グローバルな脅威情報基盤を用いたセキュリティオーケストレーションの実現

小山 高明 †1 /胡 博
永渕 幸雄 †1 /塩治 榮太朗 †2
髙橋 健司

NTTセキュアプラットフォーム研究所 †1
NTT Innovation Institute, Inc. †2

GTIP（Global Threat Intelligence Platform）はNTT Innovation Institute, Inc.（NTT I³）が開発したサイバー攻撃の脅威情報の収集・配布システムです．NTTセキュアプラットフォーム研究所のセキュリティオーケストレーション技術と連携させることで，脅威情報に基づく高度な防衛が可能となります．本稿では，共同で構築・実施した連携デモや今後のグローバル展開について紹介します．

巧妙化するサイバー攻撃

近年，公共団体や企業などに対するサイバー攻撃は進化し続けており，セキュリティアプライアンスを用いて，ウィルス定義ファイルやシグネチャ更新を基にした検知と遮断などの対策が行われています．しかし，攻撃者は，新種のサイバー攻撃手法を使って検知をすり抜けて侵入するため，インターネット経由での情報漏洩や改ざん等の被害が後を絶ちません．これらに対応するには，従来とは別のアプローチを用いたセキュリティオペレーションが必要と考えられます．本稿では，これら新種のサイバー攻撃とそれに対応するためのNTT研究所，NTT Innovation Institute, Inc.（NTT I³）の取り組み，そして，共同で構築した連携システムと今後のグローバル展開について紹介します．

新種のサイバー攻撃とその対応方法

攻撃者は，標的型メール，水飲み場攻撃などを用いて，ユーザに，インターネット上に置いてある悪性プログラムをダウンロードさせてユーザ環境に常駐させ，インターネット経由による指示により，情報漏洩，破壊行動，新たな悪性プログラムへのアップグレード，C&C（Command and Control）サーバ構築などを行います．これらの一連活動がインターネット経由で行われ，さらに新しい悪性プログラムがつくられ続けているため，次に示す3つの対応方法が有効であると考えています．

⑴ 外部から脅威インテリジェンスを積極的に取り入れ，被害を未然に防ぐ

IPアドレス，URLなどのブラックリストや，インターネット上で確認された最新の悪性プログラムの挙動などの脅威インテリジェンスは，攻撃者の侵入を防ぐことや，侵入後の活動を防ぐことに役に立ちます．

⑵ 対処設定オペレーションを自動化することで迅速に実施する

新しい悪性プログラムの出現に対して，対処設定をより迅速に行うことで，被害拡大を防止します．

⑶ 多様な脅威インテリジェンスに対して，最適な装置にて最適な対処を設定する

さまざまなセキュリティアプライアンスが民間企業等のイントラネットや，イントラネットとインターネットとの接続点に存在します．適切な対処を適切な装置に設定することで，攻撃者のインターネット経由の活動を阻止します．

NTTセキュアプラットフォーム研究所の取り組み

NTTセキュアプラットフォーム研究所では，サイバー攻撃に対して自動対処する，セキュリティオーケストレーション技術を研究開発してきました[(1)]．今後さらに巧妙化する新しいサイバー攻撃への対応方法確立に向けて，現在，以下の3つの技術要素を実現するリジリエントセキュリティエンジン（RSE）の研究開発に取り組んでいます（**図1**）．

■脅威インテリジェンスを取り入れた事前予防対処技術

インターネット経由のサイバー攻撃からユーザを守るため，外部から積極的に脅威インテリジェンスを取り入れます．具体的には，世界中のサイバー攻撃情報を収集する脅威インテリジェンス基盤と連携し，攻撃発動前に攻撃者のIPアドレス，URLなどをブラックリストとして設定し，被害を未然に防ぐ方法を用います．例えば，疑わしい挙動を検知時，脅威インテリジェンス基盤からの攻撃元情報により，より高い精度の判定が期待できます．

脅威インテリジェンスとの連携に向けて，NTTセキュアプラットフォーム研究所では，NTT I^{3}と綿密な交流を図り，NTT I^{3}が開発する脅威インテリジェンス基盤とRSEとのシステム連携を進めています．後述するオペレーションの自動化フレームワークおよび，多様なセンサ・アプライアンスを用いた最適判断対処技術を伴うことにより，攻撃・脅威に対してより迅速かつ適切な対処の実施が期待できます．

■セキュリティオペレーションの自動化フレームワーク

インシデント発生時にデータセンタのセキュリティオペレータが攻撃・脅威の検知ログにより攻撃の種別を確認し，取るべき対処を判断します．その際に，ネットワーク構成情報によりファイアウォールなどのふさわしい対処装置を探し出し，該当装置に制御命令を送る必要があります．現在，この一連のオペレーションにおいて，攻撃・脅威の情報収集がSIEM（Security Information and Event Management）[*1]基盤等により一元化され，ファイアウォールの制御が専用ツールにより簡易化される状況ではありますが，オペレータが複数の管理システムや制御ツールを用いてセキュリティポリシーとネットワーク構成を把握したうえで，手動でインシデントに対処する必要があるため，オペレーション負担と所要時間増が問題としてあります．

そのため，収集，判断，対処のセキュリティオペレーションを迅速に行う自動化フレームワークを研究開発しています．この自動化フレームワークでは，単に複数管理システム・制御ツール間の連携動作を1つのプログラムとして定義するだけでなく，ユーザが要望するセキュリティ強度によって同一種別の攻撃（例：マルウェア感染）に対しても監視強化，遮断，隔離などの異なる対処方法（例：通信トラフィックを遮断，あるいは機器をネットワークから完全隔離）を選択可能とし，さらにユーザのICT環境により同一の対処方法において異なる装置（例：物理スイッチ，あるいはハイパーバイザの仮想スイッチ）で通信遮断等の対処を実施可能とした汎用的なオペレーションの実現を目指しています．

■多様なセキュリティセンサとアプライアンスを用いた，最適判断対処技術

マルチベクタ攻撃に対して，ユーザのICT環境に分散配置される複数種類のセキュリティセンサとアプライアンスを用いる多層・面的防御が有効であると考えられています．しかしながら，IDS（Intrusion Detection System）[*2]や

*1　SIEM：サーバ，ネットワーク機器，セキュリティ関連機器などからログ情報を収集し，集められたログ情報に基づき，故障や攻撃等の異常があった場合に，管理者へ事実や対策等を通知するシステム．
*2　IDS：ネットワーク上を流れるパケットを監視し，不正なアクセス兆候があった場合に，管理者に通知するシステム．

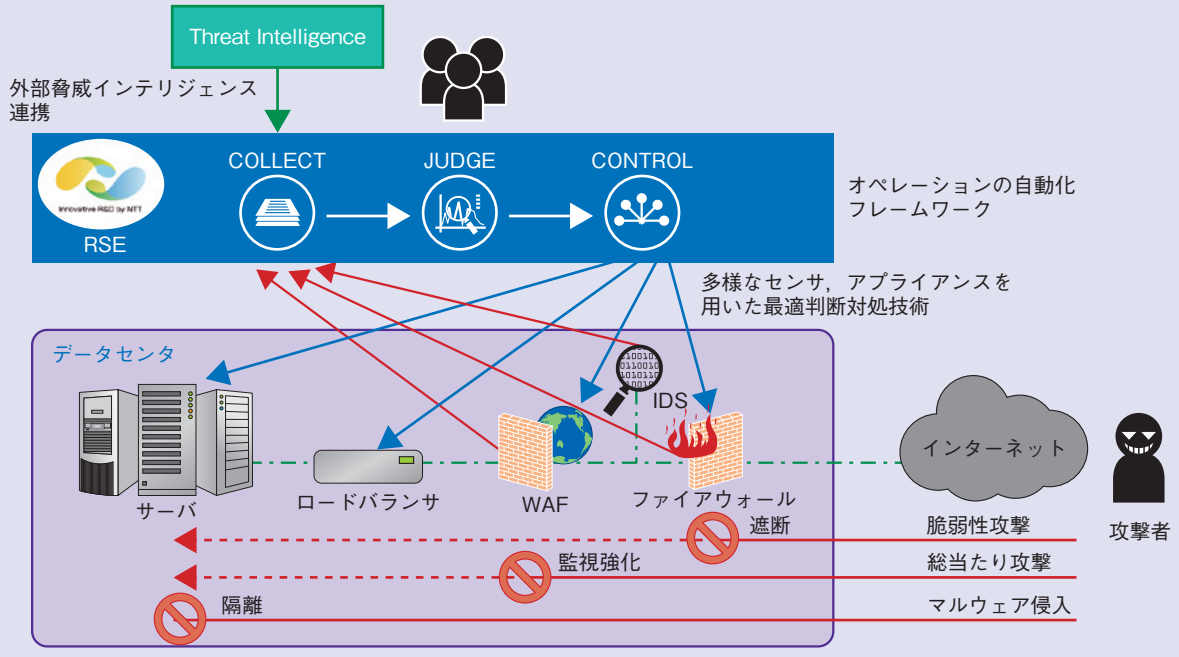


図1　リジリエントセキュリティエンジン

WAF（Web Application Firewall）[*3]などのセンサ・アプライアンスは，単体での動作を前提として設計されており，他機器との情報交換や動作連携が十分考慮されていません．一部のベンダが自社製品間の連携ソリューションを付加価値として提供していますが，マルチベンダ製品による検知・制御範囲の向上といった相乗効果が図れず，連携の効果が限定的であると考えられます．

そのため，多種多様なセンサから脅威情報を収集し，攻撃・脅威の種別および最適な対処方法を判断したうえ，ネットワーク上の最適な機器での対処を実施可能とする最適判断対処技術を研究開発しています．この最適判断対処技術では，複数センサの検出情報を併用して攻撃・脅威の事象と適切な対処方法を判断でき，さらに検出情報間の関連性を定義することで攻撃・脅威の状態管理を可能にします．一方，対処については，ネットワーク上に分散配置されたアプライアンスの構成情報を参照し，複数の候補から攻撃の根本原因に近い個所を抽出した対処を実行できます．

NTT I[3]の取り組み

NTT I[3]で開発を行っているGTIP（Global Threat Intelligence Platform）について紹介します．GTIPは，世界中の脅威情報を収集・解析し，サービスで活用可能な脅威インテリジェンスとして配布することを目的とした総合基盤です．この基盤をNTTグループ内で活用することにより，グループ全体のセキュリティサービスの品質の向上に貢献することを目指しています．

GTIPの主な特徴として，多彩な脅威情報をNTTグループ内外から幅広く収集できること（収集機能），独自の技術に基づいた高度な解析ができること（解析機能），柔軟な入出力インタフェースを有すること（共有機能）が挙げられます．これらの機能を組み合わせることで，従来のリアクティブな防御では対策が困難になりつつある近年の広範囲かつ複雑な脅威への対策を行うことが可能となります（**図2**）．

■収集機能

世界中に設置された脅威センサ（ハニーポットなど），独自の商用Webクローラ，多数のコミュニティ・ベンダから提供される情報，NTTグループのセキュリティ事業者（MSSPなど）から提供される情報を収集します．今後もネットワークトラフィックなどの情報源の追加が予定されています．

■解析機能

NTTセキュアプラットフォーム研究所の協力のもとにNTT I[3]が 開発した高度なプログラム解析技術（テイント解析[*4]技術）を用いて，マルウェアの悪性通信先リストを生成できます．加えて，レピュテーションの計算や相関分析を行うことにより，詳細な根拠情報や悪性度のスコアが付与された，活用しやすいインテリジェンスを生成することができます．

■共有機能

収集・解析された膨大なデータはHadoopクラスタにて保管され，各データには権限に応じたアクセス制限が設定されます．ユーザ向けにはWebポー

*3 WAF：Webアプリケーションのやり取りを利用した，インターネット等の外部ネットワークからの不正侵入を検知防御できるファイアウォール．
*4 テイント解析：実行時に重要なデータにタグを付与し，その詳細なデータフローを追うことで情報漏洩などの検知が可能となる解析手法．

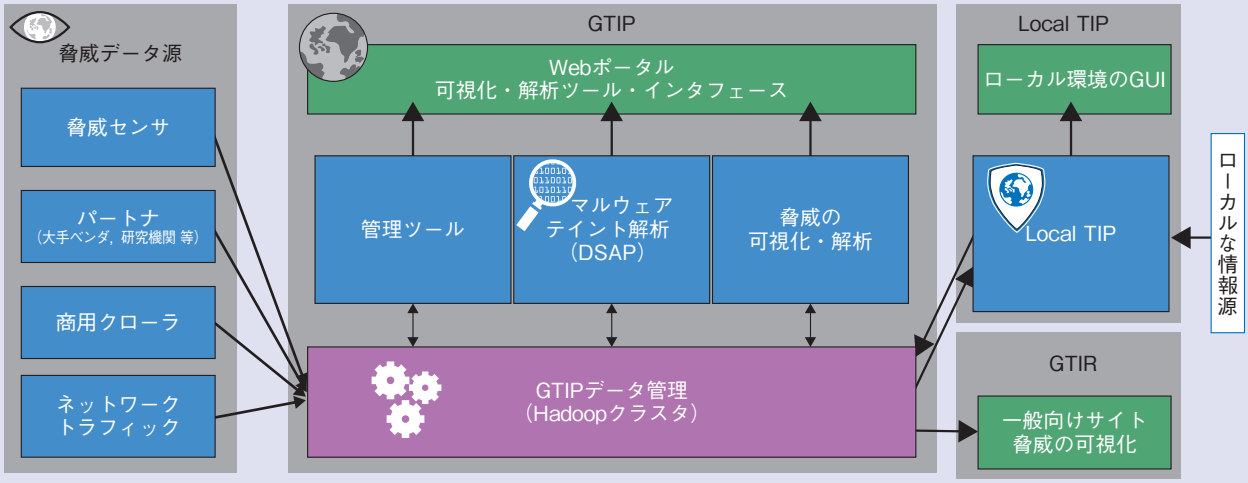


図2　GTIPの全体像

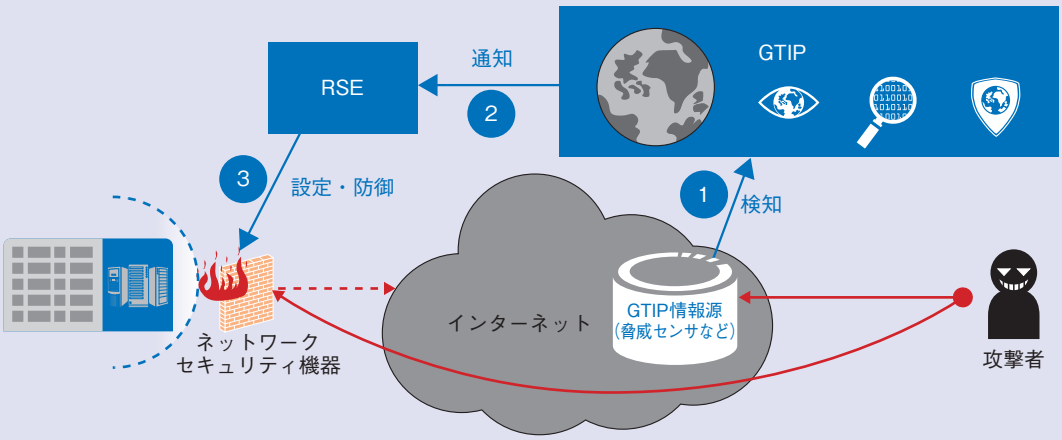


図3　GTIPとRSEの連携システム

タルやThrift APIなどのインタフェースが提供されており，さまざまなサービス形態・ニーズに対応可能です．また，ユーザのローカル環境にGTIPの情報を同期するクライアントLTIP（Local Threat Intelligence Platform）の提供や，一般向けサイトGTIR（Global Threat Intelligence Report）を介した情報の配信も担っています．

GTIPのユースケースの1つとして，共有したインテリジェンスをファイアウォールやIDS（Intrusion Detection System）などのネットワークセキュリティ機器に入力することで検知・防御能力を高めることが挙げられます．しかし，判定基準となるセキュリティポリシーや制御対象となる機器とのインタフェースなどはユーザ環境ごとに異なるためインテグレーションは容易ではありません．そこで，これらの障壁を緩和するためのレイヤとしてRSEとの連携が期待されています．

GTIPとRSEの連携システムと今後のグローバル展開

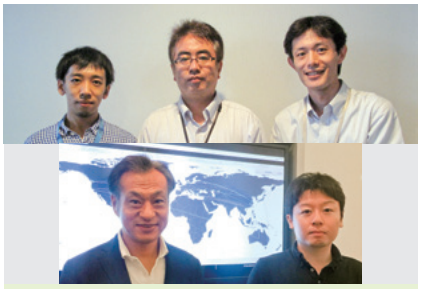
現在，NTTセキュアプラットフォーム研究所とNTT I[3]は，定期的に情報交換を進めています．2015年に入り，RSEとGTIPの連携が，RSEにとってはより高度なサイバー攻撃から防御するための脅威インテリジェンスの補強，GTIPにとってはユーザ環境へのインテグレーションの容易化を実現し，さらなる強固な防御を可能にすることが分かりました．そのため，2015年第1四半期にRSEとGTIPの連携のコンセプト実証デモの開発を共同で行いました．

システムの連携形態としてはさまざまなものが考えられますが，本デモでは一例としてGTIPの情報に基づいた自動防御を行う形態を実証しました（**図3**）．

①GTIPが攻撃を検知し，②GTIPがRSEに攻撃情報を通知し，③RSEがその攻撃情報に基づいた判断を行い，攻撃をブロックするようにネットワーク機器を設定します．この一連の流れを自動化することにより，プロアクティブな防御を行うことが可能となります．実験の結果，システム連結は問題なく可能であることが実証されたため，本システムの実用化・高度化に向けたさらなる発展が期待されています．次の段階としては2015年の後半に実施されるGTIPベータトライアルにおいて，実ユーザ環境における実証を行い，運用も含めた課題の発見と解決方法の検討を進めていく予定です．

■参考文献

⑴ 小山・波戸・北爪・永渕：“サイバー攻撃から早期回復を図るリジリエント・セキュリティ技術，” NTT技術ジャーナル，Vol.26, No.3, pp.63-66, 2014.



（上段左から）胡　博/ 永渕　幸雄/ 小山　高明
（下段左から）髙橋　健司/ 塩治　榮太朗

NTTセキュアプラットフォーム研究所では，NTT I[3]の開発したGTIPを用いて，より高度なセキュリティオーケストレーション技術の実現に取り組んでいます．

◆問い合わせ先
NTTセキュアプラットフォーム研究所
セキュアアーキテクチャプロジェクト
TEL　0422-59-6412
FAX　0422-59-5637
E-mail　kitazume.hideo@lab.ntt.co.jp