博士学位論文

（内容の要旨及び論文審査の結果の要旨）

	Okubo　Kazuhiko
氏名	大久保　一彦
学位の種類	博士（経営情報科学）
学位記番号	博　乙　第 5 号
学位授与	平成 31 年 3 月 23 日
学位授与条件	学位規定第 3 条第 4 項該当
論文題目	IT システムおよびネットワークにおける情報セキュリティ確保技術に関する一研究
論文審査委員	（主査）教授　河辺　義信[1]
	（審査委員）教授　中條　直也[1]　教授　石井　成美[2]

論文内容の要旨

IT システムおよびネットワークにおける情報セキュリティ確保技術に関する一研究

本論文は、機密性・完全性・可用性といった情報セキュリティの 3 大要素を確保するための技術について、IT システムおよびネットワークを対象に論文提出者自身が行った 4 つの研究を中心に、検討ならびに考察を行った結果をまとめたものである。本論文は全 6 章から構成される。

第一章では、初のコンピューター・ウィルスが出現したと言われる 1985 年から現在までにおける、サイバーを取り巻く環境変化とセキュリティ上の課題の変遷を踏まえつつ、「IT」「IoT/OT」「重要インフラ」のそれぞれの領域において、昨今の具現化する脅威と必要なセキュリティ技術について、領域網羅的に概説する。情報セキュリティの 3 大要素を、ここ数十年間のサイバー脅威の変遷に照らし合わせて考えると概ね、1990 年代は比較的に可用性を重視しており、2000 年代に入ると機密性・完全性の確保が課題に、そして 2010 年代は、重要インフラや制御システムへのサイバー攻撃を鑑みると、再び可用性の配慮も取り沙汰されてきていると考えられる。

特に IT の領域においては、永遠のいたちごっこの如く巧妙化・大規模化するサイバー攻撃に対抗するため、従来の監視対象である法人及びホームネットワークや ISP ネットワークに加え、よりミクロやマクロの観点から、エンドポイントならびにバックボーンネットワークへ監視対象を拡大し、新たな対策技術を確立する必要がある。また、システムやネットワークのセキュリティに着目したセキュリティ技術が開発されてきた一方で、「実際に騙されてしまうのはユーザである」という視点から、ヒューマン・コンピュータ・インタラクションに着目したユーザブルプライバシー＆セキュリティに関わる技術も注目されつつあることを言及する。

第二章では、インターネットがブレイクする以前に期待が高まっていた、双方向マルチメディアサービスについて、特に当時のセキュリティにおける可用性重視の観点から、そのシステムおよびネットワークの設計手法を述べる。具体的には、1990 年代後半に千葉県浦安市において約 350 世帯の一般家庭を対象として提供された双方向マルチメディアサービスを題材に、セキュリティ・バイ・デザインのコンセプトのもと、システム設計法について提案を行う。

まず、サービスアプリケーションの通信に関する特徴から ATM ネットワークにおける VC を 3 つに分類し、それぞれについて設計上の課題をとらえ、モデル化による分析を進める。そのうえで、(1) 加入者側伝送リンクの利用率向上を図る共用端末数の設定、(2) ユーザに不快感を与えない音声通信アプリケーション起動数の設定、(3) 実トラヒック見合いの必要 VC 数算出とシステム構成に影響を与えない VC 収容法を提案するとともに、実システムによりデータを取得し、評価を行うことにより、モデルの妥当性を検証する。

以下、第三章から第五章では、IT セキュリティにフォーカスし、開発が嘱望される 3 つのサイバー攻撃対策技術（情報セキュリティ確保のための技術）、すなわち「通

1 愛知工業大学 情報科学部 情報科学科（豊田市）
2 愛知工業大学 経営学部 経営学科（豊田市）

信ログ分析に基づくマルウェア感染検知」、「悪性 Web サイトにおける Evasive コード特定」、「メモリフォレンジックの高度なスタックトレース」について述べる。

第三章では、セキュリティログ分析において、SIEM 等の 構築や運用にかかる手間暇が、その難しさ（効果的な検知手法の確立）や膨大なログの分析に伴う稼働量の大きさゆえ課題となっている中、悪性通信ログ判定を行うにあたって、従来手法を上回る高精度なマルウェア感染端末の検知技術を提案する。

通信ログのうち、特に当該判定の重要な情報源となる URL や User-Agent 等の特徴抽出手法として Bag of Words (BoW)の手法が有名であるが、テキストのパターン変化が頻出するケースにおいてはスケールしないという課題がある。これに対し、データ圧縮アルゴリズムを用い、その圧縮率を特徴として教師あり学習に適用する特徴抽出手法を提案することで、従来手法によるマルウェア感染端末判定よりも高精度な判定が実現できることを実験を通じて示す。特に提案手法において、API 的に使われる URL 等のパターン化した URL、FQDN、Path における類似性を認識して特徴抽出を行えることが、データ圧縮アルゴリズムを用いる利点であると考えている。

第四章では、巧妙な悪性 Web サイトで活用されている Evasive コード（サンドボックスによる解析を回避する機能）を特定する技術について説明する。特に、ブラウザの癖に基づくエクスプロイト・コードすなわち、Web ブラウザをエミュレートするタイプのロー・インタラクション型のハニークライアントによる解析を回避する Evasive コードの特定手法を追究する。

具体的には、実際の Web ブラウザを用いるタイプのハイ・インタラクション型とロー・インタラクション型のハニークライアントのリダイレクション先の差異に基づいて、Evasive コードが含まれると考えられる Java スクリプトの抽出を行い、それらを想定される Evasive テクニックの観点からの分類（クラシフィケーション）する。その結果、5 種類の Evasive コードの特定に成功したが、特定した Evasive テクニックのそれぞれに対し、実際の Web ブラウザの振る舞いを検証するとともに、「setTimeout 関数の引数の扱い」と「配列における”,”の扱いの差異」に関わる Evasive コードについては、近年のアタックキャンペーンで悪用されていたことを言及する。

第五章では、メモリフォレンジックをテーマにしているが、最近の Windows x64 オペレーティングシステムでは、処理効率化等の理由から、コンパイラがフレームポインタを用いずに関数を生成するようになったことから、フレームポインタを活用した（メモリフォレンジックにおいて重要な役割を果たす）スタックトレースができない状況になっている。

Windows x64 のメモリダンプを使ってスレッドのスタックトレースを行うために、スタック・アンワインディングのエミュレーションを適用する手法を提案し、特に例外処理用のメタデータが使えない場合においては、プログラムコードの制御フロー分析を加味することで、従来のスキャンベースのものより正確にリターンアドレスが特定できる方式を提案する。提案方式の評価にあたっては、高度なフォレンジック及びインシデント・レスポンスのためのフレームワークのプラグインとして提案手法を実装し、Microsoft がフリーで提供するカーネルデバッガとの比較評価を行う。

第六章では、本論文のまとめとするとともに、AI が人知を超えると言われる Singularity の時代（2045 年問題）に向けて、現在進化を遂げつつある AI のセキュリティに関わる技術開発の現状も加えたうえで、今後の研究について展望を示す。

ＡＩによる高度なハッキング等が主流になる可能性がある中、防御側も AI 等を活用した自動化技術が必須になるが、バイナリから自動で脆弱性を発見する技術や、シンボリック実行等を活用して攻撃発動条件を自動抽出する技術といった要素技術の確立が急務であることを示す。また、技術に加え、法制度の視点からもセキュリティ課題を解決していくことが肝要であり、最近の国策レベルでの共同研究についても紹介する。最後に、永遠に続くいたちごっこの世界を、多面的視点から果敢に技術・法制度等の創出に挑んでいく姿勢が人類にとって不可欠であることを言及し、本論文を締めくくる。

論文審査の結果の要旨

大久保一彦君の提出した博士論文「IT システムおよびネットワークにおける情報セキュリティ確保技術に関する一研究」は、情報セキュリティの 3 大要素（機密性・完全性・可用性）を確保する技術について、論文提出者自身の４つの研究結果をまとめたものである。全6章から成る。

第一章では、初のコンピューター・ウィルスが出現した 1985 年から現在までのサイバーを取り巻く環境変化とセキュリティ上の課題の変遷を踏まえ、「IT」「IoT/OT」「重要インフラ」のそれぞれの領域において、脅威と必要なセキュリティ技術を領域網羅的に述べている。

第二章では、双方向マルチメディアサービスについて、セキュリティにおける可用性重視の観点からのシステムおよびネットワークの設計手法を述べている。また、1990 年代後半に千葉県浦安市において約 350 世帯の一般家庭

を対象として提供された双方向マルチメディアサービスを題材に、セキュリティ・バイ・デザインのコンセプトのもと、システム設計法について提案を行っている。サービスアプリケーションの通信に関する特徴から ATM ネットワークにおける VC を 3 つに分類し、それぞれについて設計上の課題をとらえ、モデル化と分析を行った。そのうえで、(1) 加入者側伝送リンクの利用率向上を図る共用端末数の設定、(2) ユーザに不快感を与えない音声通信アプリケーション起動数の設定、(3) 実トラヒック見合いの必要 VC 数算出とシステム構成に影響を与えない VC 収容法を提案するとともに、実システムからのデータ取得と評価を行って、モデルの妥当性を検証している。

第三章以降では、IT セキュリティにフォーカスし、3 つのサイバー攻撃対策技術が述べられている。このうち第三章では、セキュリティログ分析（とくに、悪性通信ログ判定）のための、 従来手法を上回る高精度なマルウェア感染端末の検知技術を提案している。判定の重要な情報源となる URL や User-Agent 等の特徴抽出手法として Bag of Words (BoW)の手法が有名であるが、テキストのパターン変化が頻出するケースにおいてはスケールしないという課題があった。これに対し本研究では、データ圧縮の圧縮率を特徴とした教師あり学習に基づく特徴抽出手法を提案し、従来手法よりも高精度なマルウェア感染端末の判定法を与えている。また、その有効性を実験的に示している。特に提案手法より、API 的に使われる URL 等パターン化した URL、FQDN、Path における類似性を認識して特徴抽出を行えることが示された。

第四章では、巧妙な悪性 Web サイトで活用されている Evasive コード（サンドボックスによる解析を回避する機能)を特定する技術について述べている。特に本研究では、ブラウザの癖に基づくエクスプロイト・コード、すなわち、Web ブラウザをエミュレートするタイプのロー・インタラクション型のハニークライアントによる解析を回避する Evasive コードの特定手法を開発している。具体的には、実際の Web ブラウザを用いるタイプのハイ・インタラクション型とロー・インタラクション型のハニークライアントのリダイレクション先の差異に基づいて、Evasive コードが含まれると考えられる Java スクリプトの抽出を行い、想定される Evasive テクニックの観点から分類（クラシフィケーション）を行った。その結果、5 種類の Evasive コードの特定に成功した。一方で、特定した Evasive テクニックのそれぞれに対し、実際の Web ブラウザの振る舞いが検証されるとともに、「setTimeout 関数の引数の扱い」と「配列における”,”の扱いの差異」に関わる Evasive コードについては近年のアタックキャンペーンで悪用されていたことについても、論文中で述べられている。

第五章では、メモリフォレンジックをテーマにしている。最近の Windows x64 オペレーティングシステムでは、処理効率化等の理由から、コンパイラがフレームポインタを用いずに関数を生成するようになっている。そのため、フレームポインタを活用した（メモリフォレンジックにおいて重要な役割を果たす）スタックトレースができない状況になっていた。これに対し論文提出者は、Windows x64 のメモリダンプを使ってスレッドのスタックトレースを行うために、スタック・アンワインディングのエミュレーションを適用する手法を提案している。特に例外処理用のメタデータが使えない場合において、プログラムコードの制御フロー分析を加味することで、従来のスキャンベースのものより正確にリターンアドレスを特定できる方式を提案している。提案方式の評価にあたっては、高度なフォレンジック及びインシデント・レスポンスのためのフレームワークのプラグインとして提案手法を実装し、Microsoft がフリーで提供するカーネルデバッガとの比較評価を行っている。

第六章では、本論文のまとめとするとともに、AI が人知を超えると言われる Singularity の時代(2045 年問題)に向けて、現在進化を遂げつつある AI のセキュリティに関わる技術開発の現状も加えたうえで、今後の研究について展望を示している。ＡＩによる高度なハッキング等が主流になる可能性がある中、防御側も AI 等を活用した自動化技術が必須となる。こうした動きを鑑みて、バイナリから自動で脆弱性を発見する技術や、シンボリック実行等を活用して攻撃発動条件を自動抽出する技術といった要素技術の確立が急務であることを指摘している。また、技術のみならず、法制度の視点からもセキュリティ課題を解決していくことが肝要である。こうした点についての最近の国策レベルでの共同研究や動向についても紹介している。最後に、永遠に続くいたちごっこの世界を、多面的視点から果敢に技術・法制度等の創出に挑んでいく姿勢が人類にとって不可欠であることを述べ、本論文を締めくくっている。

審査委員会の委員 3 名が論文執筆者から提出された論文原稿の内容を詳しく審査した結果、本論文は博士（経営情報科学）の学位を受けるに十分な内容を持ち、博士学位論文として受理するに値するものであるとの結論に達した。