安心・安全を目指したネットワークセキュリティ研究開発

NTT情報流通プラットフォーム研究所では，日々増大するセキュリティ脅威からネットワークを守るべく，「ネットワークセキュリティ」の研究開発とセキュリティインシデント対応の活動に取り組み，安心・安全なコミュニケーションをお客さまへ提供することを目指しています．

中村（なかむら） 伊智三（いちぞう）　/増田（ますだ） 浩樹（ひろき）

NTT情報流通プラットフォーム研究所

安心・安全なコミュニケーションを目指して

NTTは中期経営戦略において，「お客さまにとって安心・安全で便利なコミュニケーションネットワーク環境とブロードバンドアクセス基盤を構築」を宣言し，また，CSR憲章でも「安心・安全なコミュニケーション」を1つの柱として，よりよいサービスをお客さまに安心してお使いいただけるようグループ一丸となって取り組んでいます．NTT研究所においても安心・安全を目指し，さまざまなセキュリティの研究開発を推進しています．本稿ではネットワークを取り巻くセキュリティ環境とNTT情報流通プラットフォーム研究所のネットワークセキュリティの研究開発の取り組みを紹介します．

ネットワークを取り巻くセキュリティ環境

インターネットは当初は補助的なコミュニケーション手段でしたが，急速な利用の広がりにより，今日では，生活に欠かせないほどの存在となっています．一方で，インターネットを通じた，個人情報や企業情報の漏洩，コンピュータウイルスの感染，ハッカーによるコンピュータシステムへの侵入改ざん，ボットネットを利用した特定企業のシステムへの攻撃などインシデントが発生しています．インターネットが社会基盤となった現在，特定のコンピュータの被害レベルにとどまらず，コンピュータシステム停止が企業の事業活動の停止に直結する，あるいは情報漏洩が企業の信頼性低下につながるなど，セキュリティ問題の社会に与える影響が大きくなっています．

また，ブロードバンドネットワークの拡大，コンピュータ処理能力の飛躍的向上，アプリケーションの高度化など，サービスとしての利便性が進むと同時に，セキュリティ脅威を発生させる攻撃者にとっても新たな攻撃をより簡単につくり出しやすくなり，セキュリティ脅威は日々増大しています．

NTT研究所のネットワークセキュリティの研究開発

NTT情報流通プラットフォーム研究所では，日々増大するセキュリティ脅威に対し，

① セキュリティ脅威からネットワーク自体を守ること
② ネットワークを通じたセキュリティ脅威からシステムを守ること
③ NTTグループ全体のセキュリティレベルを向上すること

を目指し，ネットワークセキュリティの研究開発に取り組んでいます（図）．特に，①についてはネットワークキャリアの観点から，NTTインフラ保全，通信の正常性の担保が重要なポイントと考えています．

ネットワークセキュリティの研究開発には，大きく2つのアプローチがあります．

・セキュリティ脅威の「影響回避」
・セキュリティ脅威の「発生予防」

インターネットが緩やかな枠組みでスタートしたものが，急速に複雑化した結果，日々新たな問題が発生している状況となっており，まずは影響回避の取り組みが急務となっています．

NTT情報流通プラットフォーム研究所では影響回避の研究開発として，特に「トラフィック監視・分析技術」「マルウェア対策技術」を重点に進めています．さらに，「NTT-CERT（NTT Computer Security Incident Response and Readiness Coordination Team）」によるNTTグループ全体のセキュリティレベル向上の取り組みを行っています．また，発生予防は根本的な解決策を目指す究極のア

プローチですが，その技術の一提案として「携帯電話向けの仮想化技術（Virtual Smartphone over IP技術）」にも取り組んでいます．

トラフィック監視・分析技術

ライフラインとしてのインターネットではサービス継続性の強化が重要です．一方で，アクセス回線のブロードバンド化により，DDoS攻撃（Distributed Denial of Service攻撃：分散型サービス不能攻撃）などの影響がバックボーンネットワークにも波及するようになりました．この結果，直接被害者に加えて，攻撃の巻き添えでインターネットが使えなくなる間接被害者も多発しています．このような問題を解決するためには，ネットワークを全体視点で防御することが必要となりますが，バックボーンネットワークを流れる膨大なトラフィックを，すべて詳細に監視することは容易ではありません．

そこで，バックボーンネットワーク全体からNetFlowに代表されるようなサンプリングされたフロー情報を収集し，トラフィック変動を定常的に監視するとともに，異常的なトラフィック変動を検知した際には，その送信元および宛先を分析・特定することが有効と考えられます．また，DNS（Domain Name System）問い合わせ情報やBGP（Border Gateway Protocol）経路情報などのネットワーク制御情報については，トラフィックは少量であっても，異常発生時にネットワーク全体に与える影響が大きいため，最初から詳細に分析することも有効と考えられます．

このような背景から，これらを組み合わせた多角的な視点で，バックボーンネットワークを流れるトラフィックを監視・分析する技術の研究開発に取り組んでいます．

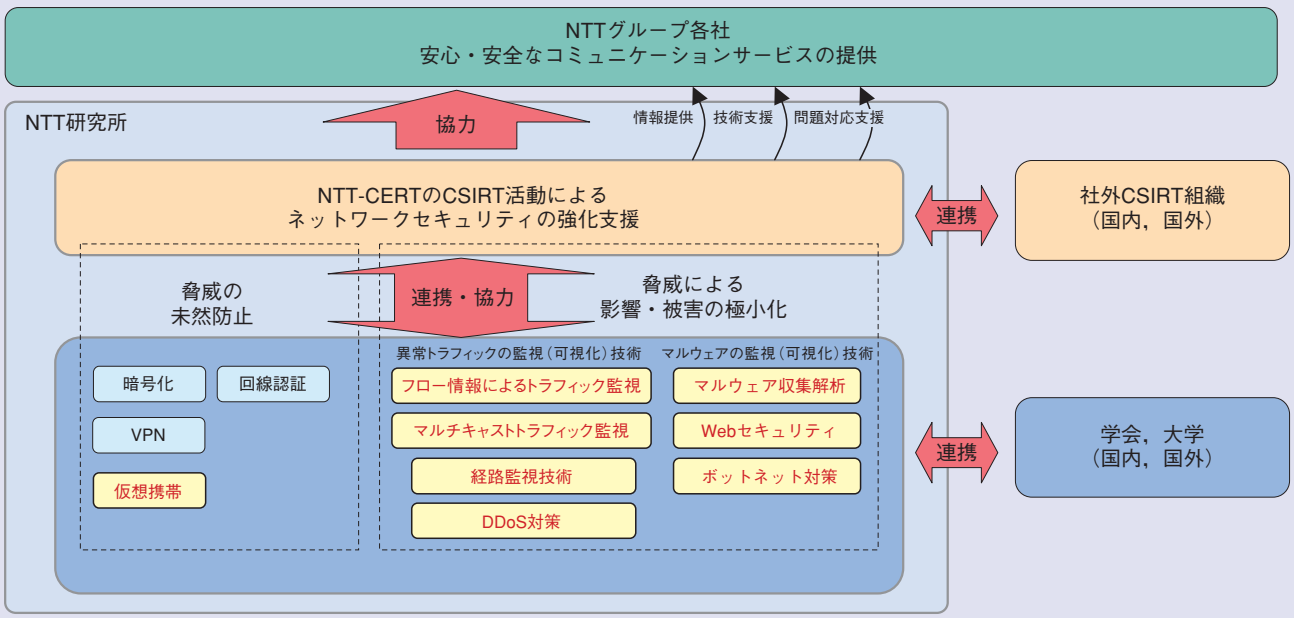

図　NTT研究所のネットワークセキュリティの取り組み

マルウェア対策技術

コンピュータウイルスに代表される悪意あるソフトウェアは，マルウェアと呼ばれています．インターネット上のサービスが生活を支える一方で，個人や企業の情報がネットワーク経由で漏洩する事例や，情報が不正に改ざんされる事例等が急増していますが，これらの多くはマルウェアが使用されています．攻撃者は，ユーザのPCやサーバをマルウェアに感染させてリモート操作可能にします．マルウェアはDDoS攻撃やスパムメールの送信などにも使用されており，サイバー攻撃の根源はマルウェアであるということもできます．マルウェアの感染方法は日々複雑化・高度化しており，感染を検知することは非常に困難になってきています．さらに，マルウェア間の連携や，マルウェアの亜種の増加は事態をより困難にしています．

そこで，おとりシステムであるハニーポットを用いてマルウェア感染を検知しています．その結果に基づき，感染した際の通信先などを分析してフィルタリングするなどの対策を講じることが有効と考えられます．さらに，マルウェアを収集し，マルウェアの一連の通信パターンの解析や，増え続けているマルウェア亜種に対する解析作業の効率化も有効と考えられます．このような背景から，感染活動を検知してマルウェアを収集し，感染経路やマルウェアを解析する技術の研究開発に取り組んでいます．

NTT-CERT

NTT情報流通プラットフォーム研究所ではネットワークセキュリティの基盤的研究開発に加え，研究所の技術，ノウハウを活かしCSIRT（Computer Security Incident Response Team）組織であるNTT-CERTによるNTTグループ全体のセキュリティレベル向上の取り組みを行っています．

CSIRTとは，コンピュータインシデントに対し，分析，対応，教育等を行う組織であり，NTTグループの各社で発生するセキュリティインシデントについての相談窓口となり，各社でのインシデント対応のサポートとセキュリティ情報の展開を行っています．

NTT-CERTの活動は，ネットワークセキュリティ技術を中心とした研究所の各種セキュリティノウハウが下支えになっています．さらに，国内外のCSIRT組織，日本シーサート協議会（NCA）やFIRSTといったCSIRT組織のハブ的組織等の外部組織との連携体制を構築することにより，セキュリティ情報やインシデント対応ノウハウ情報の交換を積極的に進め，NTTグループにおけるインシデント対応に活かしています．

今後の展開

NTT情報流通プラットフォーム研究所では，ネットワークセキュリティの研究開発に積極的に取り組むとともに，これらの技術をベースとしたNTT-CERT活動を推進し，NTTグループ各社における安心・安全なコミュニケーションサービスの提供に貢献し，よりよいサービスをお客さまに安心してお使いいただけるよう，日々研究開発を進めています．また，今後はセキュリティ脅威の影響回避のアプローチに加え，セキュリティ脅威の発生予防のアプローチにも力を入れていきます．

（左から）増田　浩樹/ 中村　伊智三

安心・安全なコミュニケーションをお客さまに提供すべく，ネットワークセキュリティの研究開発に取り組んでいきます．

◆問い合わせ先
NTT情報流通プラットフォーム研究所
セキュアコミュニケーション基盤プロジェクト
TEL　0422-59-4936
FAX　0422-59-5660
E-mail　masuda.hiroki@lab.ntt.co.jp