

はじめに

インターネットの普及、コンピュータを利用した社会が形成されていくに従い、ハイテク犯罪が増加している。重要インフラが停止するような深刻な不正アクセスは未だ発生していないが、常時接続環境の整備などによるコンピュータネットワークの規模の増大、不正アクセスの手段の多様化・複雑化が日々進んでいる。しかし同時に、コンピュータシステムを保護するための対策も日々進んでいる。警察庁では、民間企業と連携し、サイバーテロ対策に関する技術の調査、研究開発を行っている。

調査・研究開発は、次の3つのテーマに分かれて活動している。

- リスクアセスメント/脆弱性評価に係わる技術
- 防御技術
- ログ保存技術

サイバーテロ対策に関する技術の調査として、ファイアウォールなどセキュリティ製品の技術調査を実施した。また試験環境を構築し有効な活用方法などの技術検証を実施した。

今後は技術検証結果を踏まえ、被害の防止、犯人の検挙を支援するシステムの開発を目指している。調査結果などを基にセキュアなネットワーク社会の実現に向けて研究開発を実施する。

リスクアセスメント/脆弱性評価に係わる技術

リスクアセスメント/脆弱性評価の必要性

リスクアセスメントとは、情報資産、脅威、脆弱性を把握するものである。被害を受けてから行動するのではなく、被害を受ける前にシス

テムに欠点がないかリスクを把握しておくことは重要である。

このテーマではサイバー空間のインシデント事例を広く調査し、攻撃手法やソフトウェアのもつ脆弱性について調査している。また、不正アクセスで使用されるソフトウェアや擬似攻撃を行うソフトウェアの評価もあわせて実施している。これらの作業を通して、サイバーテロなどの犯罪予防のために、適切な脆弱性評価/リスクアセスメントの手法を研究開発することが本テーマの目的である。

擬似攻撃ツールの製品調査

擬似攻撃ツールを調査し、ツールの利用目的や調査対象、利用方式などにより分類を行った。ツールの特徴・問題点を整理すると同時に、各種評価機関の評価基準の観点も参考に評価項目を設定し、調査を実施している。

サイバーアタック等インシデントの調査

日々発生しているインシデント情報をインターネットなどから広く情報を収集し、特筆すべきインシデントについて背景などを整理している。

脆弱性情報の収集

各種ソフトウェアの脆弱性情報やパッチ情報を日々収集し、脆弱性評価のための基礎データを収集している。基礎データはデータベース化し、随時検索が行えるようになっている。また、このデータの一部は、警察ポータルサイトの提供情報の一部になっている。

今後の活動計画

上記調査項目の終了次第、脆弱性自動評価ツールの研究開発を行う。自動評価ツールとは、ネットワーク構成、システムの運用・管理状況などに関する問診結果と、脆弱性評価ソフトウェアとの組み合わせ、システムのセキュリティを診断し、被害予測および具体的な改善策を示すプログラムを予定している。脆弱性評価にあ

たっては、技術面だけでなく、運用面なども評価を実施する必要があり、情報資産の価値とあわせていかにバランスのとれた評価とすることができかが今後の課題である。サイバーテロからシステムや情報を確実に守るために、技術的・設備的・人的など様々な面から検討する。

防御技術

防御技術の目的

インターネットを活用し不特定多数からのアクセスを受け付けるシステムの急激な増加に伴い、これらの情報システム、ネットワークを保護することが重要な課題となっている。

本テーマでは、ファイアウォール、侵入検知装置(IDS)、トラップシステムなどのセキュリティ製品、防御技術の調査・開発を通じその課題に取り組んでいる。

この調査では、製品の特徴を捉え問題点を抽出することを目的に、標準化団体や評価機関の評価も参考に、サイバーテロ対策に有効な技術の調査を行う。

また、より確実な防御や攻撃の分析効率の向

上などを目指している。

ファイアウォールに係わる技術に関する調査

各種ファイアウォールの調査を実施した。主に、不正なパケットに対する動作の検証、アクセスログの記録方式や保存状態、侵入検知機能など、ネットワークやファイアウォール自身をセキュアに保つ方法を調査した。

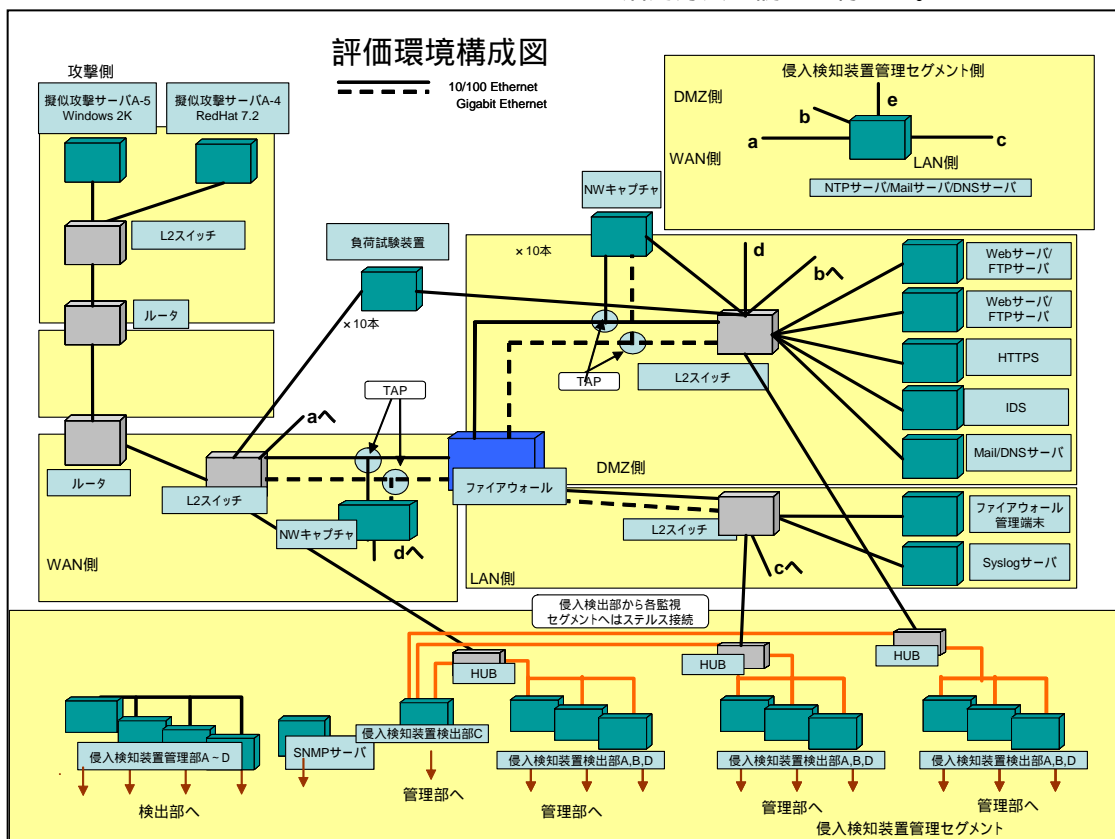
侵入検知装置に係わる技術に関する調査

各種侵入検知装置の調査を実施した。主に、検知アルゴリズムの違いによる攻撃検出状況の差異、アラートログ管理方法、ファイアウォールなど他のセキュリティ製品との連動性などを調査した。

トラップシステムに係わる技術に関する調査

トラップシステムはOSやWebサーバなどのアプリケーションを擬似的に稼働させて、攻撃者のアクセス、ふるまいを記録することができるものである。記録結果は攻撃手法の分析に利用されている。

トラップシステムの動作検証を通じて有効な活用方法の調査を行った。



今後の予定

今後も様々なファイアウォール、侵入検知装置、トラップシステムなどの調査を継続して実施していく。

ファイアウォールに係わる技術については、高負荷時でも有効に機能させる方策を、動作検証を通じて検討する。

侵入検知装置に係わる技術については、効率よい分析を目指し、異なる侵入検知装置製品間の情報を一元的に管理する仕組みを開発する。

トラップシステムに係わる技術については、OSだけでなくWebサーバなどのアプリケーションサーバを偽装する仕組みなどを研究開発する。

セキュリティ製品の導入はネットワークを確実に守ることが最たる目的であるが、万が一のセキュリティ侵害に備えて、迅速な対応や証拠保全のための適切な運用方法などを検討する。

ログ保存技術

ハイテク犯罪の脅威

コンピュータシステムの発展に伴いネットワーク化が進む昨今、ネットワークを悪用したコンピュータ関連犯罪はその割合が増加している。ネットワークを悪用したハイテク犯罪には以下の特徴がある。

- 高い匿名性の確保が容易に可能である
- 犯罪の痕跡、証拠が隠滅しやすく残りにくい
- 被害が多様で不特定多数に及ぶ
- 時間・場所に限定されない

この現状を踏まえこのテーマでは、コンピュータ内に残される/残すことが可能な情報の調査・研究を実施、ハイテク犯罪へ対抗する手段の確立を目指している。

目的

現在、ハイテク犯罪は高い匿名性、痕跡・証拠の隠滅の容易さから犯罪の捜査、追跡を非常に困難なものにしている。ウィルスの蔓延や不正アクセス、その他ハイテク犯罪に対しログはより一層、その重要性を増す。よって、ログ記録・分析技術の確立は急務である。

この問題に対応するためにはコンピュータ内に保存されるログを含む各種情報の改ざん・消去への対策と確実な記録保護が必要である。

また、記録された大容量情報から適切な情報を抽出し分析する必要がある。これらの課題を解決するために、本テーマでは次の研究を進めている。

ログ保存関連の研究

コンピュータ内に記録されるログの保護手法及び保存対象情報の調査・研究を実施している。また、保存情報の法的活用を可能とする研究も進めている

現在、各種OSのログ記録・保護手段の調査を完了しており、これを元にログ保存システムの研究・開発を実施する。

ログ分析関連の研究

大容量の情報から犯罪の行われた記録を検索、分析するには人的負荷が非常に高く、これを解消するべくログ分析の自動化の研究を進めている。

ログ分析自動化の基礎調査として、各種ログ分析ソフトウェアの調査を実施した。これを基に効率よい分析を可能とする支援ツールの研究・開発を実施する(下図参照)。

今後の予定

ログ保存関連については次の項目に重点を置き、保存システムの研究開発を行う。

- 記録した時刻の保証
- 記録情報の法的活用
- 記録情報利用者に対する利用記録や改ざん・消去防止

保存システムは犯罪の証拠を収集する手段である。よって、記録の改ざん・不正な消去を防止する手法の研究をあわせて実施していく必要がある。

ログ分析関連の研究は分析ツールの開発を進める。単一のログを分析するだけでなく、ファイアウォール、侵入検知装置、トラップシステム等に記録された複数のログを組み合わせた分析、相関分析の研究を実施する。

