[2017]九州大学情報統括本部年報 : 2017年度

出版情報：九州大学情報統括本部年報. 2017, pp.1-, 2018-10-01. Information Infrastructure Initiative, Kyushu University
バージョン：
権利関係：

第4章　先端ネットワーク研究部門

4.1 スタッフ一覧

職名	氏名	研究キーワード
教授	岡村 耕二	インターネット、新世代ネットワーク、サイバーセキュリティ、マルウェア解析、教育
助教	笠原 義晃	計算機ネットワーク、インターネット運用技術、侵入検知、ネットワークセキュリティ

4.2 研究事例紹介

「レジストリの変化量に着目した未知のマルウェアの検知」

4.2.1　概要

近年サイバー犯罪による被害が深刻化しており、サイバーセキュリティの技術が重要になってきている。従来のアンチウイルスソフトのマルウェア検知手法のほとんどは、マルウェアのデータ構造を記述した定義データとの単純比較である。しかし、この手法では、定義データが対応しない未知のマルウェアの検知が困難である。そこで、解析前の未知のマルウェアによる攻撃を防止するための技術として、振る舞い検知が有効である。本研究では、様々なツールを用いて、マルウェア実行時のファイルやレジストリへのアクセス状況を解析した。その解析結果に基づき、レジストリの変化量に着目した未知のマルウェアの検知手法について検討する [6]。

4.2.2　はじめに

近年、インターネットの急速な普及に伴いサイバー犯罪による被害が深刻化しており、サイバーセキュリティの技術が重要になってきている。従来の対策は、パターンマッチングタイプのアンチウイルスソフトウェアや、パケットモニタリングなどの人手によるものであった。しかし、近年は毎日のように新種の攻撃が出現してきており、人手による対策には限界がある。このような要因から、新たな対策手法が必要とされている。

本研究では、サイバー犯罪の中でも、マルウェアによるものに着目する。近年、電子メールや Web サイトの閲覧を通じてコンピュータウイルスに感染する被害が増えている。オリジナルを一部改変した多くの亜種ウイルス、自らのプログラムの一部を自ら変更するウイルス等があり、これらについては、従来のワクチンソフトが採用している単純な定義ファイルとの比較を主としたパターンマッチングによる手法では即時の対応・発見が困難である。そのため、定義ファイルが作成されていないウイルスの感染が瞬時に拡大する危険性がある [1]。マルウェアの作成者は、解析や検知を逃れるための新たな方法を常に探している。新種のマルウェアには、OS の機能を悪用し、ディスクにファイルを残すことなく悪意のあるコードをメモリや OS のレジストリに埋め込むものがある。ファイルを利用しない（ファイルレス）マルウェア攻撃では、レジストリにコードを埋め込む方法が現在の主流となっている。ファイルレス攻撃は多くの場合、電子メールメッセージ内のファイルまたはリンクとしてシ

ステムに侵入する。リンクまたは添付ファイルがクリックされると、マルウェアはレジストリにペイロードを書き込み、そのあと消失する。レジストリに書き込まれたペイロードには、何層ものトリックに隠されたスクリプトが含まれている。このスクリプトは正当なWindowsプログラム（PowerShellなど）を呼び出し、svchost、dllhost、regsvr32など標準的なWindowsプロセスのメモリ領域に悪意のあるコードを埋め込む。このため、悪意のあるプロセスを探してスキャンを実行しても、このコードを検出することはできない。ウイルス定義ファイルの更新だけでは、このようなファイルレス攻撃や、さらに新型のファイルレス攻撃に対する防御として不十分である[2]。レジストリは、Windowsで使用される中央階層型データベースで、１人または複数のユーザ、アプリケーションおよびハードウェア装置を構成するのに必要なシステム情報を格納するために使用さる。レジストリには、Windowsが実行中に絶えず参照する情報（各ユーザに関するプロファイル、コンピューターにインストールされているアプリケーションおよび各アプリケーションで作成可能なドキュメントの種類、フォルダおよびアプリケーションアイコンについてのプロパティシート設定、システム上に存在するハードウェアの種類、および使用中のポート、など）が格納される[3]。未知のマルウェアによる攻撃を防止するための技術として、振る舞い検知が有効である。本研究では、未知のマルウェアを検知できる振る舞い検知手法の実現を目的とし、様々なツールを用いて、マルウェア実行時のファイルやレジストリへのアクセス状況を解析した。解析結果から、通常マルウェアが実行されると、レジストリに何らかの変化をもたらすことが確認された。レジストリに関する挙動から、マルウェアのみに共通する挙動を捉えることができれば、パターンマッチングによる手法では検知できない未知のマルウェアであっても検知できる可能性がある。

本稿では、マルウェアの解析に使用するツールと解析手順について述べ、解析結果を示す。最後に、レジストリアクセスに基づいたマルウェア検知手法を検討する。

4.2.3　関連研究

マルウェアによる被害が深刻化している中、未知のマルウェアへの対策に関する多くの研究が行われている。本章では、マルウェア検知手法に関する研究のうち、マルウェアを実際に動作させ、その挙動に基づいて検知手法を提案している研究について述べる。

論文[4]では、検査対象の実行ファイルを複数回実行して得られたAPIログを比較することで、実行毎の挙動の差異を判断しマルウェアの検知を行う手法を提案している。この手法は、解析や検知への耐性を持たせて作成されたマルウェアのうち、実行毎に挙動に変化を生じさせるマルウェアに着目している。実行毎の挙動の変動を、正規のプログラムには必要がなくマルウェアのみが有する機能と仮定し、ある実行ファイルがマルウェアか否かを判断するための指標として用いている。

論文[5]では、マルウェアの攻撃対象となるシステム上におとりのプロセスを用意し、そのおとりのプロセスを強制終了させようとするプロセスを検知した場合、そのプロセスをマルウェアと判断し停止させることで、マルウェアの活動を抑止するという手法を提案している。この手法は、マルウェアの自己防衛機能の１つである、セキュリティ機能を無効化する攻撃に着目している。

4.2.4　マルウェアの解析

本章では、まず本研究でマルウェアの解析に使用するツールと解析手順について述べる。最後に解析結果を示す。

4.2.5　使用するツール

ToolWiz Time Freeze

ToolWiz Time Freeze は、システムドライブを仮想化して不要な変更や不正な活動からシステムを保護することができるソフトウェアである。システムドライブを仮想化して、それ以降に加えられた変更を、再起動すれば仮想化前の状態に戻すことができる。

Sandboxie

Sandboxie は、OS 上に仮想領域を作成しプログラムを安全に実行することができる。Sandboxie 上で実行されたプログラムはハードディスクにデータを書き込むことなくプログラムを実行することができる。

Process Monitor

Process Monitor は、OS 上のすべてのプロセスが行った処理（ファイル、レジストリ、プロセスおよびスレッドの活動）をリアルタイムで表示するツールである。システムのトラブルシューティングやマルウェア検知などに役立てることができる。例えば、アプリケーションがアクセスしているファイルやレジストリキーを特定したり、行われた処理が成功しているか失敗しているかを確認したりすることができる。

regshot

regshot は、2 つのレジストリを比較して変更を確認することができるツールである。例えば、アプリケーションを追加・削除した場合などシステムに変更を加えたときに、レジストリのどこが変更されたのかを調べるといった用途に利用できる。

4.2.6　手順

解析には Windows10 の PC を用いる。この解析用PC には、前述のツールを含め様々な解析ツールをインストールしている。また、組織内に配送された脅威メールに含まれるマルウェアを解析対象とする。

（1）ToolWiz Time Freeze を起動

PC を起動後、まず ToolWiz Time Freeze を起動し、それ以降に加えられた変更を、PC を再起動することで元に戻せる状態にする。

（2）regshot を実行

regshot を実行してマルウェア実行前のレジストリの状態を保存する。regshot は解析後に再度実行し、マルウェア実行後の状態との差分を取得する。

（3）Process Monitor を起動

Process Monitor を起動してプロセスのキャプチャを開始する。

（4）マルウェアを実行

Sandboxie 上で対象のマルウェアを実行する。

（5）ログを保存

各ツールで取得したログを保存する。解析終了後、取得したログに基づいて、マルウェア検知手法を検討する。

4.2.7　解析結果

Process Monitor で取得したログには、OS 上のすべてのプロセスが行った処理が含まれる。本研究では、マルウェアのプロセスのうち、レジストリアクセスに着目した。

表1及び表2は、通常正当な windows プロセスである regsvr32.exe の一部であるが、マルウェア実行時に悪意のあるコードを埋め込まれている。表中の RegOpenKey は、指定したレジストリキーを開く操作である。

表１のプロセスは、Path の最後に Fiddler.exe、Fiddler2.exe、Fiddler2 のいずれかを指定し、そのレジストリキーを開こうとしている。しかし、解析用PC にそれらのレジストリキーは存在しないため、処理が失敗している。Fiddler とは、HTTP (S) トラフィックに特化した、無料のネットワークキャプチャツールである。

表２のプロセスは、Path の最後に HTTPAnalyzerAddon、IEHTTPAnalyzer.HTTPAnalyzerAddOn、HTTP AnalyzerStd.HTTPAnalyzerStandAlone のいずれかを指定し、そのレジストリキーを開こうとしている。しかし、解析用PC にそれらのレジストリキーは存在しないため、処理が失敗している。HTTP Analyzer とは、HTTP パケットを調査することができるツールである。

これらのプロセスは、攻撃対象の PC に Fiddler や HTTP Analyzer といった解析ツールがインストールされているかを確認することを目的としたレジストリアクセスであると考えられる。

表 1　regsvr32.exe のプロセス 1

Operetion	Path	Result
RegOpenKey	HKLM¥SOFTWARE¥WOW6432Node¥Microsoft¥Windows¥CurrentVersion¥App Paths¥Fiddler.exe	REPARSE
RegOpenKey	HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥App Paths¥Fiddler.exe	NAME NOT FOUND
RegOpenKey	HKLM¥SOFTWARE¥WOW6432Node¥Microsoft¥Windows¥CurrentVersion¥App Paths¥Fiddler2.exe	REPARSE
RegOpenKey	HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥App Paths¥Fiddler2.exe	NAME NOT FOUND
RegOpenKey	HKLM¥SOFTWARE¥WOW6432Node¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥Fiddler2	NAME NOT FOUND
RegOpenKey	HKCU¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥Fiddler2	NAME NOT FOUND
RegOpenKey	HKLM¥Software¥WOW6432Node¥Microsoft¥Fiddler2	NAME NOT FOUND
RegOpenKey	HKLM¥SOFTWARE¥WOW6432Node¥Microsoft¥Fiddler2	NAME NOT FOUND
RegOpenKey	HKCU¥Software¥Microsoft¥Fiddler2	NAME NOT FOUND
RegOpenKey	HKCU¥SOFTWARE¥Microsoft¥Fiddler2	NAME NOT FOUND

表 2　regsvr32.exe のプロセス 2

Operetion	Path	Result
RegOpenKey	HKCR¥SOFTWARE¥IEInspectorSoft¥HTTPAnalyzerAddon	NAME NOT FOUND
RegOpenKey	HKCU¥SOFTWARE¥Classes¥SOFTWARE¥IEInspectorSoft¥HTTPAnalyzerAddon	REPARSE
RegOpenKey	HKCU¥Software¥Classes¥SOFTWARE¥IEInspectorSoft¥HTTPAnalyzerAddon	NAME NOT FOUND
RegOpenKey	HKCU¥Software¥Classes¥Software¥IEInspectorSoft¥HTTPAnalyzerAddon	NAME NOT FOUND
RegOpenKey	HKCR¥IEHTTPAnalyzer.HTTPAnalyzerAddOn	NAME NOT FOUND
RegOpenKey	HKCU¥SOFTWARE¥Classes¥IEHTTPAnalyzer.HTTPAnalyzerAddOn	REPARSE
RegOpenKey	HKCU¥Software¥Classes¥IEHTTPAnalyzer.HTTPAnalyzerAddOn	NAME NOT FOUND
RegOpenKey	HKCR¥HTTPAnalyzerStd.HTTPAnalyzerStandAlone	NAME NOT FOUND
RegOpenKey	HKCU¥SOFTWARE¥Classes¥HTTPAnalyzerStd.HTTPAnalyzerStandAlone	REPARSE
RegOpenKey	HKCU¥Software¥Classes¥HTTPAnalyzerStd.HTTPAnalyzerStandAlone	NAME NOT FOUND

表３も、通常正当な windows プロセスである regsvr32.exe の一部であるが、マルウェア実行時に悪意のあるコードを埋め込まれている。HKLM¥SOFTWARE¥WOW6432Node¥Microsoft¥Windows¥CurrentVersion¥AppPaths¥Wireshark.exe というレジストリキーを開くことに失敗しているが、HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥AppPaths¥Wireshark.exe を開くことに成功している。これは、解析用 PC に Wireshark というソフトウェアをインストールしており、このレジストリキーが存在するためである。指定したレジストリキーを開くことに成功した後は、そのレジストリキーを指定して、RegSetInfoKey、RegQueryKey、RegCloseKey という操作を行っている。RegSetInfoKey は、指定したレジストリキーに関する情報を書き込む操作である。RegQueryKey は、指定したレジストリキーに関する情報を取得する操作である。RegCloseKey は、指定したレジストリキーを閉じる操作である。

表 3　regsvr32.exe のプロセス 3

Operetion	Path	Result
RegOpenKey	HKLM¥SOFTWARE¥WOW6432Node¥Microsoft¥Windows¥CurrentVersion¥AppPaths¥Wireshark.exe	REPARSE
RegOpenKey	HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥AppPaths¥Wireshark.exe	SUCCESS
RegSetInfoKey	HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥AppPaths¥Wireshark.exe	SUCCESS

RegQueryKey	HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥App Paths¥Wireshark.exe	SUCCESS
RegCloseKey	HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥App Paths¥Wireshark.exe	SUCCESS

表４、表５及び表６は、複数のマルウェアで確認されたプロセスである。表中の RegCreateKey は、指定したレジストリキーを作成する操作である。表４では、マルウェアが、HKU¥Sandbox_{username}_DefaultBox¥user¥current¥SOFTWARE¥AppDataLow¥Software¥Microsoft¥173C91EB-8A2A-6118-4C3B-5E25409F7229 というレジストリキーを作成しようとしている。解析用PC に HKU¥Sandbox_{username}_DefaultBox¥user¥current¥SOFTWARE は存在するが、そこに AppDataLow が存在しない。そのためマルウェアは、目的のレジストリキーから Path を一つずつさかのぼって作成を試み、作成が成功すれば一つずつ Path を追加することで目的のレジストリキーを作成している。表５及び表６のように同様の挙動が確認された。

表 4　マルウェアのプロセス 1

Operetion	Path	Result
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥user¥current¥SOFTWARE¥AppDataLow¥Software¥Microsoft¥173C91EB-8A2A-6118-4C3B-5E25409F7229	NAME NOT FOUND
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥user¥current¥SOFTWARE¥AppDataLow¥Software¥Microsoft	NAME NOT FOUND
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥user¥current¥SOFTWARE¥AppDataLow¥Software	NAME NOT FOUND
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥user¥current¥SOFTWARE¥AppDataLow	SUCCESS
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥user¥current¥SOFTWARE¥AppDataLow¥Software	SUCCESS
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥user¥current¥SOFTWARE¥AppDataLow¥Software¥Microsoft	SUCCESS
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥user¥current¥SOFTWARE¥AppDataLow¥Software¥Microsoft¥173C91EB-8A2A-6118-4C3B-5E25409F7229	SUCCESS

表 5　マルウェアのプロセス 2

Operetion	Path	Result
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥MACHINE¥SOFTWARE¥WOW6432Node¥Microsoft¥Windows¥CurrentVersion¥Explorer¥SyncRootManager	NAME NOT FOUND
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥MACHINE¥SOFTWARE¥WOW6432Node¥Microsoft¥Windows¥CurrentVersion¥Explorer	NAME NOT FOUND
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥MACHINE¥SOFTWARE¥WOW6432Node¥Microsoft¥Windows¥CurrentVersion	NAME NOT FOUND
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥MACHINE¥SOFTWARE¥WOW6432Node¥Microsoft¥Windows	NAME NOT FOUND
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥MACHINE¥SOFTWARE¥WOW6432Node¥Microsoft	NAME NOT FOUND
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥MACHINE¥SOFTWARE¥WOW6432Node	SUCCESS
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥MACHINE¥SOFTWARE¥WOW6432Node¥Microsoft	SUCCESS
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥MACHINE¥SOFTWARE¥WOW6432Node¥Microsoft¥Windows	SUCCESS
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥MACHINE¥SOFTWARE¥WOW6432Node¥Microsoft¥Windows¥CurrentVersion	SUCCESS
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥MACHINE¥SOFTWARE¥WOW6432Node¥Microsoft¥Windows¥CurrentVersion¥Explorer	SUCCESS
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥MACHINE¥SOFTWARE¥WOW6432Node¥Microsoft¥Windows¥CurrentVersion¥Explorer¥SyncRootManager	SUCCESS

表 6　マルウェアのプロセス 3

Operetion	Path	Result
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥user¥current¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Internet Settings¥ZoneMap	NAME NOT FOUND
RegCreateKey	HKU¥Sandbox_{username}_DefaultBox¥user¥current¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Internet Settings	SUCCESS

RegCreateKey	HKU¥Sandbox_{username} _DefaultBox¥user¥current ¥SOFTWARE¥Microsoft¥ Windows¥CurrentVersion¥ Internet Settings¥ZoneMap	SUCCESS

4.2.8　提案手法

本章では、マルウェアの解析結果に基づき、レジストリの変化量に着目した未知のマルウェアの検知手法を検討する。レジストリに関する挙動から、マルウェアのみに共通する挙動を捉えることで、パターンマッチングによる手法では検知できない未知のマルウェアの検知が期待できる。

本研究では、マルウェア実行時のレジストリへのアクセス状況に着目した。解析で確認された、攻撃対象の PC に解析ツールがインストールされているかを確認することを目的とした挙動や、目的のレジストリキーを作成するために Path を一つずつさかのぼって作成を試み失敗を繰り返す挙動を、正規のプログラムには必要がなくマルウェアのみが有するプロセスであると判断し検知する手法を提案する。

また、マルウェアによるレジストリアクセスには、その処理が失敗しているものが多く確認された。指定したレジストリキーを開く操作や指定したレジストリキーを作成する操作といったレジストリアクセスの種類や、特定の Path でプロセスにフィルタをかけ、処理の失敗率を定義することでマルウェア検知の指標にできると考える。

提案手法の有効性を評価する指標として、従来のパターンマッチングタイプのアンチウイルスソフトウェアでは検知できないマルウェアに適用した際の検知率を用いる。この検知率が一定以上であれば、未知のマルウェアの検知手法としての提案手法の有効性が示される。また、正規のプログラムに適用した際にマルウェアとして誤検知する確率を抑えられているかも有効性を評価する指標として用いる。

4.2.9　まとめと今後の課題

本研究では、未知のマルウェアを検知できる振る舞い検知手法の実現を目的とし、様々なツールを用いて、マルウェア実行時のファイルやレジストリへのアクセス状況を解析した。取得したマルウェア実行時のプロセスのうち、レジストリアクセスに着目し、解析結果を示した。解析で確認されたマルウェアによるレジストリアクセスを、正規のプログラムには必要がなくマルウェアのみが有するプロセスであると仮定しマルウェアを検知する手法を提案した。

提案手法の有効性を示すことが今後の課題である。提案手法の評価実験を行う前に、誤検知を防ぐために、正規のプログラムによるレジストリアクセスを把握する必要がある。また、本稿で示したマルウェアによるレジストリアクセスのほかに新たな挙動を捉えられれば、検知の精度を向上させることができる可能性がある。

レジストリアクセスの種類や特定の Path でプロセスにフィルタをかけ、処理の失敗率からマルウェアを検知する手法では、フィルタのかけ方や処理の失敗率の定義の仕方が今後の検討課題である。

参考文献

[1]　“未知ウイルス検出技術に関する調査”. https://www.ipa.go.jp/security/fy15/reports/uvd/documents/uvd_report.pdf, (参照 2017-08-09).

[2]　“高度化するファイルレス攻撃に対処せよ”. http://blogs.mcafee.jp/mcafeeblog/2016/02/post-e8b5.html, (参照 2017-08-09).

[3]　“上級ユーザー向けのWindowsレジストリ情報”. https://support.microsoft.com/ja-jp/help/256986/windows-registry-information-for-advanced-users, (参照 2017-08-08).

[4]　笠間貴弘, 吉岡克成, 井上大介, 松本勉. 実行毎の挙動の差異に基づくマルウェア検知手法の提案. Computer Security Symposium 2011, 2011.

[5]　松木隆宏, 新井悠, 寺田真敏, 土居範久. セキュリティ無効化攻撃を利用したマルウェアの検知と活動抑止手法の提案. 情報処理学会論文誌. 2009, vol.50, no.9, p.2127-2136.

[6]　向野 賢人, 岡村 耕二, “レジストリの変化量に着目した未知のマルウェアの検知に関する研究”, コンピュータセキュリティシンポジウム2017論文集(2017年10月).

4.3　研究内容紹介

4.3.1 岡村 耕二

研究内容

私は、1988年に九州大学工学部で卒業研究を行って以来、三菱電機株式会社、奈良先端科学技術大学院大学、神戸大学、九州大学において、20年以上にわたって、コンピュータ・ネットワークに関わる研究や仕事、また、学生への教育をしてまいりました。九州大学の助教授に着任しました1998年以降の約12年間の教育や研究内容について、1）基礎技術的な内容のもの、2）応用・実践的あるいは国際的な内容のものに分けて紹介いたします。

1）基礎技術的な内容の教育・研究

インターネットに関する基礎的な内容の教育・研究は、学術振興会・未来開拓研究「知的で動的なネットワーキング」（コアメンバー）、総務省通信総合研究所（現在の情報通信研究機構）と取り組んだ「新世代モバイル通信技術」、韓国の大学・研究機関との総合的な共同研究である学術振興会・日韓拠点大学プロジェクト、国立情報学研究所とともに取り組んでいる CSI（Cyber Science Infrastructure）プロジェクトそして、最近では新世代ネットワークの研究などを通じて行ってきました。

1999年からコアメンバーとして参加した学術振興会・未来開拓研究「知的で動的なネットワーキング」プロジェクトでは、専門家以外には難解なネットワークの設定について、その自動化をめざし、最終的にはネットワークの構成要素が変化してもネットワークがその変化に追随して最適なネットワーク環境が自動的に構成されることを目標にした研究に取り組みました。この研究の一部は当時の学生の修士研究としても進められましたが、その成果は最終的に情報処理学会の論文誌に掲載することができました。2003年から、韓国の主要な大学・研究機関と日本の間の総合的な共同研究を行う、日韓拠点大学方式の総括責任者として、本プロジェクトを遂行するとともに、自分自身も韓国の研究機関と共同研究を行ってきました。私の主たるテーマは、国際的なネットワーク運用と、遠隔医療などの国際応用技術に関するものです。国際的なネットワークの運用のための技術として、私の研究室で行ってきた、蓄積されたネットワークのトラフィック・経路情報の統計処理技術と、韓国の実践的な解析技術を融合させることに成功し、2007年末に発生しました台湾南沖地震で発生した日本と中国の間の光ファイバ切断がインターネットに与えた影響を、私の研究室と韓国の先生と共同で解析し、災害に対する現在のインターネット運用技術の課題をまとめることができました。これは当時の学生の修士研究、博士研究の一部として取り組み、この成果は、情報処理学会、電気通信学会のそれぞれの論文誌に掲載されました。さらに、次世代ネットワーク技術について着目した研究では、韓国人の博士課程の学生と韓国で一足先に始まった、次世代ネットワーク網のデータ解析を行い、それを日本に提言することができました。この成果も情報処理学会論文誌に掲載されております。また、最近では新世代ネットワークにおける仮想ネットワーク技術、新しいデータ交換技術、省電力運用技術に着目した研究を行い、すでにいくつかの国際会議にその成果を投稿し、発表しております。

2）応用・実践的、国際な内容の教育・研究

応用・実践的、国際な教育・研究として、総務省・情報通信研究機構が提供するＪＧＮ(Japan Giga Network）に関連する公募によるもの、日韓光ファイバに関連するもの、国際遠隔医療に関するものなどに取り組んできました。JGN を用いた研究として、高精細動画像伝送に関わる研究、IPv6 に関する研究、次世代型インターネット拠点のアーキテクチャに関する研究に取り組んできました。次世代型インターネット拠点のアーキテクチャに関する研究では、福岡に設立された九州ギガポッププロジェクト（QGPOP）の主要なメンバーとして研究活動を行い、このプロジェクトで培った高度なネットワーク運用技術はのちの実証実験で活用されています。日韓光ファイバに関する研究では、九州・山口経済連合が導入した福岡と釜山の間の光ファイバの利活用について、産官学非常に多くのさまざまな方々と玄海プロジェクトを 2001 年に設立させ、2003 年にはインターネットとしての利用に成功、さらに、総務省からそのネットワークを利用した 5 年後の IT 社会を模索する研究（e! プロジェクト）を委託され、国際的な近未来的な遠隔講義、遠隔医療の実証実験に取り組みました。さらに、この活動が評価され、学術振興会による日韓拠点事業が認められました。この事業は 8 年にわたって行われ、私はその総括責任者として日韓で 200 名以上の研究者の代表として事業を成し遂げました。国際遠隔医療は、2002 年から九州大学病院と構想を練り始め、2003 年から韓国と実施をはじめ、以降、九州大学の P&P や学術振興会・アジアコアプログラムの支援などを利用してアジアの各国、オセアニア、米国、欧州などの共同研究医療機関を開拓し、現在では約 20 カ国、世界中の約 90 の医療機関と高精細動画像を用いた遠隔医療の先進的な事例実験に成功しています。この遠隔医療の実証研究の成果・評価の一つとして、九州大学病院にアジア遠隔医療センター（TEMDEC）の設置への貢献をあげることができます。遠隔医療に関する学術的な研究成果は九州大学病院の教員と共著で多くの国際会議などで発表し、高い評価を得ております。

以上のように私は、コンピュータ・ネットワーク技術について、基礎的な内容での教育・研究活動を継続して行い、その成果を論文誌、国際会議論文誌また学会誌に残してきています。また、この延長で、いままで主査として 2 名の学生に博士号（大学院　システム情報科学府）を授与させることができました。応用・実践的、国際的な教育・研究の推進で、企業や省庁、自治体と連携した実用的な研究活動や、海外の多くの研究機関とも連携した国際的な研究活動を行い、研究室の学生に国際的な共同研究の機会も与えるとともに、対外的に九州大学のプレゼンスをあげ、その研究活動で得た最新の技術を九州大学のキャンパスネットワークなどの IT インフラや九州大学病院の活動に還元してきました。

所属学会名

IEEE，教育システム情報学会，電子情報通信学会，情報処理学会

主な研究テーマ

- 新世代ネットワークに関する研究
  キーワード：新世代ネットワーク，2010.04～

- サイバーセキュリティ
  キーワード：サイバーセキュリティ，2014.03～
- 国際的インターネット実証研究
  キーワード：イーサイエンス，2013.04～

研究プロジェクト

- 実践的セキュリティ人材の育成
  2016.10～2021.03.
- 安全な IoT サイバー空間の実現
  2016.11～2022.09，代表者：岡村耕二，インド工科大学デリー校
- サイバーセキュリティ
  2014.04～，代表者：岡村耕二，メリーランド大学　ボルチモア校
- 九州大学　サイバーセキュリティ
  2013.03～，代表者：安浦寛人
- アジア遠隔医療研究開発
  2008.10～，代表者：清水周次
- 日韓およびアジア地域次世代インターネットプロジェクト
  2001.07～，日本，韓国，タイ，シンガポール　日韓およびアジアでの次世代インターネットのリーダーシップをとる

研究業績

• 原著論文

1. Sanouphab Phomkeona,Yoshitatsu Ban, Koji Okamura, An Investigation and Analysis Method for Suspicious Zero-day Malicious Emails, Proceedings of International Conference on Internet (ICONI 2017), 2017.12.
2. Mohd Zafran B Abd Aziz, Koji OKAMURA, Leveraging SDN for Detection and Mitigation SMTP Flood Attack through Deep Learning Analysis Techniques, International Journal of Computer Science and Network Security, 2017.10.
3. Sanouphab Phomkeona,Kristan Edwards,Yoshitatsu Ban, Koji Okamura, Zero-day Malicious Email Behavior Investigation and Analysis, Proceedings of Research Network Workshop 2017, 2017.08.
4. Mohd Zafran B Abd Aziz, Koji OKAMURA, A Collaborative Mitigation SMTP flood Attack using SDN platform on Multi Site, International Journal of Computer Science and Network Security, 2017.07.
5. Alaa M. Allakany, KOJI OKAMURA, Latency Monitoring in Software-Defined Networks, Proceedings of the 12th International Conference on Future Internet Technologies, 2017.06.
6. Mohd Zafran B Abd Aziz, Koji OKAMURA, A Method to Detect SMTP Flood Attacks using FlowIDS Framework, International Journal of Computer Science and Network Security, 2017.06.

7. Alaa M. Allakany, KOJI OKAMURA, Load Balance for Multicast Traffic in SDN using OnTime traffic Monitoring, International Journal of Computer Science and Information Security, 2017.04.
8. Alaa M. Allakany, KOJI OKAMURA, Efficient Multicasting Algorithm Using SDN, International Journal of Computer Science and Network Security, 2017.04.

- **学会発表**

1. 岡村耕二，サイバーセキュリティ基礎教育へのシリアスゲームの導入効果に関する研究，大学ICT 推進協議会2017年度年次大会，2017.12.
2. 向野　賢人，岡村　耕二，レジストリの変化量に着目した未知のマルウェアの検知に関する研究，コンピュータセキュリティシンポジウム，2017.10.

研究資金

- **科学研究費補助金**

1. 2016年度～2018年度，基盤研究（C），代表，サイバーセキュリティ攻撃の水平・垂直解析によるサイバー演習支援に関する研究

- **競争的資金**

1. 2016年度～2020年度，文科省 成長分野を支える情報技術人材の育成拠点の形成，分担，実践的セキュリティ人材の育成
2. 2016年度～2021年度，JST 戦略的国際共同研究プログラム，代表，安全なIoT サイバー空間の実現

- **共同研究、受託研究**

1. 2017.11～2018.03，代表，ネットワークトラフィック情報から脅威情報の抽出技術の研究

教育活動

- **担当授業科目**

1. 2017年度・後期，情報ネットワーク特論
2. 2017年度・後期，情報ネットワーク
3. 2017年度・夏学期，サイバーセキュリティ演習

4. 2017年度・冬学期，企業から見たサイバーセキュリティ
5. 2017年度・夏学期，企業から見たサイバーセキュリティ
6. 2017年度・春学期，サイバーセキュリティ基礎論

社会貢献・国際連携

• 社会貢献・国際連携活動概要

1. 通信・放送機構 委託研究評価委員
2. 北九州ギガビットラボ 利用促進部長
3. 北九州IT研究開発基盤利用促進協議会 会長
4. 福岡県 ギガビットハイウェイ 構想委員

• 一般市民、社会活動及び産業界等を対象とした活動

1. 2018.02, JMOOC「個人と組織のための最先端サイバーセキュリティ入門　反転学習」, 九州大学サイバーセキュリティセンター, 杏林大学総合政策学部, NetLearning, 杏林大学
2. 2018.03, せきゅトーク 2018 in 福岡, 九州大学サイバーセキュリティセンター, JR博多シティ会議室
3. 2017.04～，福岡県警とサイバーセキュリティに関する連携に関する協定を締結し，活動を行っている，福岡県警

大学運営

• 学内運営に関わる各種委員・役職等

1. 2012.04～，全国共同利用運営委員会
2. 2007.04～，全学情報環境利用委員会
3. 2003.04～，セキュリティ専門委員会

4.3.2 笠原 義晃

研究内容

- **安定した情報サービスのためのサーバ品質の監視・異常検知・品質改善**

インターネットではさまざまな種類の情報サービスが提供されている。九州大学でも構成員に向けてさまざまなサービスを提供している。サービスを提供する機器（サーバ等）の増加により、管理は複雑さを増しており、期待される性能が出ていなかったり、異常が発生していても迅速に対応できない場合が増えている。仮想化技術の進展により仮想計算機によるサービス構築も容易になったが、仮想化レイヤが増加することにより障害対応はより複雑になった。
本研究では、実サービスの運用管理を通して、仮想化システムも視野に入れた、統一されていない多数のサーバによるサービス提供環境において、管理者の負荷を低減し効率的に管理・運用が可能な手法の構築を目指す。

- **ネットワークトラフィック監視に基づく侵入検知・裏口検出に関する研究**

インターネットを利用した計算機への不正アクセスや、ウィルス・ワーム・ボット等の自動化された侵入・拡散ソフトウェアによる被害は年々増加し、また手口も巧妙化している。これに対抗するには、ホストレベルからネットワークレベルに到る多層的な対策が必要となる。
本研究では、このうち特にネットワークでの対策に重点をおき、組織の基幹ネットワーク管理者の立場から組織内ネットワークでの不正な活動などを監視・検出する手法を研究・開発する。具体的には、ネットワークトラフィックを受動的に収集し、パターンによらない分類手法や、プロトコルの特徴を利用した異常検知手法について検討している。これにより、既存のパターン検出型侵入検知システムでの検知が難しい活動を発見する事を目指している。

- **その他の活動**

九州大学の学内ネットワークである総合情報伝達システム（KITE）の管理・運用に参加し、学内外向け各種サーバの管理・運用、新規サービスの開発等を行っている。
また、管理者向け講習会の実施、管理者や利用者からの質問への対応、侵入検知システム等の監視による学内ネットワークの保全等、安定したネットワークを維持するための活動を続けている。

所属学会名

情報処理学会，電気情報通信学会

主な研究テーマ

- 安定した情報サービスのためのサーバ品質の監視・異常検知・品質改善
  キーワード：情報システム，サーバ管理・運用，仮想化，2012.04～.
- ネットワーク監視に基づく侵入検知・異常検知
  キーワード：インターネット，ネットワーク管理運用，侵入検知，ネットワークセキュリティ，2001.04～.

研究業績

• 原著論文

1. 松本 亮介，小田 知央，笠原 義晃，嶋吉 隆夫，金子 晃介，栗林 健太郎，岡村 耕二，精緻に解析可能な恒常性のあるメール基盤の設計， 情報処理学会研究報告インターネットと運用技術(IOT)，2018-IOT-40, 17, 1-6, 2018.03.
2. 笠原 義晃，松本 亮介，近藤 宇智朗，小田 知央，嶋吉 隆夫，金子 晃介，岡村 耕二，軽量コンテナに基づく柔軟なホスティング・クラウド基盤の研究開発と大規模・高負荷テスト環境の構築，情報処理学会研究報告インターネットと運用技術(IOT)，2018-IOT-40, 2, 1-6, 2018.03.
3. Yoshiaki Kasahara, Takao Shimayoshi, Masahiro Obana, Naomi Fujimura, Our experience with introducing microsoft office 365 in Kyushu University, 45th ACM Annual SIGUCCS Conference, SIGUCCS 2017 - Proceedings of the 2017 ACM Annual Conference on SIGUCCS, 10.1145/3123458.3123491, Part F131713, 109-112, 2017.10.

• 学会発表

1. 笠原 義晃，松本 亮介，近藤 宇智朗，小田 知央，嶋吉 隆夫，金子 晃介，岡村 耕二，軽量コンテナに基づく柔軟なホスティング・クラウド基盤の研究開発と大規模・高負荷テスト環境の構築，情報処理学会 第40回 インターネットと運用技術研究会，2018.03.
2. Yoshiaki Kasahara, Takao Shimayoshi, Masahiro Obana, Naomi Fujimura, Our experience with introducing microsoft office 365 in Kyushu University, 45th ACM Annual SIGUCCS Conference, SIGUCCS 2017, 2017.10.

研究資金

• 共同研究、受託研究

1. 2017.10～2018.03, 代表, 軽量コンテナに基づく柔軟なホスティング・クラウド基盤の研究開発と大規模・高負荷テスト環境の構築

教育活動

• 担当授業科目

1. 2017年度・後期，情報処理概論．
2. 2017年度・春学期，サイバーセキュリティ基礎論．

社会貢献・国際連携等

• 一般市民、社会活動及び産業界等を対象とした活動

1. 2018.03, 一般市民向けサイバーセキュリティ懇話会「せきゅトーク 2018 in 福岡」で「スマートフォンのセキュリティ対策」講演, 九州大学 サイバーセキュリティセンター, JR 博多シティ会議室 会議室３

大学運営

• 学内運営に関わる各種委員・役職等

1. 2016.10～，ウエストゾーン安全衛生部会 委員
2. 2014.04～，情報基盤研究開発センター安全衛生部会 委員
3. 2013.04～，九州大学病院情報基盤専門委員会 委員
4. 2012.04～，生涯メール運営会議 構成員