報道発表（お知らせ）

- スピア型サイバー攻撃判定システム開発のための共同実証実験を開始
  ー特定の組織に限定したサイバー攻撃を早期に検知するシステムの実現に向けてー
- 平成20年3月3日

独立行政法人情報通信研究機構（以下、「NICT」という。理事長：宮原 秀夫。）は、インターネットにおいて最近頻繁に出現している「スピア型サイバー攻撃*1」に対処するため、この攻撃を早期検知する技術開発に取り組んでいます。この一環として、NICTはスピア型サイバー攻撃判定システムを試作し、本日から実証実験を開始しました。この実験には、トレンドマイクロ株式会社（「トレンドマイクロ」）、株式会社ラック（「ラック」）が参加し、平成20年3月末日まで実施する予定です。

＜背 景＞

近年、インターネットにおけるサイバー攻撃はますます先鋭化しており、政府機関や、金融、情報通信など、重要な社会インフラの運営体等を狙った「スピア型サイバー攻撃」が問題となっています。スピア型サイバー攻撃は通常のサイバー攻撃と異なり、特定の組織のみに対してマルウェア（ウィルス等）を送り付けるなど、攻撃対象が限定的であることから、攻撃発生の早期検知が困難な状況となっていました。そのために、スピア型サイバー攻撃を早期に検知し、判定するためのシステム開発が切望されていました。

＜今回NICTが試作したスピア型サイバー攻撃判定システムの特徴＞

スピア型サイバー攻撃の判定においては、通信の秘密を確保しながら、その攻撃が特定の組織を狙ったものであるか、否かを判定しなければなりません。

こうした課題解決のために、NICT情報通信セキュリティ研究センター・トレーサブルネットワークグループでは、準同形暗号理論に基づく秘匿共通集合計算プロトコル*2という暗号学的手法を改良・応用し、スピア型サイバー攻撃を直ちに検知判定するための試作システムを構築しました（別紙2参照）。

これまで、こうしたプロトコルを活用した手法は、国際的にも理論的研究という位置づけで取り組まれてきましたが、ハードウエアを含めた統合システムへの実装化は、本試作システムが世界で初めてとなります。

＜実証実験の目的と概要＞

本実験は、NICTが開発試作した上記システムの有効性を検証するとともに、試作システム上での課題抽出を目的としています。さらに、こうした実証実験に産業界の参加を得ることで、今後想定される産業界への技術移転の促進も目指します。

また、本実験では、実験参加企業（トレンドマイクロ、ラック）が、インターネットから収集したウィルス検体や攻撃パケットを本試作システムに対し別々に入力し、そのウィルス検体等がスピア型サイバー攻撃によるものか、否かを判定します。

今回の共同実証実験は、平成20年3月末日まで実施する予定ですが、それ以降については体制等を見直し、さらなる実証実験も計画しています。

＜今後の展開＞

本共同実証実験で得られた課題等を改善し、それを新たなシステム開発に反映させます。この先、新システムをネットワーク事業者やセキュリティ事業者に提供することにより、ネットワークセキュリティの向上に役立て、ネットワーク社会の安心安全に貢献します。

＜ 広報 問い合わせ先 ＞
総合企画部 広報室
栗原　則幸
Tel：042-327-6923
Fax：042-327-7587

＜　本件に関する　問い合わせ先　＞
情報通信セキュリティ研究センター
トレーサブルネットワークグループ
守山 栄松
Tel：042-327-7580
Fax：042-327-6640

別紙1

＜ 用語 解説 ＞

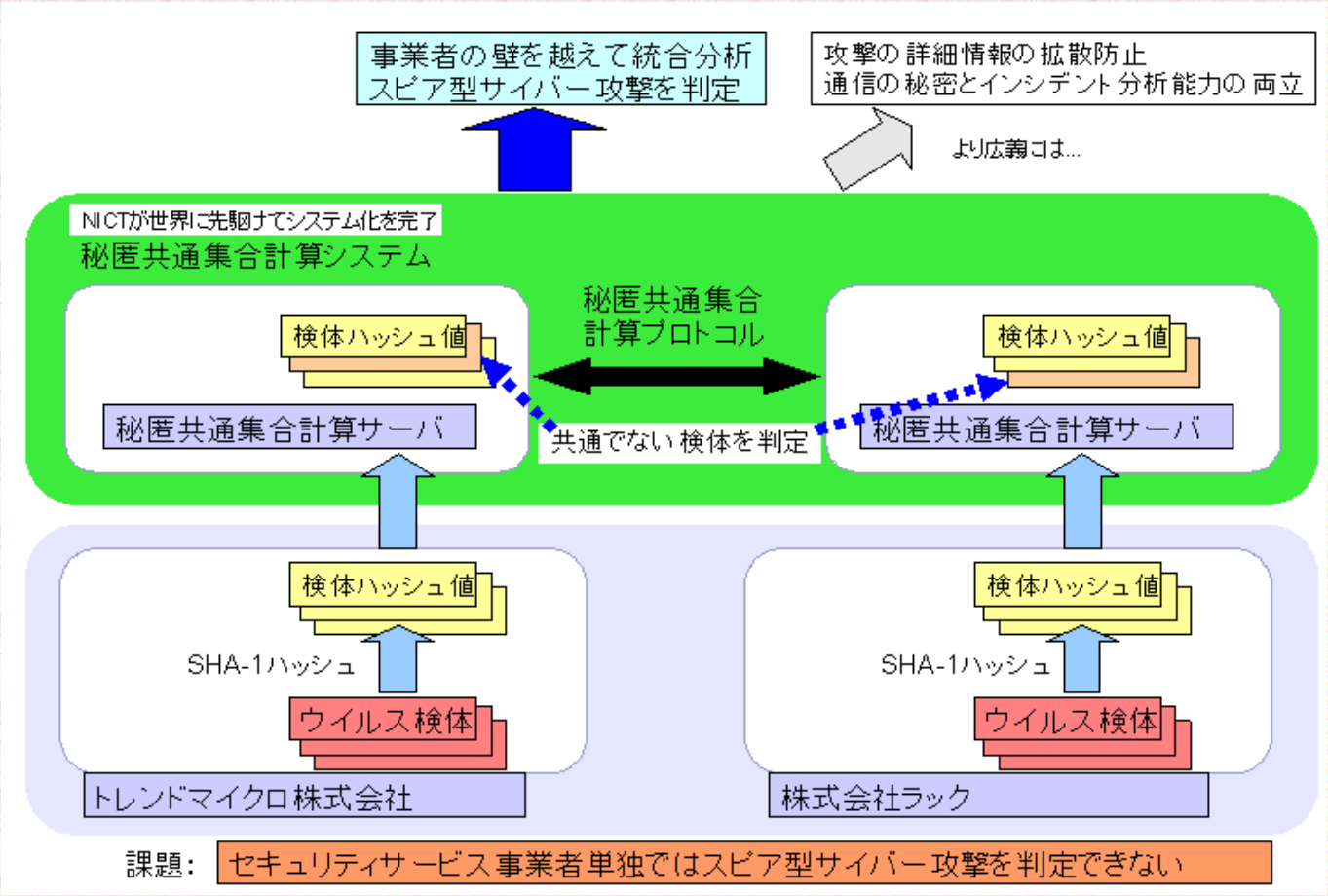
***1 スピア型サイバー攻撃**

スピア（Spear）は槍のことであり、特定の対象に限定して攻撃するパターンのサイバー攻撃のことを指します。通常のサイバー攻撃は、不特定多数にウィルスをばらまくような行動を取るので、ネットワークを観測して比較的早期に検知することができますが、スピア型サイバー攻撃はウィルスの拡散の範囲が小さいため発見しづらく早期検知が難しいという問題があります。また、攻撃対象に応じた電子メールの文面を使うなど高度な偽装が行えるので、騙される可能性が高いという特徴があります。

***2 準同形暗号の理論に基づく秘匿共通集合計算プロトコル**

秘匿共通集合計算プロトコルは互いに信頼しない二者間で、共通集合を秘密裏に計算することができる暗号プロトコルです。このプロトコルにより、自分の保持する情報を相手に開示することなく、また、相手の保持する情報を入手することなく、自分の保持する情報と相手の保持する情報が同一のものであるか否かを判定することができます。本システムでは準同形暗号理論に基づく秘匿計算を行っています。

別紙2



スピア型サイバー攻撃判定システム　概念図