I−3
安心・安全に情報をやりとりできるネットワークセキュリティの研究開発を推進

高橋 幸雄（たかはし ゆきお）
ネットワークセキュリティ研究所
研究所長

出身は島根県の西の端、益田市の中国山脈を見渡せる周りに誰もいない星のきれいな田舎で育ちました。1982 年京都大学理学部(修士)を卒業し、郵政省電波研究所(現 NICT)に入所しました。VLBI と呼ばれる電波望遠鏡を使ったプレート運動、日本等の位置の基準、さらには天文の研究を行い、また、日本の標準時のもとになる日本標準時、さらには位置認証の研究を実施してきました。2008 年情報セキュリティ大学院大学で学位(情報学)を取得しました。毎週自転車の遠乗りとジョギングとお酒を楽しんでいます。

「情報通信社会の中で大きな脅威となっているサイバー攻撃時のセキュリティの課題に関して、安心・安全な情報をやり取りできるように、ネットワークセキュリティの研究開発を推進しています。」

はじめに

今やインターネットに代表される情報通信ネットワークは、生活において不可欠なライフラインの 1 つになっており、またクラウドやスマートフォンなど新しい技術により大きな変革を迎えています。その中で、サイバー攻撃は、DDoS 攻撃や、標的型・APT 攻撃、Web、SNS、メールを介した攻撃など、多種多様でかつ極めて巧妙になってきており、大きな脅威となるとともに、防御や対策が難しくなってきています。サイバー攻撃は、金銭目的や主義主張、さらには国家的な紛争・脅威にも使われ、オールジャパンあるいは国際連携で協力して対抗する必要があります。

ネットワークセキュリティ研究所の目指すもの

ネットワークセキュリティ研究所では、誰もが安心・安全に通信を行うことができるように、NICT の中立性を活用し、サイバー攻撃に対抗するための理論と実践を融合させたネットワークセキュリティの研究開発を実施し、世界的な研究拠点になることを目指しています。

サイバー攻撃は、多くの場合、ウィルス、ワーム、ボット等の総称である“マルウェア”によって引き起こされており、日夜新種の攻撃が出現しています。そのため、日々の攻撃に対応を行う“現在志向”の実践的研究開発と、中長期的視点で攻撃

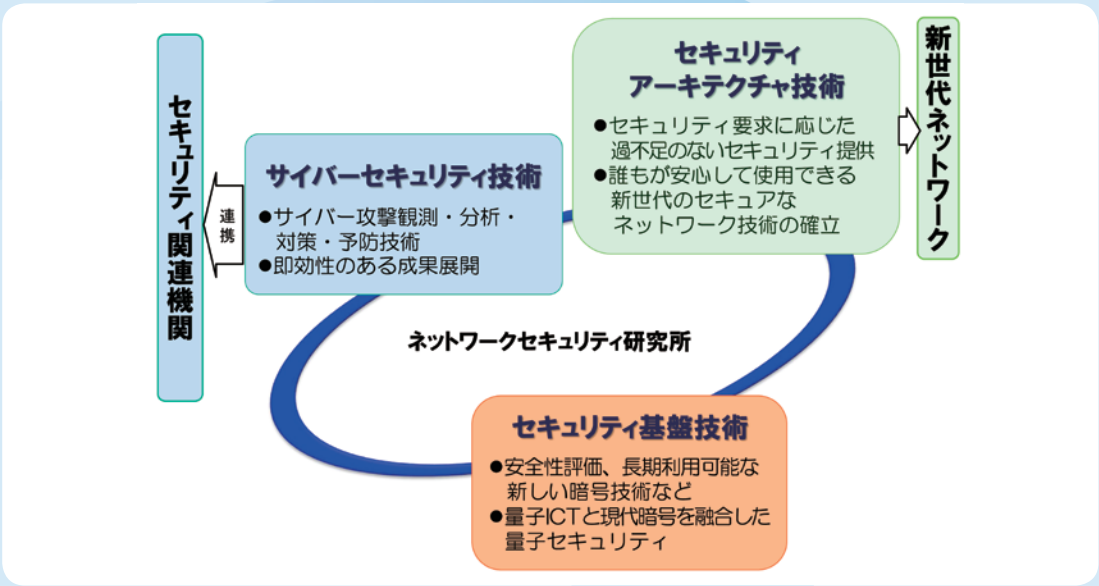


図　ネットワークセキュリティ研究所の3つの研究課題

をしにくくする“未来志向”の先進的研究開発の両輪で推進し、攻撃側優位の現状から防御側優位にしていきたいと考えています。

ネットワークセキュリティ研究所の研究開発について

当研究所は、サイバーセキュリティ技術、セキュリティアーキテクチャ技術、セキュリティ基盤技術の研究開発を、三位一体で実施しながら、ネットワークセキュリティの研究を推進しています。

サイバーセキュリティ技術では、サイバー攻撃をリアルタイムで把握し適切な対応を実施するため観測・分析・対策技術の研究開発を行うとともに、攻撃の前兆を捕えて予防を行うための基盤技術を確立し、攻撃者にとって抑止力となる実践的かつ先行的対策を可能にしていきます。また、Web、SNS、スパムメール等のサービスレイヤでのサイバー攻撃や標的型攻撃に対応した観測・分析・対策の技術開発を進めていきます。さらに、得られたマルウェアや攻撃トラフィックのデータを、研究や人材育成に役立てることで、日本のセキュリティ技術のポテンシャル向上に貢献していきます。

セキュリティアーキテクチャ技術では、クラウドやモバイル技術の急速な発展による多様化したネットワーク環境や利用環境に対応し、利用者の要求に応じたセキュリティが確保できるアーキテクチャ技術の研究開発を実施しています。多様化したネットワーク環境では、インターネットのような一様なネットワーク、一様なセキュリティでは対応できなくなり、安全性も不十分となってしまいます。そのため、サイバー攻撃の回避、複雑度の高いシステムに対応可能な過不足のない脆弱性管理、大規模認証などが行えるセキュアな新しいネットワークを実現するための技術開発を行っていきます。

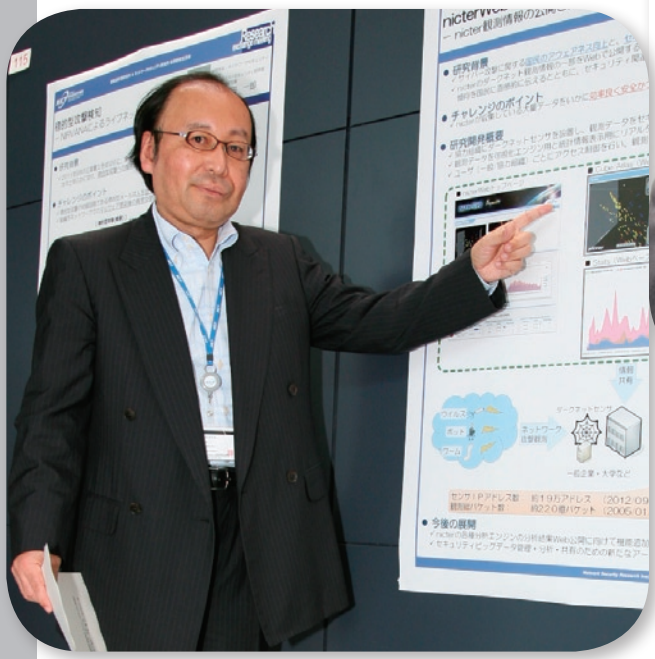
セキュリティ基盤技術では、盗聴検知が可能で極めて安全性が高い量子セキュリティ技術や、既存の現代暗号よりも遥かに安全性が高く超高速の量子計算機が実現しても安全な長期間利用可能な新しい暗号技術を開発していきます。また、電子政府推奨暗号リストの維持等への貢献など、暗号の安全性に関する研究や活動を行っていきます。

おわりに

研究の成果展開や社会貢献を積極的に行い、国内外の研究機関等とも連携し、国民誰もが安心・安全に情報通信を行うことができるように研究開発を進めて参ります。

インシデント分析センター nicter

ー世界最先端のサイバーセキュリティ技術の研究開発ー



「nicter は進化型のセキュリティフレームワーク。日本の、そして世界のセキュリティを向上させるため、実践的なサイバーセキュリティ技術の研究開発を行っています。」

中尾 康二 (なかお こうじ)
ネットワークセキュリティ研究所
主管研究員

1979 年早稲田大学卒業後、国際電信電話株式会社に入社。KDD 研究所を経て、現在 KDDI 情報セキュリティフェロー、及び NICT ネットワークセキュリティ研究所 主管研究員兼務。ネットワーク及びシステムを中心とした情報セキュリティ技術に関わる技術開発に従事。

井上 大介 (いのうえ だいすけ)
ネットワークセキュリティ研究所
サイバーセキュリティ研究室 室長

2003 年横浜国立大学大学院工学研究科博士課程後期修了後、独立行政法人通信総合研究所(現 NICT)に入所。2006 年より nicter の研究開発に従事。現在ネットワークセキュリティ研究所 サイバーセキュリティ研究室 室長と、ネットワーク研究本部 ネットワークシステム総合研究室 研究マネージャーを兼務。博士(工学)。SF 小説や SF 映画、テクノ、ハウス、エレクトロがエネルギー源。

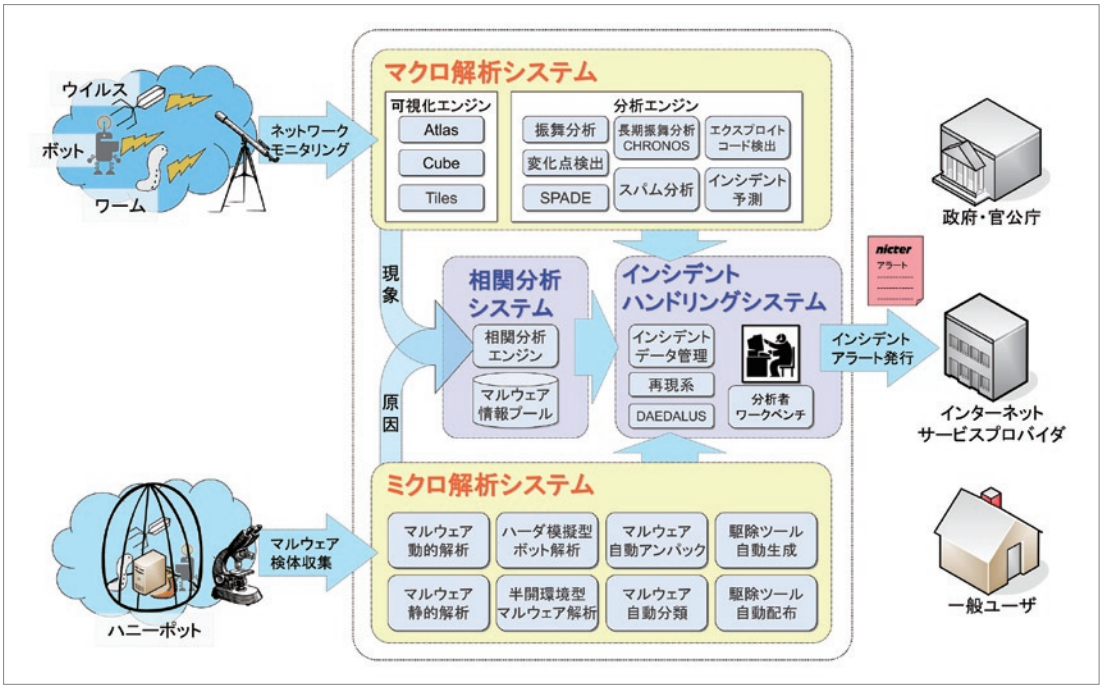


図1　nicterの全体像

はじめに

インターネットは私たちの社会活動や経済活動に多大な恩恵をもたらし、インターネット普及以前の時代にはもはや逆戻りできない不可逆的変化を現代社会の隅々にまで及ぼしています。一方、その発展と同調するように、インターネットにおけるサイバー攻撃の脅威も拡大の一途を辿っています。サイバー攻撃は人間であるクラッカー*1 が引き起こすものですが、そのツールとして使われるのがマルウェア*2 と呼ばれる不正なプログラムです。90 年代前半までマルウェアは愉快犯もしくは自己顕示を目的として作成・流布されることが多かったのですが、90 年代後半以降は金銭詐取を目的とした組織的な犯罪のツールとして利用され始め、高度化・巧妙化が急速に進んでいます。

このような、マルウェアに起因するサイバー攻撃に対抗するために、ネットワークセキュリティ研究所サイバーセキュリティ研究室では、インシデント分析センター nicter*3 の研究開発を進めています。

インシデント分析センター nicter

nicter はリモート感染型マルウェア*4 の世界的な活動傾向をリアルタイムに把握し、それに起因したサイバー攻撃の早期発見、原因究明、対策導出を可能にするため、マクロ解析システム、ミクロ解析システム、相関分析システム、インシデントハンドリングシステムの 4 つのサブシステムから構成されています(図 1)。以下では、これらのサブシステムの概要を紹介します。

● マクロ解析システム

マクロ解析システムでは、国内外の複数地点に観測用のセンサを設置し、「未使用」の IP アドレス

*1　悪意を持ってハッキング行為を行う者。
*2　ウィルス、ワーム、トロイの木馬、スパイウェア、ボットなど情報漏えいやデータ破壊、他のコンピュータへの感染など有害な活動を行うソフトウェアの総称。"malicious"と"software"を組み合わせた造語。
*3　Network Incident analysis Center for Tactical Emergency Response.
*4　ネットワークを経由して能動的に攻撃を行うことで感染を広げるタイプのマルウェア。最近では 2008 年 11 月に感染爆発を起こした Conficker や、2011 年 8 月から増加傾向が確認されている Morto などが有名。

を大量*5 に観測しています。本来、未使用の IP アドレスに対して通信は成立し得ませんが、実際に観測してみると相当数のパケットが届きます。これらの大部分は、マルウェアが次の感染対象を探すためのスキャンや、マルウェア同士が P2P ネットワークを確立するためのランデブー用の通信など、マルウェアに起因したパケットなのです。したがって、未使用の IP アドレス（以下、ダークネット）を観測・分析することによって、インターネットにおけるセキュリティインシデントの一大要因となっているマルウェアの活動傾向を捉えることが可能になります。以下、マクロ解析システムに含まれる可視化エンジンについて概説します。

(1) Atlas

Atlas（図 2）は、ダークネットに流れ込むトラフィック（以下、ダークネットトラフィック）を世界地図上でリアルタイムにアニメーション表示する可視化エンジンです。ダークネットに到着したパケットの 1 つ 1 つについて、送信元 IP アドレスから送信元の緯度・経度を割り出し*6、その送信地点から宛先 IP アドレスが属する国の首都に向けてパケットが飛来する様子をアニメーション表示することで、世界的なマルウェアの活動傾向を直感的に把握することができます。各パケットの色はパケットの種別*7 を表し、パケットの軌道の高さはポート番号の大きさに比例（対数軸）しています。また、マウス操作による視点の変更や拡大縮小、パケットオブジェクトのクリックによる詳細情報の表示など、分析者のインタラクティブな操作が可能です。

(2) Cube

Cube（図 3）は、ダークネットに到達したパケットを、その送信元と宛先の各種情報に基づいて、三次元空間に浮かぶ立方体中にアニメーション表示する可視化エンジンです。立方体の縦軸に送信元 / 宛先 IP アドレスを、横軸に送信元 / 宛先ポート番号を取り、送信元（図 3 の左平面）から宛先（図 3 の右平面）に向けてパケットを通過させることで、マルウェアによるスキャンの形状などが可視化されます。Cube は Atlas と同様、マウス操作による視点の変更や拡大・縮小、パケットの詳細情報などを表示でき、送信元ホストからの攻撃の様子をリアルタイムに把握することが可能です。

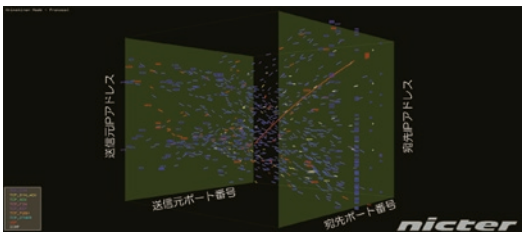


図3　Cube

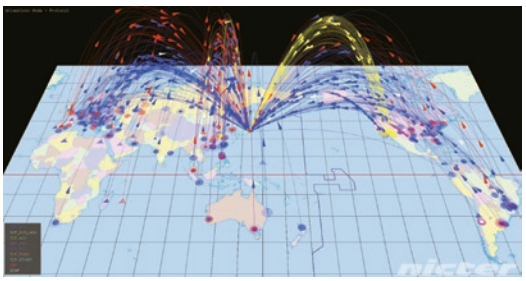


図2　Atlas

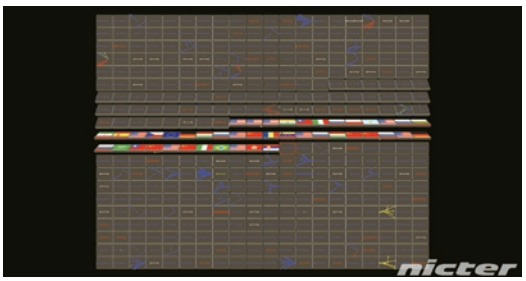


図4　Tiles

*5　2012 年 3 月末現在で約 19 万の IPv4 アドレス。
*6　IP アドレスと緯度・経度のマッピングは MaxMind 社の GeoIP City Database を利用
*7　青：TCP SYN、黄：TCP SYN-ACK、緑：TCP ACK、桃色：TCP FIN、紫：TCP RST、橙：TCP PUSH、水色：TCP OTHER、赤：UDP、白：ICMP（後述の Cube、Tiles における色も同様）

(3) Tiles

Tiles(図 4) はダークネットトラフィックを送信元ホストごとにスライスし、各ホストの短期間(30 秒間) の挙動を分析・可視化するエンジンです。図 4 の小さなタイルの 1 つ 1 つが送信元ホストごとの挙動を表しており、最新の分析結果に随時更新されていきます。タイルの裏側は送信元ホストが属する国の国旗が示されています。1 つのタイルは、パケットの時刻、送信元 / 宛先ポート番号、宛先 IP アドレスを用いて可視化および分類されます。この分類の履歴を蓄積することによって、ある送信元ホストの挙動が既知のスキャンパターンであるのか、あるいは新規のスキャンパターンであるのかをリアルタイムに判定することが可能となります。

マクロ解析システムでは前述の可視化・分析エンジンに加えて、図 1 上部に示すような各種分析エンジンの研究開発を行っています。

● ミクロ解析システム

ミクロ解析システムは、ハニーポットと呼ばれる囮(おとり)サーバや Web サイトの巡回を行う Web クローラなどでマルウェアの検体を捕獲し、その検体を自動解析するシステムです。以下、ミクロ解析システムに含まれる動的解析エンジン(図 5) について概説します。

リアル空間においてウィルスをシャーレで培養して観察するように、動的解析はマルウェアをサンドボックスと呼ばれる箱庭環境で実行し、その際にマルウェアが使用した API[*8] やネットワークアクセスなどの挙動を解析する手法です。ところが、近年の高度化されたマルウェアは動的解析に対抗するため、自己の周囲のネットワーク環境を調査して、自己がサンドボックス内にいることを検知すると実行停止や自己消去を行なうなどの解析回避機能を持っています。そのため、nicter の動的解析エンジンは、サンドボックス内に DNS サーバや Web サーバなど多数のダミーサーバからなるインターネットエミュレータを配置することで、マルウェアの解析回避機能を無効化しています。また、マルウェアが解析回避のために行う仮想マシン検出に対抗するため、マルウェアを実行する犠牲ホストは OS 自動復元機構を持った実マシンによって構成されています。

このようなサンドボックス内での動的解析の結果、犠牲ホストからは API ログが、インターネットエミュレータからはサーバログが出力され、それらのログからマルウェアの挙動が抽出できます。加えて、犠牲ホストとインターネットエミュレータの間で観測されるパケットデータに含まれるスキャンが、後述する相関分析の鍵となります。

動的解析エンジンは 1 検体あたり 6 ～ 9 分の高速な解析を実現し、さらに解析の並列化により 1 日あたり最大 7,000 検体の解析が可能となっています[*9]。

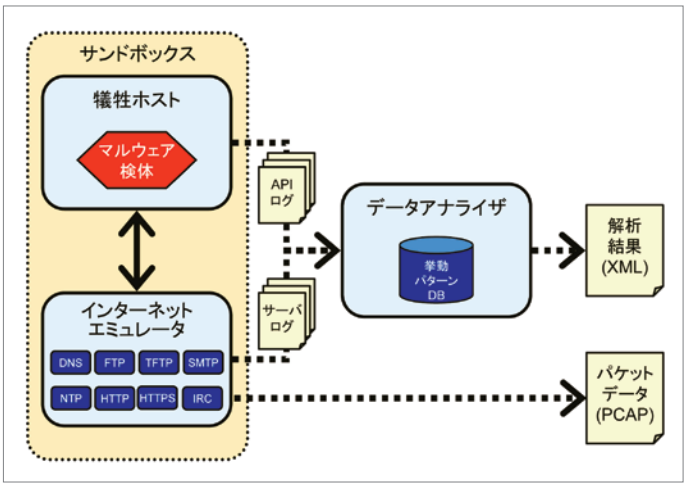


図5　マルウェア動的解析エンジン

*8　Application Program Interface.
*9　2012 年 3 月末現在。

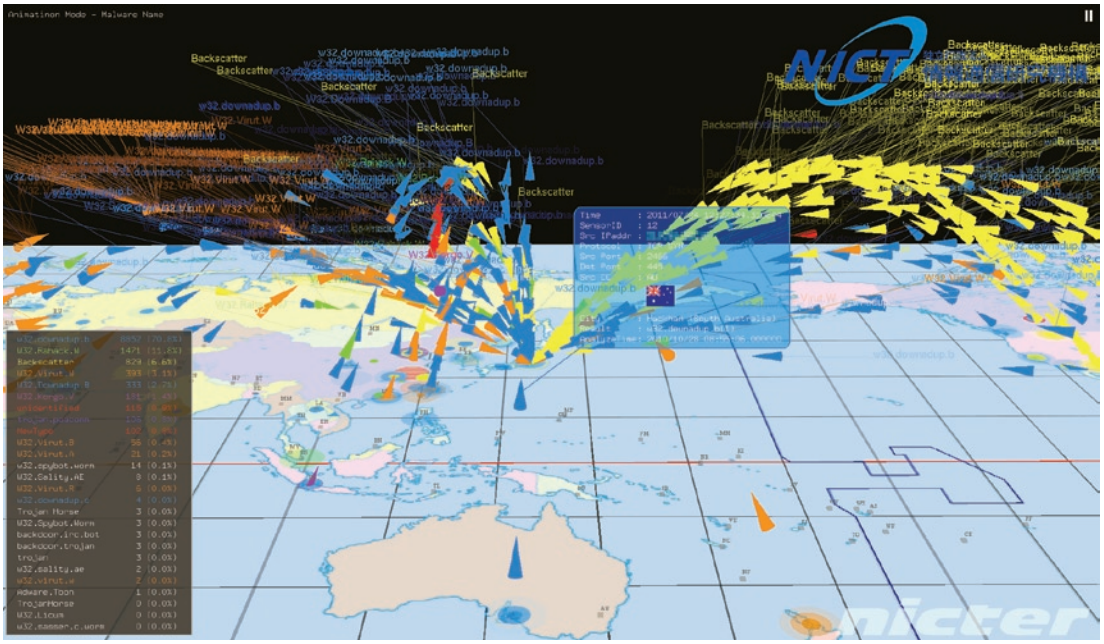


図6　相関分析結果の可視化

ミクロ解析システムでは、前述の動的解析エンジンに加えて、図1下部に示すような各種解析エンジンの研究開発を行っています。

● 相関分析システム

相関分析システムは、マクロ解析システムにおいて観測されたマルウェアからのスキャンを各種の特徴*10によってプロファイリングし、ミクロ解析システムにおいてマルウェアから抽出されたスキャンのプロファイルとの照合を行い、類似したプロファイルを持つマルウェアの候補を探し出します。つまり、マクロ解析システムで捉えた「現象」(サイバー攻撃)と、ミクロ解析システムで蓄積した「原因」(マルウェア)とを結びつける答え合わせのシステムです。マクロ解析結果とミクロ解析結果はマルウェア情報プール(MNOP: Malware kNOwledge Pool)に蓄積されるとともに、相関分析エンジンによってリアルタイムに照合が行われます。

図6は可視化エンジンAtlas上で相関分析結果を可視化したものです。各パケットオブジェクトの上方に、相関分析の結果、第一候補として挙げられたマルウェア名を表示しています。また、パケットの詳細情報の中にもマルウェア名(図6の例ではw32.downadup.b)を表示しています。さらに、相関分析の結果を累計することで、マルウェアの世界的な活動傾向を把握することが可能となります。図6の左下のボックスは、相関分析結果(マルウェア名ごとのユニークホスト数)の累計を表しており、2011年時点で70%を超えるホストがw32.downadup.b(あるいはそれと同様のスキャンエンジンを持つマルウェア)に感染しているものと自動推定しています。

● インシデントハンドリングシステム

インシデントハンドリングシステムは、マクロ解析、ミクロ解析、相関分析の各サブシステムからの出力を集約・蓄積し、インシデント発生時の

*10 パケットのプロトコル、TCPフラグ、送信元ポート番号およびその変化、宛先ポートのセット、宛先IPアドレスの遷移(シーケンシャル/ランダム)、単位時間あたりのパケット数、ペイロード長など。

データ管理や、その再現を可能にします。また、DAEDALUS[*11] はnicterの大規模ダークネット観測網を応用したアラートシステムです。以下、DAEDALUSについて概説します。

従来のダークネット観測は組織外からダークネットに飛来するパケットを観測する、つまり“外から内”への異常な通信を収集するという考え方でした。一方、DAEDALUSは組織内から送出されたパケットを分散配置されたダークネットで観測する、つまり“内から外”(または内から内)への異常な通信を網にかけるという、従来とは逆転したダークネットの活用法に基づいています。換言すると、DAEDALUSは組織内で起こったマルウェア感染などをダークネットによって検知し、該当する組織にアラートを自動送信することで、ダークネット観測をサーバやホストが存在するライブネットの保護に活かすシステムです。

図7はDAEDALUSの可視化エンジンです。中央の球体がインターネット、その周りを周回している各リングが、nicterのセンサを設置している各組織のネットワークを表しています。球体とリングの間を飛び交う流星状のオブジェクトはダークネットトラフィックを表しています。リングの水色の部分がライブネット、濃紺の部分がダークネットであり、リングの外周の「警」のマークは組織内でアラートの原因となった送信元ホストを指し示しています。この可視化エンジン上でのアラート表示と同時に、該当組織にはメールベースのアラートが自動送信され、実際のセキュリティオペレーションのトリガとして活用されています。

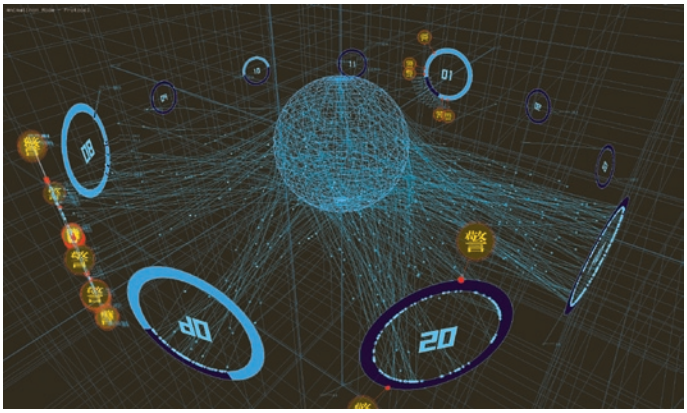


図7　DAEDALUSの可視化エンジン

まとめと今後の課題

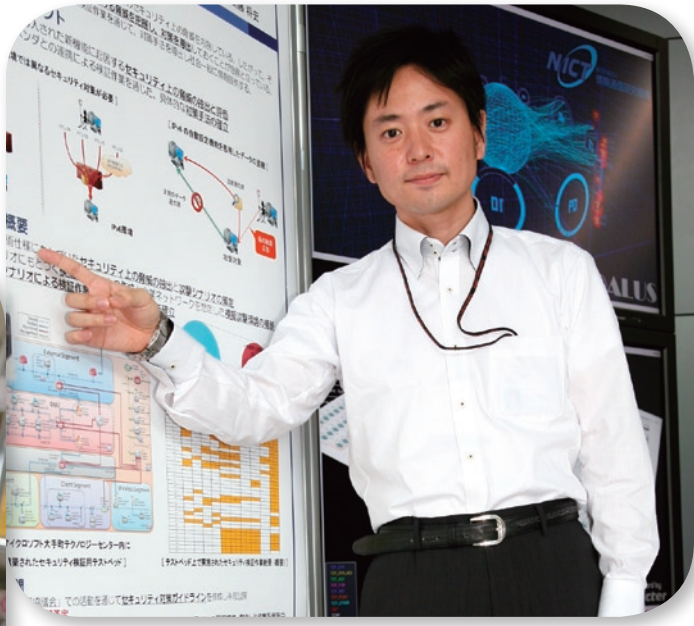
本稿では、セキュリティインシデントの早期発見、原因究明、対策導出を目的としたインシデント分析センターnicterについて概説しました。nicterの研究開発によって、ネットワーク経由で感染を広げるリモート感染型マルウェアの大局的な活動傾向の把握と迅速な原因究明が可能となり、その分析結果の一部はnicterWeb[*12] というサイトから一般公開を行っています。また、nicterの大規模ダークネット観測網を応用したアラートシステムDAEDALUSの外部展開など、研究成果の社会還元を推進しています。

一方、本稿の冒頭でも述べたように、インターネットにおける脅威は日々進化しており、Webを媒体とした攻撃手法(ドライブ・バイ・ダウンロード攻撃)や、SNSを媒介したマルウェア、特定の組織を狙った標的型攻撃など、これまでのnicterの仕組みでは捉えられない新たな脅威が生まれてきています。今後も、このような新たな脅威に対抗可能な実践的研究開発を推進するとともに、攻撃者側が圧倒的に有利な現在の状況を一変させ得る根源的なセキュリティ技術の研究開発を、産学官の連携の下に取り組んでいきます。

*11 Direct Alert Environment for Darknet And Livenet Unified Security.
*12 http://www.nicter.jp/

ネットワークリアルタイム可視化システムNIRVANA

ートラフィックの「今この瞬間」を描き出すネットワーク管理支援ツールー



「複雑化するネットワークを見える化し、ネットワーク管理を『苦しみのない世界』に。NIRVANA は nicter からスピンオフした強力なネットワーク管理支援ツールです。」

井上 大介（いのうえ だいすけ）
ネットワークセキュリティ研究所
サイバーセキュリティ研究室 室長

2003 年横浜国立大学大学院工学研究科博士課程後期修了後、独立行政法人通信総合研究所（現 NICT）に入所。2006 年より nicter の研究開発に従事。現在ネットワークセキュリティ研究所 サイバーセキュリティ研究室 室長と、ネットワーク研究本部 ネットワークシステム総合研究室 研究マネージャーを兼務。博士（工学）。サッカーアルゼンチン代表と S.S. ラツィオがエネルギー源。

衛藤 将史（えとう まさし）
ネットワークセキュリティ研究所
サイバーセキュリティ研究室 主任研究員

2005 年、NICT 入所。以来、nicter プロジェクトや IPv6 セキュリティなど、情報通信セキュリティ技術の研究開発に従事。nicter プロジェクトでは主に次世代型サイバー攻撃観測プラットフォームの研究に取り組む。博士（工学）。

はじめに

ネットワークが生活空間の隅々にまで張り巡らされ、地球上のどこかに蓄積された膨大なデータにハンドヘルドデバイスやタブレットコンピュータからアクセスし、海外にいる同僚とリアルタイムにビデオ会議をする…。私たち 21 世紀初頭の人類を取り巻く通信環境は、スタートレックの生みの親、ジーン・ロッデンベリー氏の豊かな空想をも上回るスピードで進化を続けているようです(もちろん亜空間通信はまだ実現していませんが)。しかしながら、その通信環境を支えるネットワークの管理は、エンタープライズ号の艦内のようにコンピュータ任せとはいかず、現代のネットワーク管理者達を悩ませ続けています。

そこで、ネットワークセキュリティ研究所サイバーセキュリティ研究室では、通信環境の進化とともに複雑化するネットワーク管理の負荷を軽減するために、ネットワークリアルタイム可視化システム NIRVANA*1 の開発を行っています。NIRVANA は、ネットワークを流れるトラフィックをリアルタイムに可視化することで、ネットワークの疎通確認や障害検知、輻輳の把握や設定ミスの検出などを迅速に行うことを可能にし、組織のネットワーク管理の効率を劇的に向上させる支援ツールです。そして、その可視化の仕組みは、同研究室で研究開発を進めているインシデント分析センター nicter で培ってきた技術群を応用したものです。

ダークネットからライブネットへ

インシデント分析センター nicter は、サイバー攻撃の発生を早急に把握するために、インターネット上に複数のセンサを設置し、未使用の IP アドレス(以下、ダークネット)の大規模観測を行っています。ダークネットにはマルウェアが次の感染対象を探すためのスキャンなど、不正なトラフィック(以下、ダークネットトラフィック)が大量に届きます。nicter では、ダークネットトラフィックを自動分析すると同時にリアルタイムに可視化し、迅速なセキュリティオペレーションを実現するための研究開発を行っています。

この nicter のダークネットトラフィック向けに開発した可視化技術を、ライブネットトラフィック(ユーザ端末やサーバ等が接続された実ネットワークを流れる通信)に応用し、強力なネットワーク管理支援ツールとしてスピンオフしたシステムが NIRVANA なのです。

NIRVANA のシステム構成

NIRVANA は、観測対象ネットワークからトラフィックを収集するセンサシステム、収集したトラフィックを集約するゲートシステム、集約されたトラフィックを視覚化する可視化システムという 3 つのサブシステムからなります(図 1)。これは、nicter のダークネット観測システムから継承したシステム構成です。

センサシステムには、観測対象ネットワークからポートミラーリングやネットワークタップによって複製・分岐されたライブネットトラフィックを入力します。また、sFlow*2 によってサンプリングされた情報を入力することもでき、組織のネットワーク環境に応じた柔軟な観測方法を選択可能です。センサシステムは観測対象ネットワークに複数設置できるため、例えば、組織のネットワークが日本各地に分散しているような場合にも対応できます。

ゲートシステムは、センサシステムにおいてパケットサマリデータ*3 に変換されたライブネットトラ

*1 nicter real-network visual analyzer
*2 高速・大容量化したネットワーク管理の効率化を可能にする、ネットワークスイッチ等における情報収集技術のインターネット標準(RFC 3176)。
*3 パケットをネットワーク層とトランスポート層のヘッダ情報と、アプリケーション層のハッシュ値に圧縮したデータ。ライブネットトラフィックに比べ、大幅なデータ量の削減が可能。

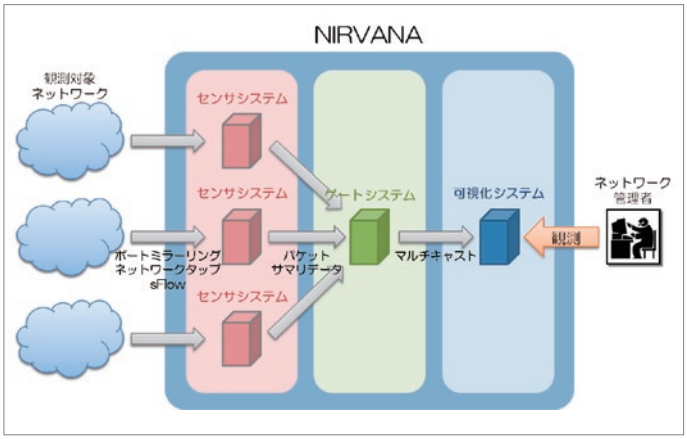


図1　NIRVANAのシステム構成

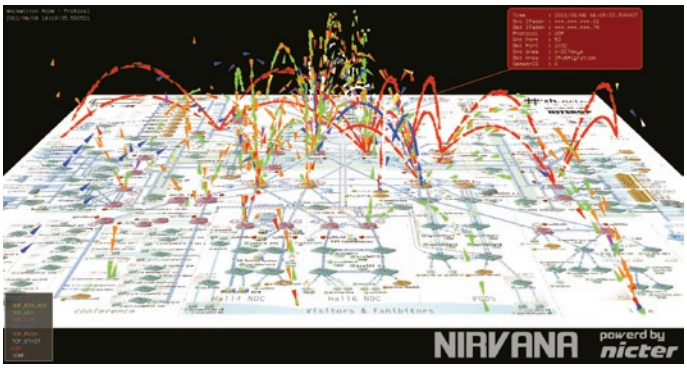


図2　NIRVANAによるライブネットトラフィックの可視化（パケットモード）*4

NIRVANAによるライブネットの可視化

NIRVANAの可視化システムは、リアルタイム性、インタラクティブ性、カスタマイズ性を重視して設計・開発されています。リアルタイムに可視化されたライブネットトラフィックは、ネットワーク管理者の操作によってインタラクティブに拡大縮小や視点切替え、一時停止、詳細情報の表示などが行えます。また、3Dオブジェクトの形状や色、軌道の高度、スピードなど多岐に渡るパラメータをカスタマイズ可能です。さらに、フィルタリング機能も充実しており、送信元 / 宛先IPアドレスやプロトコル、ポート番号、センサシステムのIDなどによってトラフィックのフィルタリングが可能です。

NIRVANAにはパケットモードとフローモードという2つのモードがあります。パケットモードは、ライブネットトラフィックをパケット単位で可視化するモードであり、ネットワークの疎通確認や、経路の障害検知などに威力を発揮します。図2は、Interop Tokyo*6 2011の展示会場ネットワーク「ShowNet*7」にNIRVANAを導入し、パケットモードでトラフィックを可視化したものです。各パケット(ロケット)の色はパケットの種別*8を表し、パケットの軌道の高さはポート番号の大きさに比例(対数軸)しています。また、図右上の赤色のウインドウには、選択されたパケットの詳細情報が表示されています。パケットはルータをホップするように流れていきますが、これにはOSPF*9によって

フィックを集約し、可視化システムに向けてマルチキャストします。組織のネットワーク規模に応じて、ゲートシステムを複数設置することも可能です。

可視化システムは、ゲートシステムからマルチキャストされたパケットサマリデータを受信し、リアルタイムに3Dアニメーション表示します。可視化に必要な情報はマルチキャストされていますので、ネットワーク管理者が複数いるような場合でも、可視化システムのハードウェアを追加してマルチキャストを受信すれば、多地点でのモニタリングが可能になります。可視化システムは単体動作させることも可能であり、ローカルに保存したPCAPファイル*5を再生して可視化することができます。

*4 Copyright (c) Interop Tokyo 2011 NOC Team Member and NANO OPT Media, Inc. All rights reserved.
*5 ネットワーク上を流れるパケット情報を保存するためのファイル形式。多くのネットワーク管理ツール(tcpdump、Wireshark 等)で利用されています。
*6 例年、数百の出展社が最新のネットワーク機器やソリューションを展示し、同時に多数の講演やコンファレンス等が開催される、ネットワーク分野における世界最大規模のイベント。
*7 国内外のネットワークベンダが世界最先端のネットワーク機器を結集して構築する、Interopの心臓部とも言える展示会場全体のネットワーク。

定期的に取得したルーティングテーブルを利用しており、パケットの送信元 / 宛先 IP アドレスの組からその経路を決定しています。そのため、観測中に経路の変更が起こった場合でも動的に追従可能です。

一方、フローモードはトラフィックの流量を直感的に把握するためのモードです。フローモードではネットワーク機器間のトラフィック量を表現するためにリボン状の曲線を用い、その高さや太さ、色によって相対的な流量を表しています。図 3 は「ShowNet」をフローモードで可視化したものです。図中央の基幹ルータ間のホップが赤いリボンで表現されており、この機器間を流れるトラフィック量がネットワーク中で最大であることが把握できます。また、各機器の上に表示されている青と赤のバーは、それぞれ送・受信パケット数(設定によってはデータ量)を表しています。フローモードを用いることで、ネットワークのボトルネックを迅速に把握することが可能になり、前述のパケットモードとの併用で、ネットワーク管理の負荷を劇的に軽減できます。

NIRVANA の中で描かれるネットワーク図は、汎用の作画ツール Microsoft Visio*11 によって作成できます。NIRVANA はネットワーク図中の各オブジェクト(ネットワーク機器)に設定された IP アドレスを読み込んで、図中の座標に IP アドレスを自動設定することができます。そのため、ネットワークの構成変更が頻繁に起こるような組織でも、容易に NIRVANA のネットワーク図をアップデートすることができます。また、ネットワーク管理者のアイデア次第で、様々なネットワーク図を用いることができます。

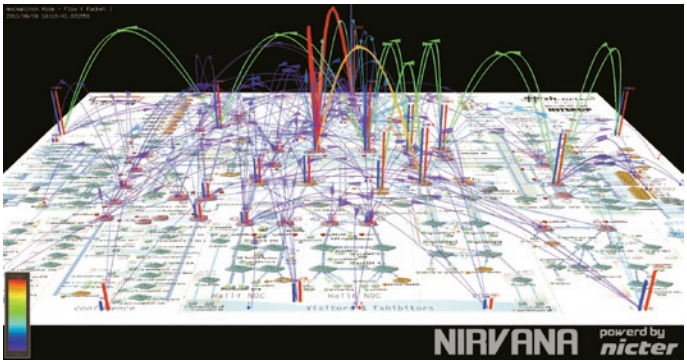


図3　NIRVANAによるライブネットトラフィックの可視化 (フローモード) *10

まとめ

仮想化技術の発達やクラウドコンピューティングの普及などにより、ますます複雑化するネットワーク管理が「苦しみのない世界」となることを目指し、インシデント分析センター nicter の研究成果からスピンオフした NIRVANA の社会展開と、さらなる高度化を進めていきます。

*8　図 2 の例では、青 : TCP SYN、黄 : TCP SYN-ACK、緑 : TCP ACK、桃色 : TCP FIN、紫 : TCP RST、橙 : TCP PUSH、水色 : TCP OTHER、赤 : UDP、白 : ICMP。
*9　Open Shortest Path First。ダイクストラ法によって最短経路のルーティングテーブルを作成するルーティングプロトコル。
*10　Copyright (c) Interop Tokyo 2011 NOC Team Member and NANO OPT Media, Inc. All rights reserved.
*11　Microsoft 及び Visio は、米国 Microsoft Corporation の米国及びその他の国における登録商標又は商標です。

セキュリティ情報交換と標準化（CYBEX）

ー地球規模でのサイバーセキュリティ構築に向けてー

高橋 健志（たかはし たけし）
ネットワークセキュリティ研究所
セキュリティアーキテクチャ研究室 研究員

早稲田大学理工学研究科修了、2002 年 Tampere University of Technology にて研究員、2004 年同大学国際情報通信研究科にて研究員、2006 年（株）ローランド・ベルガー社にてコンサルタントを経て、2009 年より現職。情報通信プロトコル、サイバーセキュリティ、およびマルチメディア符号化に関する研究に従事。好きなことは新たな経験。経験の積み重ねこそが人生と信じ、現在はサイクリング、テニス、クッキング、そして中国語の学習に注力。博士（国際情報通信学）。

「組織・国境を越えた情報交換を促進することにより、サイバーセキュリティを向上させたい。その土台となる情報交換フレームワークについて、研究・標準化活動を展開しています。」

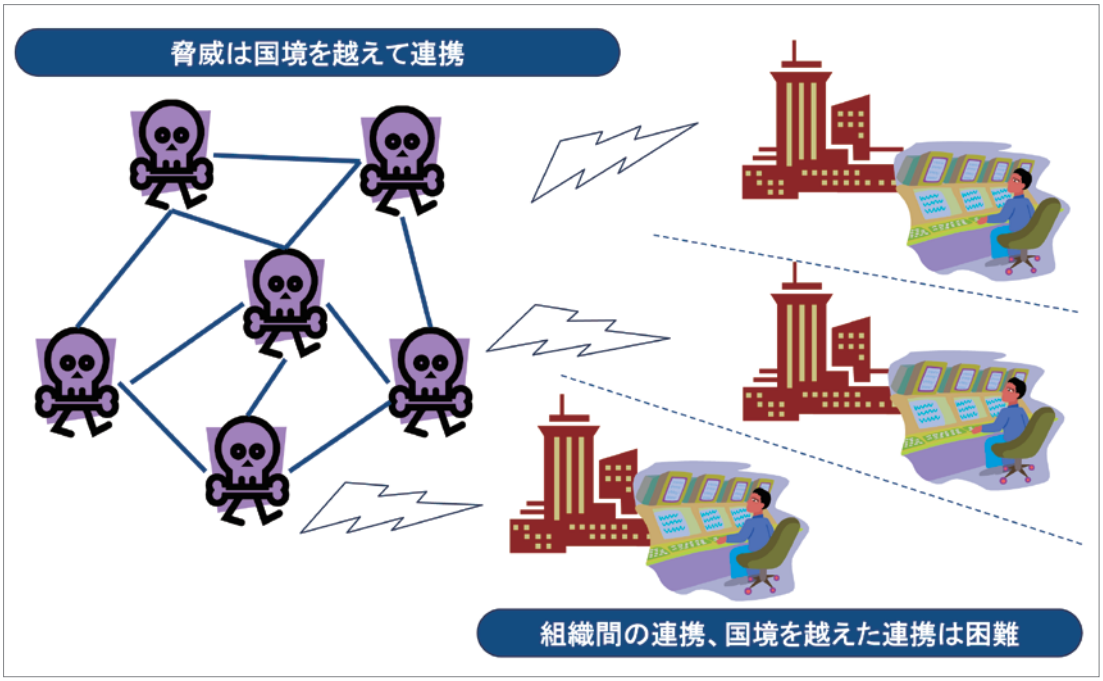


図1　脅威に劣後する対策

研究活動の背景

インターネットが世界規模で普及したことにより、近年、サイバー社会が急速に発展してきました。しかしながら、サイバー社会におけるセキュリティ、すなわちサイバーセキュリティに関しては、未だ発展途上の段階にあります。サイバー社会には国境はなく、脅威は国境を越えて襲ってきますが、その対策は各国・各組織が個別に対応しているのが現状です(図 1)。すなわち、悪意のあるユーザーはリターンキーを押すだけで、互いに連携して世界中のコンピュータに対し攻撃が可能ですが、その対策は各国・各組織で独立して実施されています。各組織が連携するには、組織の壁を越えた情報交換が効率的に行われる必要がありますが、現時点では、必要に応じてメール、電話、対面での打ち合わせなど、時間と人手を要して実施しているのが現状です。

このような状況が生じている主な要因の１つに、情報交換のフォーマットやフレームワークが各国・各組織で統一されていないことが挙げられます。各国・各組織が協力してサイバーセキュリティ対策を実施するためには、サイバーセキュリティ情報の交換フォーマットやフレームワークがグローバルに共有される必要があります。

国際標準 CYBEX(X.1500)の構築

前述の情報共有フレームワークを構築すべく、我々は現在、国際標準化組織 ITU-T において CYBEX(Cybersecurity Information Exchange Techniques)という、組織間でのサイバーセキュリティ情報を交換するのに必要な技術群・フレームワークを定義しています。尚、CYBEX は組織間での情報交換に特化しているため、その情報の取得・活用については CYBEX の範囲外です(図 2)。

CYBEX では、この「サイバーセキュリティ情報の交換・共有」を実現するために、情報の表現手法、発見・交換手法、信頼性構築手法、

伝送手法のそれぞれを規定しています。特に、この情報の表現手法、発見・交換手法においては、後述する我々のオントロジの研究が大きく活かされています。CYBEX 自体は、ITU-T 勧告 X.1500 として勧告化されましたが、CYBEX を実現する具体的な技術については、今後も更なる発展が求められ、私も研究成果を積極的に ITU-T や IETF という国際標準化機関での活動に活かしています。

情報交換の基礎となるオントロジ

CYBEX に貢献する活動の 1 つとして、我々はサイバーセキュリティ情報のオントロジを構築しました（図 3）。オントロジとは、世界を概念レベルでモデリングしたものを指しますが、ここでは、サイバーセキュリティオペレーションのあるべき姿をモデル化したものを指し、サイバーセキュリティオペレーションの業務領域、そのそれぞれの領域の業務を実施するプレイヤー、および彼らが扱う情報群という、3 種類の情報を構造化して定義しています。すなわち、「どのオペレーションを」「誰が」「どの情報を利用して」実施するかをモデル化しています。本オントロジ構築に当たっては、日本だけでなく、米国、韓国のサイバーセキュリティ

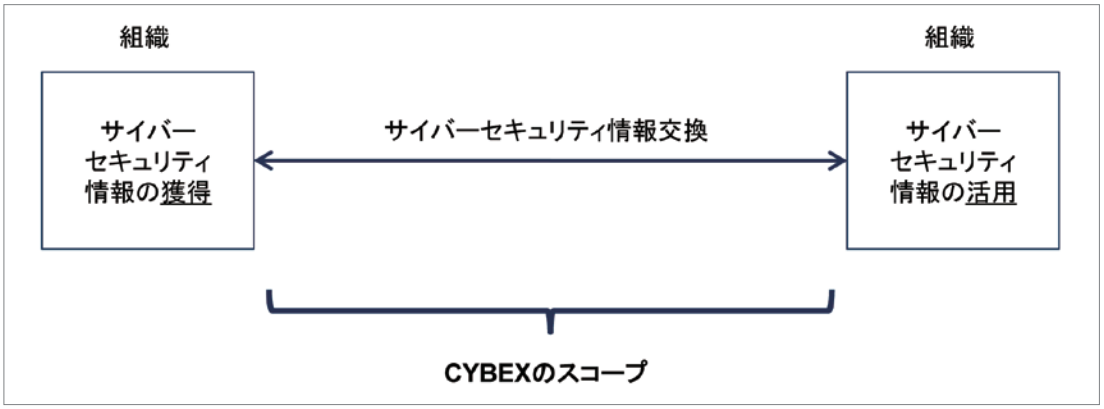


図2　CYBEXの範囲

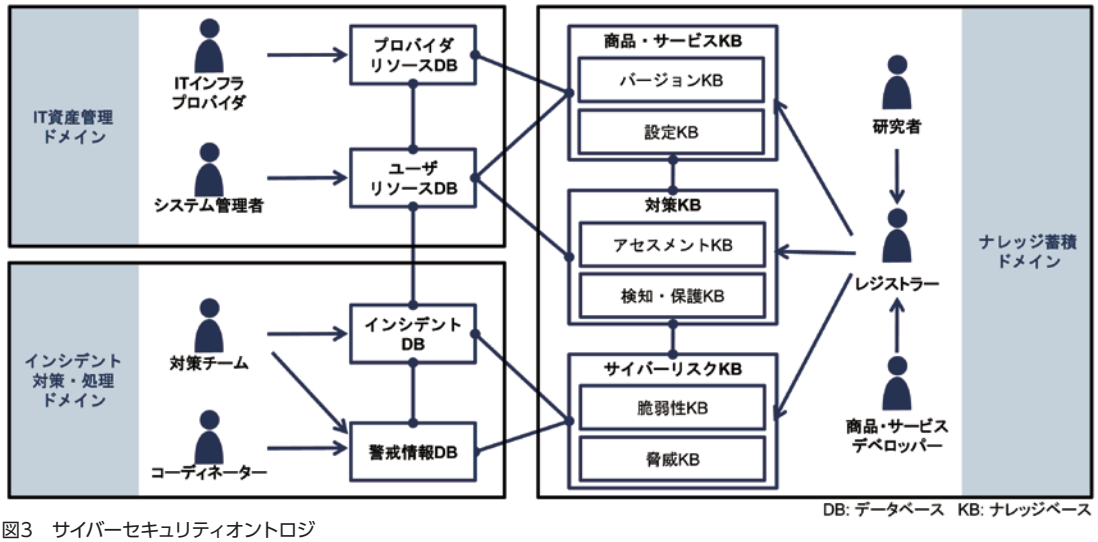


図3　サイバーセキュリティオントロジ

オペレーションの現状を鑑みており、サイバーセキュリティ先進国の知見が大いに活かされています。

本オントロジにより、サイバーセキュリティオペレーションの中でどのようなプレイヤーがどのような情報を必要とし、どのような情報交換がなされるべきかというものを体系立てて議論していくことが可能となり、CYBEX で交換されるべき情報を網羅的に議論するための土台となっています。これまでも様々な業界標準の動きはあったものの、部分最適な規格になる傾向がありました。CYBEX では、本オントロジに基づいて検討を進めることにより、サイバーセキュリティオペレーションを広く俯瞰しての規格制定を構築することを目指しています。

地球規模でのサイバーセキュリティ向上を目指して

このように、私はサイバーセキュリティ情報を「知」として共有するための手法・フレームワークを研究しております。ここにご紹介したもの以外にも、これらの世界中に存在するサイバーセキュリティ情報を、効果的に発見するための手法などの研究および開発も手掛けています。本オントロジに限らず、研究の成果を世の中に活きる形に昇華すべく、成果の国際標準化活動への展開、およびデモツールの構築・公開にも積極的に貢献しています。詳しくは、我々のホームページ(http://cybex.nict.go.jp/)をご参照ください。

暗号技術の新展開

野島 良 (のじま りょう)
ネットワークセキュリティ研究所
セキュリティ基盤研究室 主任研究員

大学時代に暗号技術を試みましたが、全く歯が立ちませんでした。その延長線上に今の自分がいますが、今は暗号解読ではなく、暗号技術を設計する立場になりました。博士(工学)。

「盗聴者への情報漏えいを防ぐことを主目的として発展してきた暗号技術に対する新たな展開先、プライバシー確保型 IP トレースバックを紹介します。」

暗号技術の広がり

暗号技術は、2 者間の通信において盗聴者にメッセージの内容が漏れないようにすることを主目的として発展してきました。しかし、近年のインターネットの発展に伴い、その応用範囲は急激に拡大しています。その中でも、我々が所属するネットワークセキュリティ研究所においては、内積暗号、秘匿計算プロトコルと呼ばれる汎用性の高い暗号技術の研究・開発に力を注いできました。ここでは、秘匿計算プロトコルの一種である「オブリビアス秘密鍵暗号プロトコル」とその応用技術「プライバシー確保型 IP トレースバック」について紹介したいと考えています。

そもそも IP トレースバック技術とは、インターネット上で不正を働いたユーザを追跡する技術です。もう少し具体的に述べると、IP トレースバックにおいては、各ルータが通過するパケットを保存しておきます。そして、実際に攻撃が行われた際には、攻撃を行ったパケットが保存されているルータを探索することにより、結果的に攻撃を行ったコンピュータを見つけ出すことが可能となります。

この IP トレースバック技術は非常に有用な技術ですが、探索する際に不正ユーザだけではなく、正当なユーザのプライバシーをも暴露してしまう可能性があります。我々が提案したプライバシー確保型 IP トレースバック技術は、IP トレースバック技術の一種です。ただし、正当なユーザのプライバシーを確保しながら、不正ユーザを追跡することが可能になります。

IP トレースバックとプライバシー確保型 IP トレースバックに関する問題は、次のように単純化することができます。2 人のユーザ(花子と太郎)を考えます。太郎は IP アドレスの集合 $A=\{a_1, \cdots, a_n\}$ を、花子は IP アドレス a を保持しているとします。花子の目的は、A の中に a が含まれているかどうか調べる事です。この問題は、花子が a を太郎に送り、太郎が A の中に a が含まれているかどうかを調べる事により解決可能になります。実際に IP トレースバックでは、同じようなことが行われます。一方、プライバシー確保型の IP トレースバックにおいては、問題が若干難しくなります。この技術を実現するためには、太郎が A を漏らさずに、そして花子が a を漏らさずに、a が A に含まれているか調べることが必要になります。この一見解決不可能な問題を、我々は、オブリビアス秘密鍵暗号プロトコルを開発・応用することにより解決しました。ここでは、このオブリビアス秘密鍵暗号プロトコルの概要とその応用についてご紹介します。

秘密鍵暗号

秘密鍵暗号においては、秘密鍵 SK を使いメッセージ M を暗号化することができます。

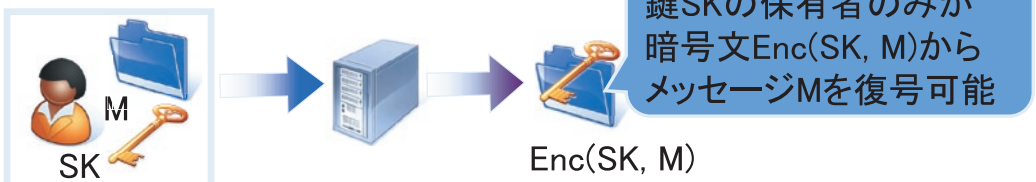


図1　秘密鍵暗号の説明

この暗号化されたメッセージを Enc(SK, M) と表します。ここで秘密鍵 SK を保有する人だけが、Enc(SK, M) から M を取り出すことが可能になります。逆に、SK を保有していない人は M に関する情報を一切得る事ができません(図 1)。秘密鍵暗号として代表的なものに、DES(Data Encryption Standard) と AES (Advanced Encryption Standard) があります。

オブリビアス秘密鍵暗号

オブリビアス秘密鍵暗号プロトコル(以降、OEP) は、2 者(太郎、花子) 間の暗号プロトコルです。

太郎は秘密鍵暗号の秘密鍵 SK を、花子はメッセージ M を保有します。このプロトコルは、お互いの情報 SK と M を秘密にしたまま暗号文 C = Enc(SK, M) を計算することを可能にします。ここで、もちろん C を得られるのは花子であり、太郎は C に関する情報を一切得る事ができません(図 2)。

ここで「オブリビアス」という単語に関してですが、直訳すると「気付かない」という意味があります。太郎と花子は相手の入力について「気付かない」ため、プロトコル名にオブリビアスという用語が使われています。

IP トレースバックへの応用

プライバシー確保型 IP トレースバック技術において、太郎と花子は、お互いの情報を隠しながら、a が $A = \{ a_1, \cdots, a_n \}$ に含まれているかどうかを検証する必要がありました。この問題は、OEP を使うと簡単に解決できます。

(1) 太郎は、秘密鍵暗号の秘密鍵 SK を選び、Enc(SK, a_1)、…、Enc(SK, a_n) を花子に送ります。

(2) 花子は、OEP を使い Enc(SK, a) を得ます。そして、Enc(SK, a_1)、…、Enc(SK, a_n) の中に、Enc(SK, a) と同じになるものがあった場合、a が A に含まれていると判定します。OEP を使うことにより、お互いに SK と a が漏れないため、花子の秘密情報である a が太郎に漏れる事はありません。さらに、SK が花子に漏れないので、n 個の暗号文から太郎の秘密情報 A が漏れることもありません(図 3)。

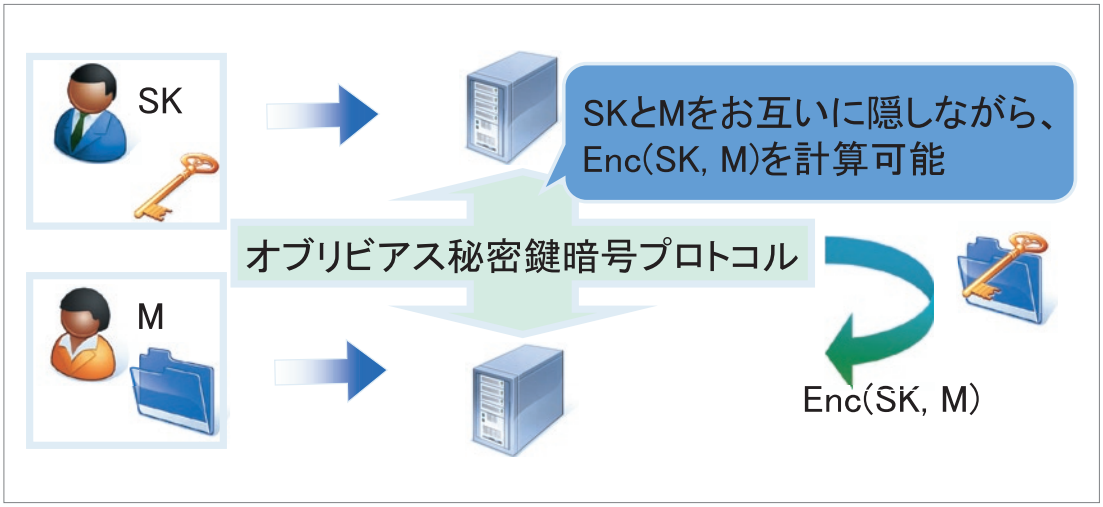


図2　オブリビアス秘密鍵暗号プロトコルの説明

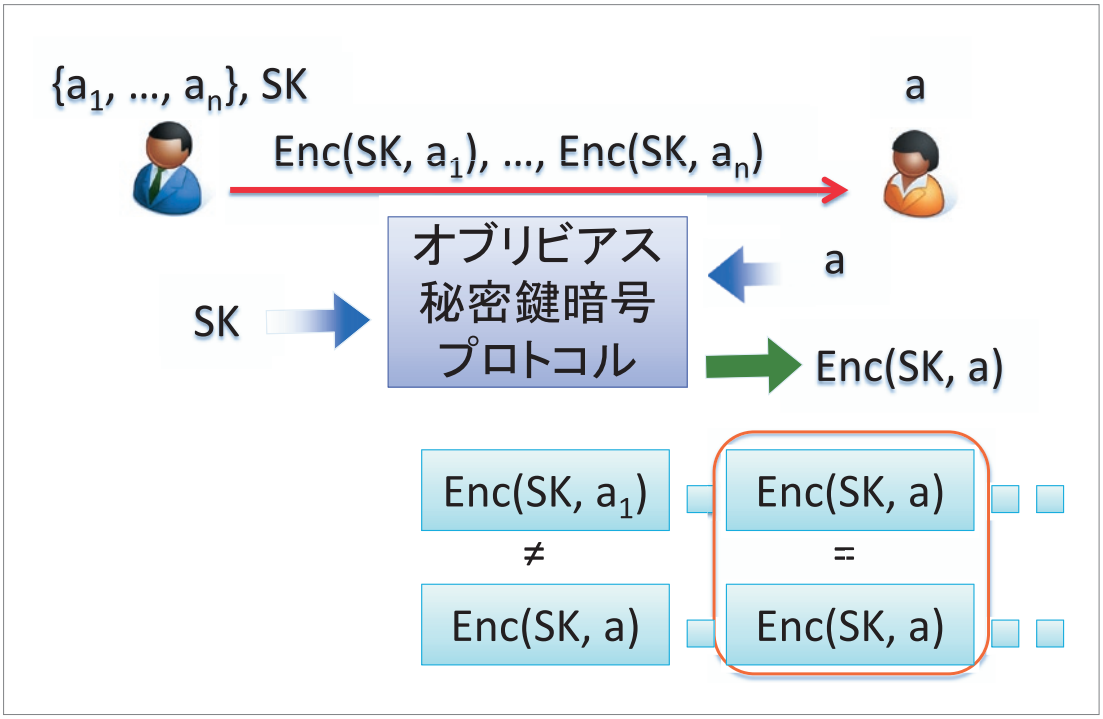


図3　プライバシー確保型IPトレースバックの説明

今後の研究について

ここまでオブリビアス秘密鍵暗号プロトコル、及びプライバシー確保型 IP トレースバック技術を簡単に紹介してきました。その具体的構造まで説明することはできませんでしたが、既にオブリビアス秘密鍵暗号プロトコルは、実装・実験が無事に終了しています。今後は、IP トレースバック技術、オブリビアス秘密鍵暗号の更なる発展・普及に努めたいと考えています。

プライバシ保護技術

大久保 美也子 (おおくぼ みやこ)
ネットワークセキュリティ研究所
セキュリティアーキテクチャ研究室 主任研究員

のどかな景色の水のきれいな田舎で育ち、子どもの頃は暗くなるまで野山を駆けて遊んでいました。スポーツの経験は、陸上競技(短距離走や幅跳び)、バレーボール、剣道を少々…。基本的にスポーツ全般好きです。近視＆乱視で中学の頃眼鏡をかけ始め、現在では体の一部です。暗号の研究は社会人になってから本格的に始めたのでやや遅めのスタートでしたが、生涯現役!を目指しています。

「複雑に入り組んだサービス間の中にあっても個々の要求に応じ、プライバシーを守れる仕組み作りが今後ますます重要となります。本稿では、ネットワーク上でフレキシブルにプライバシ保護を実現する技術について紹介します。」

はじめに

ネットワークの用途が日々変化し拡大をし続けている昨今、これまで対面もしくは書面でしか扱えなかった契約・取引・売買などの手続きもインターネットを介して行えるようになってきました。このように利便性の向上に伴い、ネットワーク上で不正なくこれらの手続きが行えるよう、意識して防御しなければならないことも増えてきています。また、近年では、インターネットを活用することにより様々な情報が入手可能となり、簡単にほしい情報を集めたり調べたりすることができるようになりました。その一方で、自分で気がつかないうちにプライバシに関わる情報を侵害されうる可能性も高くなっています。

このような状況を踏まえ、私たちの研究室ではネットワークを本来の効率性や利便性を損ねることなく、安全性とプライバシ保護機能とをフレキシブルに提供できる大規模認証基盤の実現を目指して研究を進めています。

ネットワークの利用用途の変化と求められる機能

ネットワーク上で不正行為が行われないようにするためには様々な要求条件が満たされなければなりません。例えば、契約の場合では、ネットワーク上で通信している相手が本当に契約相手本人か？電子データで送られてくる契約書の内容は通信の途中で改ざんされていないか？本人の意思確認が出来ているか（本人印のようなものが確認できるか）？などをチェックできる仕組みが必要になります。

一方で、個人的な内容を含む契約・取引・売買などの場合には、必要以上には個人個人のプライバシに関わる情報は漏らしたくないという要求が出てきます。例えば、電子オークションなどでは、応札の手続きを匿名で進めたいなどの要求が出てきます。また、電子投票などでは、有権者が投票を行う際に誰であるかが特定されてはいけない、立候補者の誰に投票したのかが識別されてはいけない、などの要求が出てきます。

一見すると不正を防止し安全性を保つための要求条件とプライバシを保護するための要求条件が相反する要求事項に見えますが、暗号技術を活用することによりそれらの要求事項を両立させることができるようになります。

保護したいプライバシ情報は、ユーザごとに、また利用シーンごとに異なります。さらに大規模ネットワークへ多数の端末が接続するこれからのネットワーク上では、考慮すべき状況が複雑化・多様化します。同一ユーザであったとしても用いる端末やデバイスが異なる場合や異なるサービス間でユーザ情報の交換などが行われる場合など、起こりうる複合的な事象を全て踏まえた上で、守られるべきセキュリティレベルを保ちつつ個々のプライバシを保護することが望まれます。例えば、複数のサービス間で同一ユーザであることが識別される必要がある場合、同一ユーザであることを識別されることがプライバシの侵害につながる場合等も出てきます。また、複数の異なるデバイスを用いていても、同一ユーザであることが識別されることによりプライバシ侵害などの可能性も出てきます。

ある用途や目的に特化し、保護すべきプライバシ情報を確定するようなシステム設計であれば、従来からある暗号技術などを複数用いることにより、ある程度構成することができます。しかし、目的が多様化し、また保護すべきプライバシ情報も画一的でなくなってきている昨今、それらの方向性の異なる要求事項を１つのシステムで実現することは困難もしくは構成すること

が出来たとしてもシステムの肥大化を招いてしまいます。

我々の目指す安全かつ利便性の高いセキュリティ技術

そこで私たちの研究室では、プラットフォーム上でのユーザおよびサービス提供側などの様々な要求条件にフレキシブルに応えられるプライバシ保護機能を備えた認証方法の提供を可能にする暗号技術を研究対象としています。

例えば１つのプラットフォームで、電子投票や申請システムやアンケートなどそれぞれの目的・保護したいものの要求条件に沿った機能を提供可能となる総合情報基盤を目指しています。

これらの実現により、コスト面では、１システム数百万から数億円かかる複数システムを１システム分のコストで提供することが可能となります。また、機能面では、1つのプラットフォーム上でユーザ・サービス提供側双方の安全性を保持した上で、個別ユーザごとの、またサービス提供者ごとの異なる要求事項や、ユーザの利用目的や提供サービスごとに異なる必要な機能などをフレキシブルに実現できるプライバシ保護機能を備えた認証の提供が可能となります。

具体的には、図に示すように、目的により異なるプロトコル（メッセージの内容を匿名にするブラインド署名、署名者の ID を匿名にするグループ署名など ）を構成するために、それぞれのプロトコルを個別に構成するのではなく、１つのディジタル署名を活用することにより、両方のプロトコルの機能を同一のプラットフォーム上で提供することが可能となります。また、効率面では従来技術を複数用いた構成に比べ、システム全体としてのコンパクト化を実現でき、利便性についても、用途ごとへのフレキシブルな機能提供が可能となります。

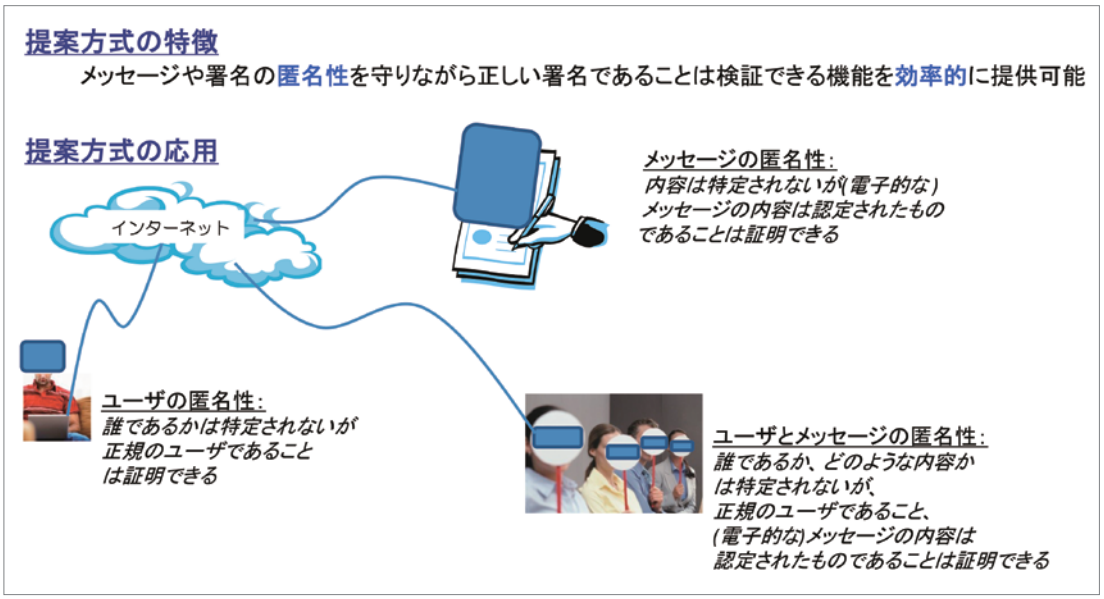


図　プライバシ保護のための提案方式の活用イメージ

今後の展望

ネットワークの利用用途は限りなく広がっていく可能性を秘めています。私たちの研究室ではその可能性を最大限に伸ばしていけるよう、セキュリティの技術を防御するためだけの手段として用いるのではなく、その可能性を促進する手段として活かしていきたいと考えています。

過不足のないセキュリティを実現するセキュリティアーキテクチャ

ーネットワーク利用者の状況に合わせたセキュリティの実現ー

松尾 真一郎 (まつお しんいちろう)
ネットワークセキュリティ研究所
セキュリティアーキテクチャ研究室 室長

博士（工学）。大学院修了後、1996年にNTTデータ通信株式会社に入社、情報セキュリティと暗号の応用に関する研究に従事。2009年にNICTに入所、2011年から現職。情報セキュリティの研究は国際標準化が重要であり、ISO/IEC JTC1における暗号技術の標準化作業の日本における主査を務め、国際標準化のために世界を飛び回る日々を送っています。日本発のセキュリティ技術が世界で利用される例を1つでも多く作るのが夢です。

「ネットワーク上のサービスを利用する際に、利用者にとって確認しにくいセキュリティを可視化し、複雑なシステムでも適切なセキュリティ技術を利用可能にします。」

ネットワークの多様化とセキュリティ対策の複雑化

近年、ネットワークにおける様々な処理やサービスの環境が大きく変化しています。従来は、いわゆるクライアント・サーバという形態でサービスが実現され、情報セキュリティの設計もこの形態に合わせた形で行われてきました。しかし、クラウドコンピューティングが普及し、セキュリティを考える際の出発点となる情報資産の保管場所が多様化するとともに、スマートフォン、センサーやRFIDタグなど、従来のセキュリティ技術が保護の対象としていなかったデバイスが大量にネットワークに接続されるようになっています。NICTが実現を目指している新世代ネットワークにおいても、およそ10兆個のデバイスがネットワークに接続され、ネットワーク仮想化やID・ロケータ分離[*1]などの技術をベースにして、状況に応じた通信環境を提供することが目標になっています。

従来の情報通信技術(ICT)でのシステムにおけるセキュリティは、ITU-T[*2]やIETF[*3]などで標準化されている技術を利用して実現されてきていますが、これらの技術は画一的な環境やセキュリティ要求に対応するものでした。しかし、ネットワーク環境が多様化・複雑化する場合には、ネットワークにおけるセキュリティ上の脅威も複雑化し、脅威への対策を見つけ出すことは非常に困難になります。このような状況では、既存のセキュリティ技術では、必要なセキュリティ対策が取られていなかったり、逆に過剰な対策で通信速度を犠牲にするケースが多く出現することになります。

そこで、このような複雑なネットワーク上の脅威に対して、過不足のないセキュリティ対策をタイムリーに実現するための仕組みが必要となっています。

過不足のないタイムリーなセキュリティ対策

ICTにおけるセキュリティ確保の基本的な考え方は従来から存在しますが、いたってシンプルです。

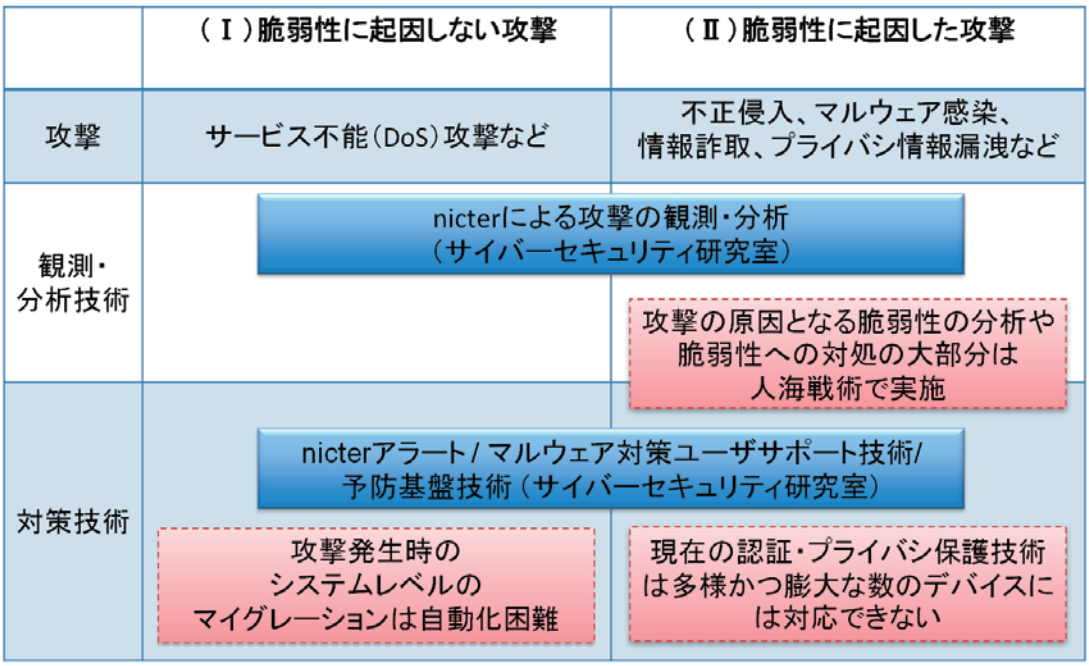


図1　ICTにおけるセキュリティの分析と対策の分類と課題

あるサービスを実現するシステムを設計するときに、守るべき情報資産(クレジットカード番号、個人情報、パスワード)などと、その保管場所を洗い出し、個々の場所に保管された情報への攻撃の成功確率を見積もり、損害の期待値から優先順位付けを行い、カバーすべき攻撃について、必要な対策技術をシステムに組み込みます。この考え方自体は普遍的なものであり、将来においても大きくは変わらないと考えられます。しかし、システムが稼働した後にシステムの脆弱性が新たに発見された場合の対処は、該当するシステムの仕様に精通し、かつネットワークセキュリティのエキスパートが人海戦術で行っているというのが実情です。何が適切なパッチなのか、新しいパッチがセキュリティや性能の問題を引き起こさないのかなど、セキュリティパッチの管理だけでも膨大で、難しい作業になります(図 1)。

新しい時代のネットワークに必要なことは、システム設計の時点だけではなく、いつまでもシステムがセキュアであることです。そのために、システム設計の時に必要な対策を見つけ出すこと、システム運用時に発生する脆弱性にタイムリーに対応できること、脆弱性や脅威への対策は過不足がない、すなわち十分かつ通信性能を極力犠牲にしていないことが求められます。

新たなセキュリティアーキテクチャの実現に向けて

現在、我々が研究しているセキュリティアーキテクチャでは、複雑化するネットワークにおいて過不足のないタイムリーなセキュリティを提供する「フレキシブルセキュリティ基盤」と、モノに付けられるような計算能力の低いデバイスを含む 10 兆個のノードに対応できる認証・プライバシ保護技術「セキュリティコンポーネント」の実現のための技術の実現を目指しています。

フレキシブルセキュリティ基盤では、過不足のないタイムリーなセキュリティ対策を導出するための、セキュリティ知識ベース・分析エンジンの実現を目指しています(図 2)。セキュリティ知識ベースは、ネットワーク機器等に潜む脆弱性、対策技術、ネットワーク形態、ネットワーク機器の性能などのデータベース(DB)を総称したものです。

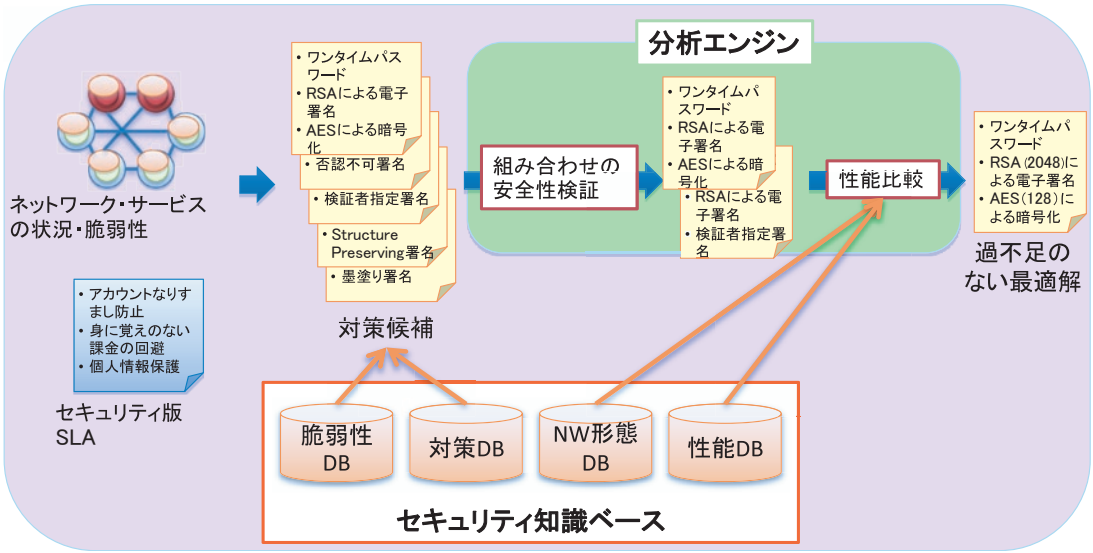


図2　セキュリティ知識ベース・分析エンジンの概念図

サイバーセキュリティ研究室の nicter の観測結果とも連携します。そして、分析エンジンは、セキュリティ知識ベースと連携し、複数のセキュリティ対策案の中から、安全かつ処理性能が一番高い対策を選び出すことで、過不足のないセキュリティを実現するものです。すでに、第一歩としてモバイル機器の利用者に向けて、その時に使っているサービスの脆弱性をセキュリティ知識ベースから引き出し iPad や Android タブレット上で可視化する Risk Visualizer(図 3)のプロトタイプを構築しました。フレキシブルセキュリティ基盤は、ネットワーク仮想化や ID・ロケータ分離といった新世代ネットワークの特長を活かすことで、新世代ネットワークにおける次世代のセキュリティの基盤となります。

セキュリティコンポーネントにおいては、計算能力の低いデバイスでも利用可能な認証・プライバシ保護技術を確立するとともに、異なる管理下にあるネットワーク同士でも認証やプライバシ保護ができる技術を研究しており、匿名性と文書の秘匿性を同時に実現できるプライバシ保護技術や、RFID タグ向けの認証技術を確立しています。これらの研究も、新世代ネットワークの実証に組み込む予定です。

図3　Risk Visualizerシステムにおけるネットワーク利用のリスク表示例

用語解説

＊1　ID・ロケータ分離

端末の名前と位置を示す識別子を別々に管理し、方式が異なるネットワークでも、同じ ID を使用することで、端末の移動や経路上の障害等によりネットワークが切り替わっても継続して通信を可能とする NICT が開発している技術。

＊2　ITU-T

国際連合の専門機関の 1 つである国際電気通信連合(ITU)の電気通信標準化部門。

＊3　IETF

インターネット技術の標準化について検討を行う組織。ここで策定された技術仕様は RFC として公表される。