能についても、今後のシステム全体の最適化に効果があると期待しています。「管理者としては、各事業所でどれくらいのトラフィックが発生し、ニーズが賄えているのか、どの端末がどこと通信していたのか、どのサーバにどのようなトラフィックが集まっているのか、などを把握できることがうれしいですね。」（黒川氏）

また、ネットワークトラフィックのトラブルシューティングにおいて、フローデータによる解析だけではなく、トラフィックデータそのものを取得して実際の通信パケットの状況を調べる必要が出てくることもあります。理研では、ネットワークの完全な通信パケットを記録できるプラグインである「Flowmon Traffic Recorder」により、ネットワーク障害の対応能力をさらに強化することも検討しています。「現在はインシデント対応ですが、せっかく10Gでトラフィック情報を取得する環境があるので、ネットワークで何か障害が発生した場合にその原因を調べるなど、Flowmonの積極的な活用方法を考えています。」（本多氏）

◆ 全国拠点をつなぐFlowmon機器導入状況

Ⓐ 筑波地区（茨城県）
Ⓑ 和光地区（埼玉県）
Ⓒ 横浜地区（神奈川県）
Ⓓ 大阪地区（大阪府）
Ⓔ 神戸地区（兵庫県）
Ⓕ 播磨地区（兵庫県）



ORIZON
オリゾンシステムズ株式会社
https://www.orizon.co.jp/products/flowmon/
〒160-0022
東京都新宿区新宿6-27-56 新宿スクエア7F
Tel.03-6205-6082　Fax.03-3205-6040

お問い合わせ