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。

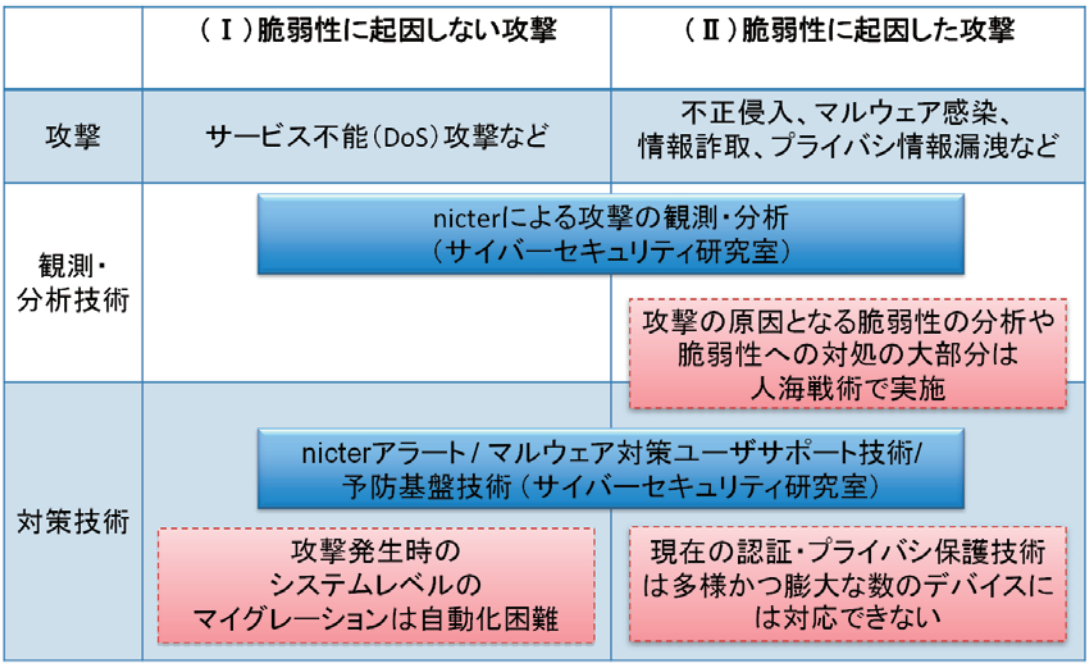

図1　ICTにおけるセキュリティの分析と対策の分類と課題

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。

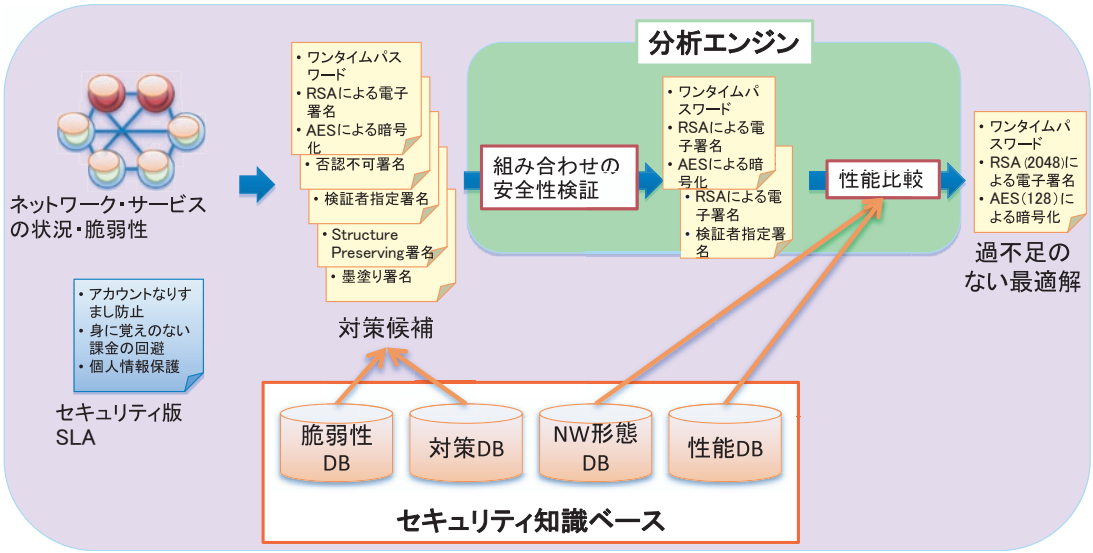

図2　セキュリティ知識ベース・分析エンジンの概念図

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。