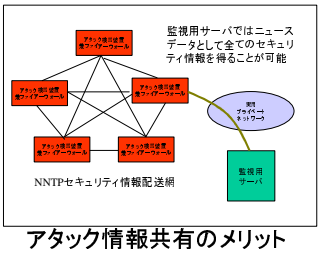
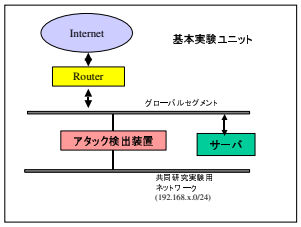
エージェント利用広域高速ネットワーク運用支援システムの研究

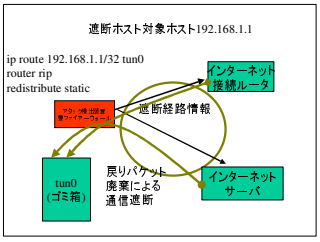


アタック情報共有のメリット

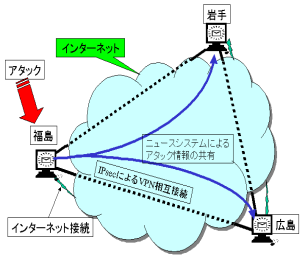


アタック検出装置の配置

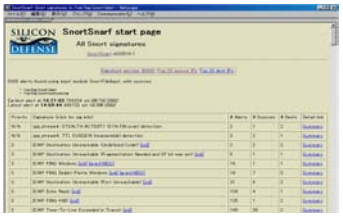
構築したアタック検出装置



経路情報による通信遮断

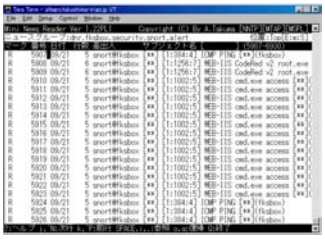


News Group	用途
dnr.security.snort.alert	snortのalert　log投稿用(全体)
dnr.security.popper.alert	pop3服似 デーモン投稿用(全体)
dnr.security.tcpd.alert	TCP wrapper log 投稿用(全体)
dnr.system.mail.root	rootあてメール投稿用(全体)
dnr.system.mail.news	newsあてメール投稿用(全体)
dnr.fksbox.security.snort.alert	snortのalert　log投稿用(福島)
dnr.fksbox.security.popper.alert	pop3服似 デーモン投稿用(福島)
dnr.fksbox.security.tcpd.alert	TCP wrapper log 投稿用(福島)
dnr.fksbox.system.mail.root	rootあてメール投稿用(福島)
dnr.fksbox.system.mail.news	newsあてメール投稿用(福島)
dnr.iwtbox.security.snort.alert	snortのalert　log投稿用(岩手)
dnr.iwtbox.security.popper.alert	pop3服似 デーモン投稿用(岩手)
dnr.iwtbox.security.tcpd.alert	TCP wrapper log 投稿用(岩手)
dnr.iwtbox.system.mail.root	rootあてメール投稿用(岩手)
dnr.iwtbox.system.mail.news	newsあてメール投稿用(岩手)
dnr.hrsbox.security.snort.alert	snortのalert　log投稿用(岩手)
dnr.hrsbox.security.popper.alert	pop3服似 デーモン投稿用(岩手)
dnr.hrsbox.security.tcpd.alert	TCP wrapper log 投稿用(岩手)
dnr.hrsbox.system.mail.root	rootあてメール投稿用(岩手)
dnr.hrsbox.system.mail.news	newsあてメール投稿用(岩手)



全体アタック情報の統合表示と解析

次世代ファイアーウォール実験網



データ共有用ニュースグループ

インターネットから行われる新パターンのセキュリティ攻撃から守るために、複数のアタック検出装置を広域分散配置することを特徴とする次世代型のファーアーウォールシステムの開発研究を行いました。その結果、実用化の見通しを得ました。

ＡＤＳＬ*、ＦＴＴＨ*等、高速な「ブロードバンドインターネット*接続サービス」が安価に提供されるようになり、県内中小企業においても導入・利用が検討されています。しかし、インターネットでは、サーバ権限奪取、ホームページ改ざん、ウィルス等の攻撃が日常的に行われており、新しい攻撃手法・パターン・ウィルスによる攻撃が出現しています。

セキュリティ攻撃対策として、ファイアーウォール装置が利用されますが、新しく出現する攻撃手法や、ウィルスには効果がない場合が多いです。

本研究では、セキュリティ攻撃がポートスキャンと呼ばれるサーバの弱点を自動ツール利用によって探す作業をきっかけに行われることが多いことに着目し、攻撃検出装置を、インターネット上の複数地点に設置することで、ポートスキャン攻撃を事前に検知することで、未知のアタックを未然に防止することができる、次世代型ファイアーウォールシステムを提案しプロトタイプシステムの開発を行いました。

本研究成果により、高速ブロードバンドインターネットを安全に利用できる効果が期待できるほか、システムで用いているVPN技術*等の要素技術も、県内企業の情報化の推進に役立つものです。

応用技術部　電子応用科
本田修啓　尾形直秀　高樋昌　浜尾和秀　太田悟
小柴誠

ADSL【Asymmetric Digital Subscriber Line】

一般電話回線網で利用する１対の銅線を利用し高速なデータ通信を行うための規格。上りと下りの通信速度が異なるため「非対称(asymmetric)という名称になっている。下り速度は1.5MBPS～12MBPS。上り速度は0.5～1.0MBPSであるが、電話回線品質によって実際の通信速度は遅くなる場合も多い。安価で提供され、これによって一般家庭のインターネット接続の常時接続化、高速化が大きく進んだ。

FTTH【Fiber To The Home】

すべての家庭に光ファイバーを引き、インターネット接続サービスをはじめとする統合化された高速ネットワークサービスを行う計画。具体的なサービスとしてNTT東西会社のBフレッツ等があり、100MBPSの安定したインターネット接続サービスが提供されている。

ブロードバンドインターネット

動画像や音声を快適に利用できるインターネットサービス。ADSLやFTTHの普及により、家庭においても安い料金で利用できるようになった。反面セキュリティ攻撃対策を家庭においても行う必要が出てきている。

VPN技術【Virtual Private Network】

ファイアーウォールの内側のネットワーク（プライベートネットワーク）間を安全に接続するための技術。プライベートネットワーク間は専用線で接続することが行われていたが、安価なインターネット接続サービスを利用し、暗号化してプライベートネットワークを仮想専用線的に接続する。専用線利用に比し低コストである。