事業を支えるサイバー攻撃対策技術のR&D

NTTセキュアプラットフォーム研究所では，セキュリティ事業を支える世界最先端のサイバー攻撃対策技術の研究開発に取り組んでいます．本稿では，マルウェア感染の防御や検知に有効なドメイン名の解析技術，MDR（Managed Detection and Response）サービスを支えるマルウェア解析技術，リジリエントセキュリティエンジンとマルウェア対策用ブラックリストを活用したUTM（Unified Threat Management）ソリューションについて紹介します．

針生 剛男（はりう たけお）/千葉 大紀（ちば だいき）/秋山 満昭（あきやま みつあき）
八木 毅（やぎ たけし）/川古谷 裕平（かわこや ゆうへい）/永渕 幸雄（ながふち ゆきお）
小山 高明（こやま たかあき）

NTTセキュアプラットフォーム研究所

ドメイン名の解析技術

現在のインターネットにおいて欠かすことのできないものとしてドメイン名とDNS（Domain Name System）が挙げられます．ドメイン名とはWebサイトへのアクセスやメールの送受信を行う際に通信先を識別するために利用されるexample.comのように記載される情報です．また，ドメイン名と実際の通信で必要となるIPアドレスを対応付ける仕組みがDNSです．ドメイン名とDNSは通常のインターネットで利用されるだけでなく，サイバー攻撃を実施するための攻撃インフラとしても悪用されているのが現状です．具体的には，攻撃者は日々新たなドメイン名を用意して悪意のあるソフトウェア（マルウェア）を配布するほか，正規のサービスに類似するドメイン名を用意してユーザを騙すフィッシングを実施したり，マルウェアを操作するための指令（C&C：Command and Control）サーバを運用してDDoS（Distributed Denial of Service）攻撃やスパムメール送信および情報窃取に代表されるサイバー攻撃に利用したりしています．

これまで，NTTセキュアプラットフォーム研究所（SC研）ではマルウェア感染に関連する悪性情報（セキュリティインテリジェンス）を創出するさまざまな技術の研究開発を行い，グローバルセキュリティビジネスへ貢献してきました[(1)]．例えば，マルウェア感染が発生する際の挙動を正確かつ安全に観測するおとりシステムである各種ハニーポット技術や，システムがマルウェア感染した後の挙動を実際のマルウェアを動作させて解析するマルウェア動的解析技術の研究開発を行ってきました．しかし，日々進化し続けるサイバー攻撃では解析技術や対策への回避策が攻撃者によって講じられるようになり，これらの技術だけでは特定できない攻撃が見受けられるようになってきました．

そこで，SC研では高度化・巧妙化するサイバー攻撃に対応し続けるため，攻撃者が攻撃インフラとして悪用している悪性ドメイン名の性質に着目した攻撃解析技術の研究開発に着手し，セキュリティインテリジェンスの拡張に取り組んできました．具体的には，悪性ドメイン名を特定することができるドメイン名のレピュテーション技術や，悪性ドメイン名を基にサイバー攻撃を効果的に防ぐ情報を生成することができるドメイン名のカテゴライズ技術を創出しました．この2つの技術を活用して生成されるセキュリティインテリジェンスを利用することで，マルウェア感染を未然に防ぐ感染防御（入口対策）やマルウェア感染端末の発見（出口対策）をはじめとするサイバー攻撃対策をより強化することができます．

■ドメイン名のレピュテーション技術

SC研で独自に蓄積した情報や公開情報を活用して，ドメイン名の悪性度を多角的に評価します．私たちが実現したドメイン名のレピュテーション技術では，入力されるドメイン名の中から攻撃者によって利用される悪性ドメイン名を特定して出力します（**図1**）．

攻撃者は悪性ドメイン名を日々新たに生成し，攻撃で利用する悪性ドメイン名を変化させ続けることで，対策されるのを回避しながらサイバー攻撃を実施しています．例えば，攻撃者はDGA（Domain Generation Algorithm）と呼ばれる仕組みで短期間のみ有効となるような悪性ドメイン名を大量生成したり，元々異なる目的で利用されていた正規なドメイン名を再取得して悪用したりすることで，一般的な対策を回避しようとしています．

このような状況に対応するため，本

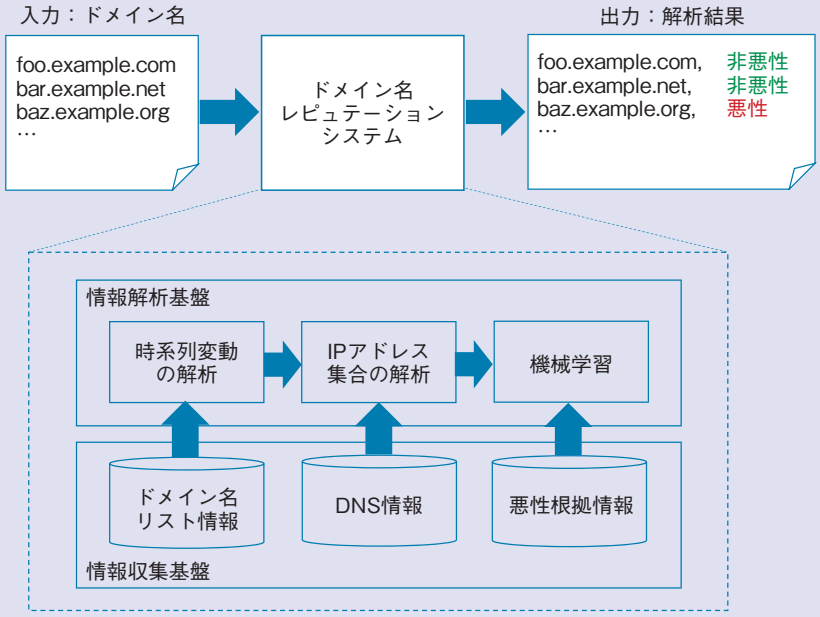

図 1　ドメイン名のレピュテーション技術

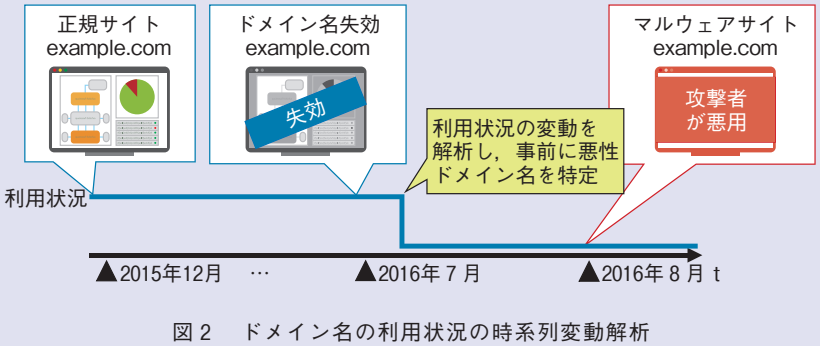

図 2　ドメイン名の利用状況の時系列変動解析

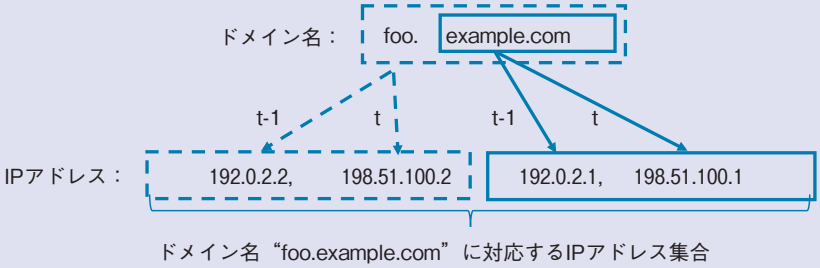

図 3　ドメイン名に対応するIPアドレス集合解析

レピュテーション技術では，ドメイン名が登録されてから失効するまでのライフサイクルに着目し，サイバー攻撃に起因して変化するドメイン名の特性を時系列変動パターンとして解析することで，攻撃者が保有・運用するドメイン名を正確に特定します．例えば，元々正規サイトで利用されていたexample.comというドメイン名がいったん失効したあとに攻撃者によって再取得されマルウェア配布サイトとして利用されていた事例では，私たちのレピュテーション技術はドメイン名の失効とその後の利用状況の変化をとらえることで攻撃が発生する前に悪性ドメイン名を特定することができます（**図 2**）．

また，本レピュテーション技術ではドメイン名に対応するIPアドレス集合に基づく解析も同時に実施します．具体的には，入力ドメイン名foo.example.comやその上位のドメイン名example.comに対して，各々に過去に対応したことのあるIPアドレス集合を調査します（**図 3**）．特に，SC研で蓄積されたセキュリティインテリジェンスを活用することで，過去にサイバー攻撃で利用された際に観測された情報を参照し，悪性ドメイン名を運用する攻撃者ならではの傾向をとらえることができます．このようなIPアドレス集合の解析結果と，前述の時系列変動パターンの解析結果に基づき，機械学習技術を利用することで，ドメイン名が悪用されている可能性を悪性度として算出・予測するシステムを実現しました．

実際のサイバー攻撃で用いられた悪性ドメイン名を利用した大規模な評価を行った結果，本レピュテーション技術は，これまで一般的な技術では特定

することができなかった悪性ドメイン名を精度良く予測することに成功しています．また，本技術をまとめた論文[2]は，世界トップレベルの学術会議にて当該分野で日本から初めて採録されるなど，世界で高く評価されています．

■ドメイン名のカテゴライズ技術

ドメイン名の生成された経緯や状況をとらえ，各悪性ドメイン名に対し実施すべき対策を客観的に提示します．私たちが実現したドメイン名のカテゴライズ技術では，入力される各悪性ドメイン名に対して，サイバー攻撃を防ぐために具体的にどのような対策を実施すべきなのかを提示して出力します（**図4**）．

攻撃者は特性の異なる悪性ドメイン名を利用してサイバー攻撃を実施することで，一様に対策されるのを防いでいます．例えば，悪性ドメイン名の中には正規のインターネットサービスで利用されている仕組みを悪用して生成されるものが存在します．この場合，単純にドメイン名をブラックリストとして通信ブロックなどの対策を行ってしまうと，正規ユーザや正規サービスの利用を誤って妨げてしまう可能性があります．一方で，DGAをはじめとして攻撃目的のためだけに用意された悪性ドメイン名も存在します．この場合，ドメイン名単位での通信ブロックがもっとも効果的です．このように，さまざまな生成構造を持つ悪性ドメイン名が悪用されていることから，前述のレピュテーション技術で悪性ドメイン名を多数特定できたとしても，それをそのままセキュリティインテリジェンスとして有効活用できるとは限りません．

このような状況をふまえ，私たちは単に悪性ドメイン名を提示するだけではなく，各悪性ドメイン名に対してどのような対策をとるべきなのかという対策アクションを提示する重要性にたどり着きました．そこで，レピュテーション技術で特定された悪性ドメイン名に対し，各ドメイン名の生成構造を体系的に特定するドメイン名のカテゴライズ技術に着手しました．

本カテゴライズ技術は，対策を実施する際に考慮すべき悪性ドメイン名の生成構造を体系的にとらえます（**図5**）．具体的には，悪性ドメイン名を大きく2つのカテゴリに分けてとらえます．1番目のカテゴリは，正規サービスを悪用することで生成された悪性ドメイン名です．例えば，オンライン広告サービスやCDN（Content Delivery Network）サービス，Webホスティングサービスの悪用が該当します．このようなサービスで用いられるドメイン名は元来正規サービスの提供のために用意されたドメイン名であるため，単純にドメイン名でブロックするべきではなく，正規サービスは誤って妨害しないように，例えば

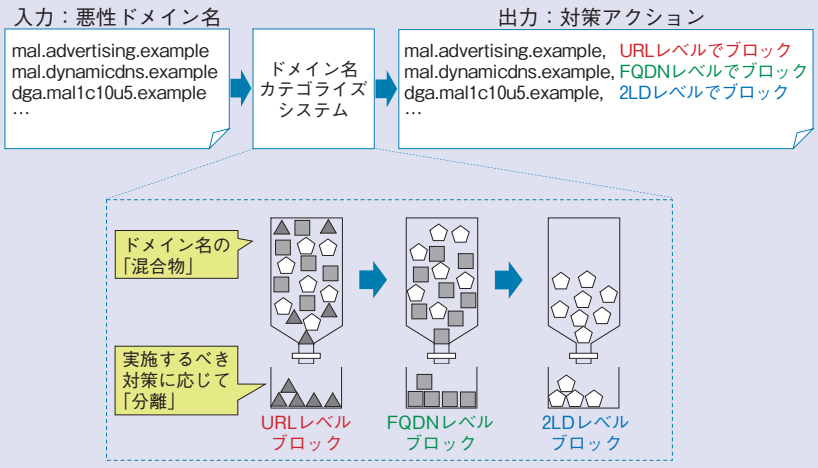

図4　ドメイン名のカテゴライズ技術

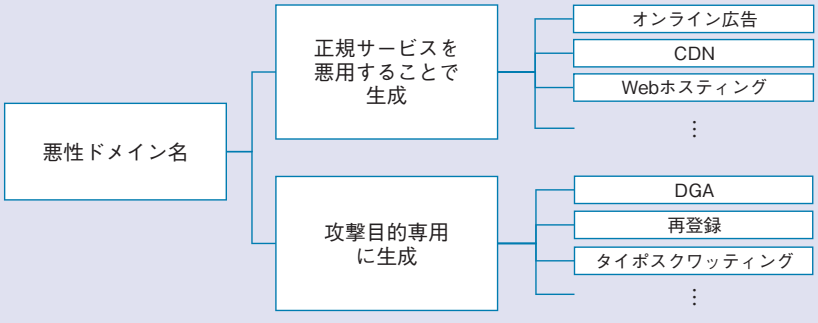

図5　悪性ドメイン名の生成構造解析

URL単位で対策用の情報を生成する必要があります．2番目のカテゴリは，攻撃目的専用に生成された悪性ドメイン名です．例えば，DGAで生成されたドメイン名や，攻撃者によって再登録されたドメイン名，ユーザのタイプミスをねらって取得されるタイポスクワッティングと呼ばれるドメイン名が該当します．これらの悪性ドメイン名のように攻撃のみに利用されるドメイン名であれば，積極的にドメイン名でブロックすることで攻撃の被害を防ぐことができます．

悪性ドメイン名の生成構造を正確にとらえるカテゴライズ技術を創出した結果，さまざまな生成構造を持つ大量な悪性ドメイン名から構成されるいわば「混合物」から，各悪性ドメイン名に対して最適な対策アクションを提示するシステムを実現しました．このシステムにより，正規サービスへの悪影響を発生させない範囲で，もっとも効果的な対策用情報をセキュリティインテリジェンスとして提示することができるようになりました．

実際の悪性ドメイン名に対して，本カテゴライズ技術を適用した結果，生成された対策アクションを利用することで，正規サービスは一切妨害せずに，サイバー攻撃のみを効果的に防ぐことができました．本技術をまとめた論文[3]は，メジャーな学術会議で採録されるなど，世界で認められています．

MDRを支えるマルウェア解析技術

標的型攻撃などマルウェアの高度化に伴い，従来のネットワークレベルのセキュリティ監視を拡張し，レスポンスを含めて対応するMDR（Managed Detection and Response）や端末内の挙動を含めて監視を行うEDR（Endpoint Detection and Response）が注目を浴びています．

SC研では，MDRサービス高度化のために，端末内でのマルウェアの悪性挙動を検知する根拠となる定義ファイル，IOC（Indicator of Compromise）の自動生成技術の研究開発に取り組んでいます．具体的には，マルウェアを投入すると，高度なマルウェア解析技術で解析し（**図6**①），そのマルウェアに特有の挙動を抽出し（図6②），それらを基にNTT独自のIOCである，カスタムIOCを生成します（図6③）．

NTTのお客さまのネットワークから収集したマルウェアを基に生成したカスタムIOCを適用することで，一般

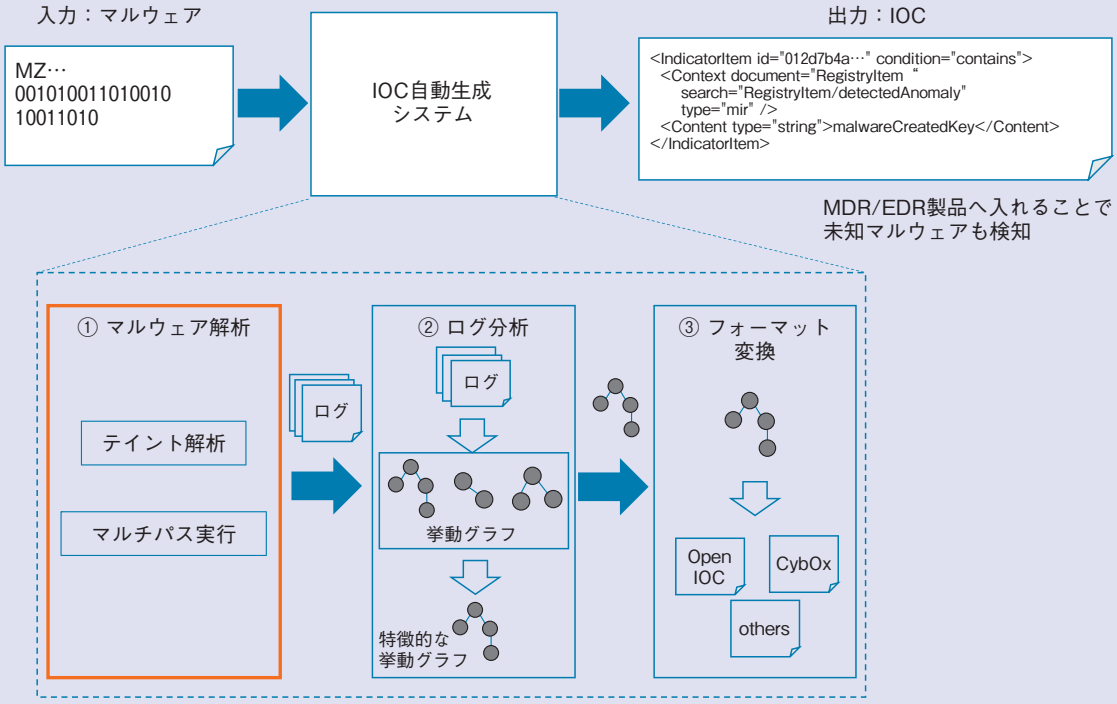

図6　IOC自動生成技術

的な攻撃から防御することを目的に設計されたベンダ提供のIOCでは検知することができない，NTTのお客さまをねらう特有の攻撃を検知できるようになり，お客さまのネットワークや資産を守るのに適したMDRサービスを提供することができます．

■従来技術の問題点

通常マルウェアは解析や検知されることを避けるため，さまざまな解析妨害機能を持っています．例えば，悪意のあるコードの一部を他プロセスに注入するコード注入や，自身が仮想マシン上で動作していることを検知するVM（Virtual Machine）検知などです．

⑴　コード注入

コード注入は，正規のプロセス（例えばexplorer.exe）に対してコードの一部を注入し，その正規プロセスの中で悪意のある行動を行います．通常のマルウェア解析，検知システムはマルウェアの実行プロセスは監視対象としますが，正規のプロセスは監視対象外としていることが多く，正規プロセスの中で行われた挙動を見逃してしまうことがあります．また，正規プロセスを監視対象としていた場合でも，正規のプロセスの正規のコードが行った挙動と，正規のプロセスの悪意のあるコードが行った挙動の区別が難しくなってしまいます（**図7** ⒜）．

⑵　VM検知

VM検知は，マルウェア自身が動作している環境の情報を収集し，VM上で動作しているかを判断します．マルウェアがVM上で動作していると分かると悪意のある活動を停止し，通常とは異なった挙動（無害な挙動）をとることで解析，検知システムを欺きます．

■テイント解析

本解析システムでは，テイント解析を利用することで，コード注入を追跡し，実行されたマルウェアの挙動を正確に捕らえます（図7 ⒝）．

テイント解析とは，データフロー解析技術の1つで，監視対象とする特定のデータが端末内をどのように移動するかを追跡する技術です．具体的には，監視対象データに対して，テイントタグと呼ばれる識別子を設定します．このテイントタグは通常プログラムの実行環境の外（例えば仮想マシンモニタ内）で管理されます．テイントタグの設定されたデータが移動やコピーされる場合，その移動先，コピー先のデータに対してもテイントタグを伝搬させます．このタグの伝搬を繰り返していくことで端末全体でのデータの流れを解析します．

このテイント解析を利用してマルウェアが持っているデータを追跡することで，マルウェアが自身のコードを正規プロセスに注入しても，その注入

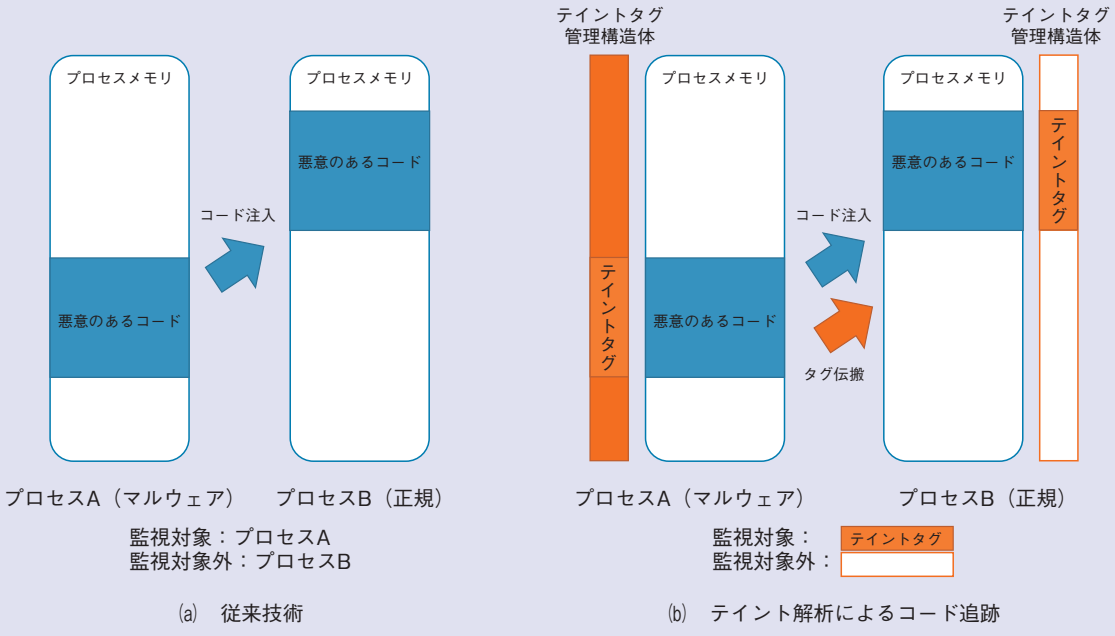

図7　従来技術と本解析システムの比較

動作を追跡し，正規プロセス内にコピーされた悪意のあるコードを特定します．そして，その悪意のあるコード，つまりテイントタグのついたコードが実行されることにより起こる挙動を特定し，正規コードの実行により発生する挙動と正確に区別します[4]．

■マルチパス実行

本解析システムでは，マルウェアの複数パスを解析するマルチパス実行技術を用いて網羅的にマルウェアの挙動を抽出します．

マルチパス実行とは，プログラムが持つ複数のパスをたどり解析する技術です．通常プログラムはさまざまな分岐（例えばif文）を持ちます．この分岐条件に応じて，プログラムの挙動を変化させることで，プログラムとしての処理を行います．マルチパス実行では，プログラムの実行が分岐に達した際，選択された分岐先を記憶しておきます．そのプログラムの実行が終了した後，再度そのプログラムを実行し，先ほど選択した分岐とは異なる分岐先を取るように，実行状態を調整することで実行のたびに異なるパスを実行させることができます．

このマルチパス実行を利用することで，例えばマルウェアがVMを検知した際に通常とは異なる実行パスを選択したとしても，再解析の際に最初とは異なる実行パスを選択させ，マルウェアが本来持っている挙動を引き出すことができます．この技術を利用することで，マルウェアが持つ挙動を網羅的に抽出することができます．

■今後の展開

今後の展開として，上記の技術で生成したIOCを各エンドポイント製品に合わせてチューニングする技術を開発し，さまざまなベンダのエンドポイント製品で私たちのカスタムIOCを利用可能にします．また，それらカスタムIOCを利用しMDRサービスの高度化を行うためにフィールド実験を行います．

セキュリティオーケストレーション

■中小企業でのUTM利用によるサイバー攻撃への対策

近年，公共団体や企業などに対する標的型攻撃やランサムウェアなどサイバー攻撃は進化し続けています．サイバー攻撃は，企業規模に関係なくすべての企業で対策が必要です．一般的には，セキュリティ機器を用いて，ウイルス定義ファイルやシグネチャ更新を基本とした検知と遮断などの対策が行われています．中小企業のお客さまにおいてもセキュリティ意識の高まりにより，低価格で導入可能なUTM（Unified Threat Management）*1の導入が増えています．

次に，日本企業の大多数を占める中小企業向けにサイバー攻撃に対応するための取り組みとして，SC研で開発したリジリエントセキュリティエンジンとUTMを連携させたシステムと，実際にNTTグループでの利用例を紹介します．

■セキュリティオーケストレーションへの取り組み

SC研では，サイバー攻撃から早期回復を図ることを目的として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おり，ICT向けに「リジリエントセキュリティエンジン（RSE）」を開発しました[5],[6]．リジリエントセキュリティエンジンは，データセンタや企業内のネットワーク上に設置され，WAF（Web Application Firewall）やファイアウォールなどのさまざまなセキュリティ機器からログなどの情報を収集します．収集した情報を分析することで攻撃を検知し，検知結果に基づきさまざまなセキュリティ機器への自動対処の実施や，オペレータに攻撃検知を提示，対処策を提案（リコメンド）することでサイバー攻撃に対して迅速な対応やオペレータの稼働削減が可能になります．

さらにリジリエントセキュリティエンジンは，外部からの攻撃だけでなく，標的型攻撃・ゼロデイ攻撃といったすでに内部潜入されているマルウェア外部アクセス遮断を目的として，各セキュリティベンダが提供する膨大な脅威情報基盤（ブラックリスト）からファイアウォールやUTMに設定可能な量でかつ優先度の高いブラックリストを抽出する機能を持ち，これをファイアウォールやUTMに設定することで複数セキュリティベンダの脅威情報を設定している状態と同等の効果を実現できます（**図8**）．

■リジリエントセキュリティエンジンを活用したUTMソリューションと事業会社での利用例

急増する中小企業のセキュリティニーズに対応するため，NTT東日本では，お客さまから受託しUTMの保守運用を行っています．リジリエントセキュリティエンジンは，NTT東日本が保守運用しているUTMへSC研の脅威情報基盤である「マルウェア対策用ブラックリスト（RELIEF）*2」を

*1 UTM：ファイアウォールやウイルス対策，IPS（不正侵入防御），迷惑メール対策，Webフィルタなど，複数のセキュリティ機能を統合した機器です．

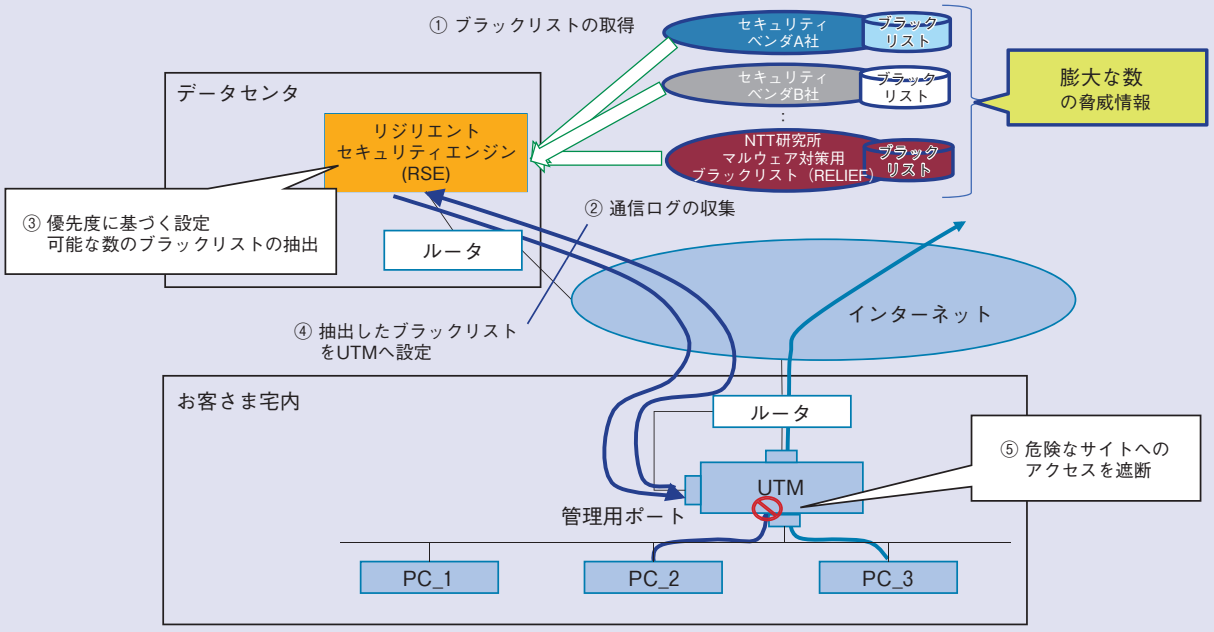

図 8　RSEを活用したUTMソリューション

配信することにより，UTMが持っているブラックリストに加え，SC研のブラックリストを追加することが可能になります．これにより，NTT東日本が保守運用するUTMをご利用のお客さまは，より安全にネットワークの利用ができるようになります．このようにリジリエントセキュリティエンジンは，NTTグループと他社とのセキュリティサービスの差別化や急激な成長を遂げているUTM市場において安心・安全を付加価値としたサービス提供を可能にします．

■今後の展開

今後は，セキュリティアプライアンスを提供する実フィールドへの適用を増やし，ブラックリストだけでなく他の情報も含めた新たな対処策創出に取り組みます．

*2　マルウェア対策用ブラックリスト（RELIEF）：NTTセキュアプラットフォーム研究所独自の脅威情報基盤であり，ハニーポットや動的解析により生成される他社での発見が困難な悪性サイトを含んだブラックリストです．

■参考文献

⑴ 針生・横山・畑田・矢田・八木・秋山・幾世・高田・千葉・田中：“NTTグループのセキュリティビジネスを支えるマルウェア対策用セキュリティインテリジェンス，” NTT技術ジャーナル，Vol.27，No.10，pp.18-22，2015.
⑵ D. Chiba, T. Yagi, M. Akiyama, T. Shibahara, T. Yada, T. Mori, and S. Goto：“DomainProfiler: Discovering Domain Names Abused in Future，” Proc. of DSN 2016，pp.491-502，Toulouse，France，June 2016.
⑶ D. Chiba, M. Akiyama, T. Yagi, T. Yada, T. Mori, and S. Goto：“DomainChroma: Providing Optimal Countermeasures against Malicious Domain Names，” Proc. of COMPSAC 2017，pp.643-648，Turin，Italy，July 2017.
⑷ Y. Kawakoya, M. Iwamura, E. Shioji, and T. Hariu：“API Chaser: Anti-analysis Resistant Malware Analyzer，” RAID 2013，LNCS，Vol.8145，pp.123-143，2013.
⑸ 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.
⑹ 小山・胡・永渕・塩治・高橋：“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，” NTT技術ジャーナル，Vol.27，No.10，pp.23-26，2015.

（上段左から）川古谷　裕平/ 千葉　大紀
針生　剛男/ 八木　毅/
秋山　満昭
（下段左から）永渕　幸雄/ 小山　高明

NTTセキュアプラットフォーム研究所では，今後もさまざまなサイバー攻撃対策技術の研究開発やビジネス化に取り組み，進化し続けるサイバー攻撃への対策の強化と，安心・安全なサービスの実現をめざします．

◆問い合わせ先

NTTセキュアプラットフォーム研究所
サイバーセキュリティプロジェクト
TEL　0422-59-4908
FAX　0422-59-3844
E-mail　yuuichi.murata.sd@hco.ntt.co.jp