SHIELD Security Research Center

Hisys Security Journal

VOL.55

HITACHI
Inspire the Next

日立システムズ

Hisys Security Journal VOL.55

TABLE OF CONTENTS

●はじめに

本文書は、株式会社日立システムズ サイバーセキュリティリサーチセンタが運営するセキュリティ情報サイト、S.S.R.C.(Shield Security Research Center) の公開資料です。本サイトでは、本文書のバックナンバーをはじめ、S.S.R.C. によるリサーチ結果などを随時公開しています。

S.S.R.C. https://www.shield.ne.jp/ssrc/

日立システムズとともに産学連携の
セキュリティ人財育成の
取り組みを続ける

布広永示
インタビュー

工学博士
東京情報大学 学長
学校法人 東京農業大学 理事

取材・文・撮影＝吉澤亨史
編集＝斉藤健一

写真提供：東京情報大学

この春、東京情報大学の学長に就任した布広永示氏は、17 年間の日立製作所勤務を経て、大学の教員へと転身。以来、日立システムズとの産学連携を 11 年にわたって継続しており、多くのセキュリティ人財を輩出している。IT や IoT のセキュリティ知識を備えた人財は、デジタル化が進むあらゆる業界で高い能力を発揮すると考えられる。今回は、布広氏に産学連携や人財育成、今後の取り組みなどについてお話を伺った。

11 年間にわたって
日立システムズとの連携で人財を輩出

吉澤（以下 Y）：まず、経歴についてお願いします。

布広（以下 N）：大学で博士課程を経て、1985 年に日立製作所に入社しました。以降、2002 年 3 月までの 17 年間、一貫してスーパーコンピューター関連の開発に携わってきました。そして、2002 年 4 月に東京情報大学に移り、主に言語処理や、人工知能を取り入れた学習支援システムの研究に取り組んできました。東京情報大学は、学校法人 東京農業大学が 1988 年に設立した大学です。2002 年当時は助教授でしたが、2007 年に教授となり、以降は情報サービスセンター長、大学院総合情報学研究科委員長、先端データ科学研究センター長、副学長などを経て、2023 年 5 月から東京情報大学の第 7 代目となる学長、また学校法人 東京農業大学の理事に就任しました。

Y アカデミアでのキャリアは一環して東京情報大学なのですね。

N 日立製作所勤務時代の縁から、2011 年に日立情報システムズ（現日立システムズ）と産学連携の話が持ち上がりました。企業が持っているノウハウを大学教育に活かし、そして学修した卒業生を企業へと送り出す取り組みです。

Y その産学連携がサイバーセキュリティに関わるきっかけになったのでしょうか。

N 2011 年当時、わが国のセキュリティ人財不足がさまざまなところで指摘されており、内閣府が人財育成強化のために産学連携を推進していました。当時、防衛関連企業へのサイバー攻撃が発覚し、大々的に報じられたり、2020 年の東京オリンピック誘致を目指している時期でもあったりしたことから、サイバーセキュリティが社会全体の課題になっていました。

Y 2011 年が政府のサイバーセキュリティに対する取り組みの転換点だと言うセキュリティ業界関係者は多いですね。

N サイバー攻撃に対する技術的な対策の不足だけでなく、サイバー攻撃を受けた後に何をすれば良いのかを適切に判断できる情報セキュリティ人財の不足も明らかになりました。一方で、大学におけるセキュリティ教育はセキュリティ技術の理論が中心で、セキュリティ技術者に必要な実践的な教育内容が不足していたのです。これでは産学連携の目的である、企業に必要な人財を即戦力として送り出すことが難しくなってしまいます。そこで、持ち上がったのが、日立システムズとの産学連携の話です。2013 年に東京情報大学で第 1 回目のサイバーセキュリティ人財育成のための授業が開始されました。今年で 11 年目となります。

Y 11 年も継続されているのは素晴らしいです。

N サイバーセキュリティの人財育成には、セキュリティ技術の理論だけでなく、実際に企業の現場で起きている問題を活用した実践的な技術を学ぶ必要があります。そこで日立システムズと連携し、講師の派遣、研究課題の提示、研究のサポート、研究成果の実証、そして、セキュリティ関係の評価基準などをしていただいています。東京情報大学からは、設備が整っていることから教育環境の提供や活用の機会を設けているほか、研究活動の推進、そして質の高い人財を送り出すことに努めています。これらの活動で使う教材は日立システムズと共同で開発していて、研究成果も共有しています。

セキュリティ人財育成における 3 つの課題

Y 現在の日本のサイバーセキュリティ人財の状況と課題について教えてください。

N IPA（独立行政法人 情報処理推進機構）から「情報セキュリティ白書 2023」が公開されています。それによると日本における 2022 年のサイバーセキュリティ関連従事者は約 38.8 万人と推定されるが、まだ 5.6 万人不足しているとあります。

Y 常に不足している状況が続いていますね。

N 増えてはいるのですけどね。サイバーセキュリティ人財育成の課題については、大きく 3 つあると考えています。1 点目は、サイバーセキュリティの技術者に求められる知識が広範囲になっていることです。IoT はあらゆる業界で採用されていますし、DX の推進によってデジタル化が進み、多くの企業がテック企業へと変わっています。それらの技術をすべて習得しながらサイバーセキュリティを実施していくことは非常に困難だと思います。2 点目は、セキュリティ技術者の評価が十分ではないということです。企業はセキュリティ技術者の重要性を強く認識しているのですが、ビジネスとして考えたときに、収益面での存在感や価値観に対して、経営層がもっと真剣にセキュリティに取り組むべきだと思います。特に、サイバーセキュリティの運用への対価が少ない印象があります。

布広永示（ぬのひろ・えいじ）
1985 年日本大学大学院生産工学研究科博士後期課程単位取得満期退学（数理工学専攻）。株式会社日立製作所勤務。1987 年工学博士（日本大学）。2002 年東京情報大学助教授。2007 年同大学教授。2023 年同大学学長、および学校法人 東京農業大学理事に就任。

Y 確かに、経営から見るとセキュリティは利益を生み出しませんから、コストとして捉えられ、重視されないことも多いと聞きます。

N 3 点目は、セキュリティエンジニアの仕事に対して学生が明確な目標を持ちにくいという点にあります。学生に聞くと、情報分野では成果を競うことがよくあります。例えば、コンピューターであれば、性能や操作性をいかに上げていくかという競争があるわけです。その効果は実際に目に見えますし、体感もできます。また、運用面におい

てもいかに業務効率を上げるかという競争があります。しかし、サイバーセキュリティはそういう感覚を持つことが難しいのです。

Y そうした日本のサイバーセキュリティ人財の課題に対して、東京情報大学では特にインシデント対応ができる人財にフォーカスしています。取り組んでいること、工夫していることはありますか。

N 日立システムズとの連携が始まった 2011 年当時は、セキュリティはネットワーク分野の一部でした。そのため、学生がセキュリティ人財に興味を持ってもらうところから始める必要がありました。そこで、サイバーセキュリティ人財育成の認知度向上のために 3 つのポイントを挙げて啓発活動を行いました。まず「動機付け」です。サイバーセキュリティ人財の不足が深刻化している状況であるため、キャリアパスが充実しており、就職しやすいこと。次に「充実感」。セキュリティ人財は国家的に推進されている事業であるため、やりがいがあること。そして「学習意欲」。サイバーセキュリティ技術を習得することで、幅広い情報技術に関する知識が身につくことです。

Y 講座には、具体的にどのような内容が盛り込まれているのでしょうか。

N データ解析、AI、システム開発などが挙げられます。こうした内容をサイバーセキュリティの人財育成の枠組みの中で学習することで、達成感が得られるようになりますし、就職にも役立ちます。これを 2013 年から続けていることで、学生が興味を持って講座に参加してくれるようになったと思っています。また、単位認定講座として「IT システムセキュリティ・インシデントレスポンス概論」を設けました。CSIRT の役割とセキュリティインシデント発生時の対応フローおよび事前準備、デジタルフォレンジックの基礎とマルウェア解析入門で構成されています。

産学連携を最大限に活かした単位認定講座

Y 講座は日立システムズの現役セキュリティエンジニアが講義を担当しているのですよね。

N はい。実際に日立システムズで調査対応を行ったインシデント事例や、日々収集しているサイバーセキュリティの新たな情報を反映し、毎年ブラッシュアップしているので、学生にとっては新鮮な内容だと思います。受講した学生の反応も良く、「実際に挙動を見ながら解析を行うことができた」などの声があります。現役のセキュリティエンジニアによる講義は、学生によい緊張感をもたらしてくれます。さまざまな講師と触れ、セキュリティは需要があるし、関心が高いということを肌で感じてくれたと思います。また、単に単位認定講座を立ち上げるだけでなく、「インシデントレスポンス概論」といった公開セミナーも開催しました。こうした取り組みには、地域の方々をはじめ、防衛関係者や法執行機関の方々にも参加していただきました。

Y 学生に対して何かフォローしていることなどありますか。

N 講義を受けて身についた能力、成果を実感してもらうために、「MWS Cup」に参加させています。MWS Cup は CSS（情報処理学会主催のコンピュータ・セキュリティ・シンポジウム）内の企画として開催されるセキュリティコンテストで、日立システムズと東京大学や明治大学、静岡大学などの学生連合などが参加しており、優勝すると SECCON（日本ネットワークセキュリティ協会内の有志によるセキュリティコンテスト）への出場権が得られます。2014 年と 2015 年は東京情報大学の学生がメンバーとして加わったチームが優勝し SECCON に出場しています。

Y 実績も残されているわけですね。これまで輩出

した人数はどのくらいですか？

N PC の台数や環境の問題で、講座は 40 名に抑えています。開始した当時は 350 名を目標にしていましたが、それからの 11 年で約 400 名が単位認定を受けています。当初の目標は達成しましたが、さらに継続していきたいと考えています。

Y 最近、高度セキュリティ教育を受けた人財がサイバー攻撃をして逮捕された事件が注目されましたが、セキュリティ教育は技術と共にリテラシーやモラルも併せて高めていく必要があると考えます。東京情報大学ではリテラシーやモラルについて、どのような方針を持たれていますか。

N 東京情報大学では、情報モラルに関する講習を学部に関係なく全学を対象に実施しています。学生はみな学内ネットワークを使うわけですから、正しい使い方を学ばなくてはなりません。この講習を受けてレポートを提出しないと、学内ネットワークのアカウントが発行されません。これまでに数人、アカウントが停止されています。単位認定講座においては、講義の最初に合意書を熟読させて署名をしてもらいます。講義で扱うセキュリティ関係の情報や習得する技術は、実際に使ってしまうと社会に大きな影響を及ぼす危険性が高いためです。合意書には、技術を悪用した場合に受ける法的措置についても明記されています。

これからのセキュリティ人財に必要になるものを見極めていく

Y 2023 年 4 月、東京情報大学は総合情報学部を「情報システム学系」「データサイエンス学系」「情報メディア学系」の 3 学系 9 研究室の新体制としました。これを含めて、今後の展望について教えてください。

N 情報システム学系はゲーム・IoT 研究室、AI・システムデザイン研究室、ネットワーク・セキュリティ研究室の 3 つ、データサイエンス学系は心理学研究室、データサイエンス基盤研究室、生命・環境科学研究室の 3 つ、情報メディア学系は経営情報研究室、メディアデザイン研究室、メディア文化研究室の 3 つとなります。ただ、セキュリティを実践的に学ぶ上で、どのような科目が必要になるのかは、柔軟に対応していくつもりです。また、学ぶべき技術をセットにして計画的に学生の理解を促すようにしています。今後は、こうしたセットを達成目標に応じてグルーピングしていくことも重要だと考えています。

Y 具体的にはどのようなイメージでしょうか。

N サイバーセキュリティの人財育成に必要な教育内容を広範囲に考えて、フォレンジックの講座に横断的な技術教育の要素を加え、知っておくべき関連技術を拡大するということです。例えば、ディープラーニングでは、セキュリティの挙動、兆候などを評価するために、AI を活用する研究が増えています。また、情報システムのセキュリティ対応においても、ソフトウェアやネットワークの構成や DX 化などについて理解しておく必要があります。そうした関連技術の知識をセットにしてサイバーセキュリティの教育プログラムを考えていくことが必要だと思います。

Y より実践的なカリキュラムになりそうです。その反面、基準がないので難しいとも言えますね。

N はい。産学連携の中で企業側から「こういう技術レベルのエンジニアが必要なので、こういう内容の教育をしてほしい」などの提案していただきながら教育内容や達成度の検討を進めていくことが良いと考えます。

Y サイバーセキュリティ人財の育成や確保に苦労している組織に対して、どのように取り組めばいいのか、アドバイスをお願いします。

N 最近では、リスキリングやリカレント教育に大学を活用するケースが増えている印象があります。最近の例でいえば、日立システムズの関連企業に就職した東京情報大の卒業生が企業人のまま本学の博士課程に在籍しています。こうした形でセキュリティ人財を育成する方法もあると思います。業務に支障がない範囲でエンジニアが博士の学位を取得するといったことも良いことだと考えます。

Y セキュリティ人財をどんどん輩出されることを期待しています、今回はありがとうございました。

社会のさまざまな動向を把握し、リスクの変化に対応したセキュリティ体制を構築

HISYS CSI（Cyber Security Intelligence）Watch 2023.11

文＝SHIELD Security Research Center

OSINT の悪用について

【概要】公開情報を収集し、情報分析を行うOSINT（Open source Intelligence）の活用がさまざまな観点で重要視されており、ビジネスの世界で今後も拡大していくと考えられる。その一方でOSINT を有効活用するために利用者として注意すべき点があり、本号では攻撃者による OSINT の悪用とその対策について述べる。

【内容】OSINT は、公開情報から取集した情報を分析し、意思決定の判断材料を生み出す活動である。OSINT の種類には取引先の信用調査や財務状況調査、競合他社の動向調査、脅威調査などがあり、ビジネスを有利に進めるための重要な手法として注目されている。一方で、攻撃者によってOSINT が悪用される場合もある。OSINT は今後のビジネス展開に大きな影響を与えるため、そのような場合には正規の OSINT の利用者がビジネス上の損失を被るリスクもある。

攻撃者による OSINT の悪用例を示す。一例目は、攻撃目標とする「組織」および「組織のステークホルダー（取引先・業界団体・管轄官庁関係者）」に関する情報を、公開 Web や SNS などから収集し、その情報を駆使して海外企業の取引先関係者を装い「組織」に接触し、自らを正当な取引担当者であるかのように誤信させた上で、取引代金決済用の銀行口座証明書類を偽造して振込先口座の不正変更に成功した事例である（図 1）。

二例目は、公的なセキュリティ情報機関や IT 企業やソフトウェアベンダーから発表されたセキュリティ脆弱性情報をもとに影響度や特徴を把握したうえで、「SHODAN」や「Censys」といった IoT 機器検索ツールなどを用いてサイバー攻撃が成功しやすい対象を特定し、さまざまな攻撃を試みて侵入を成功させた事例である（図 2）。

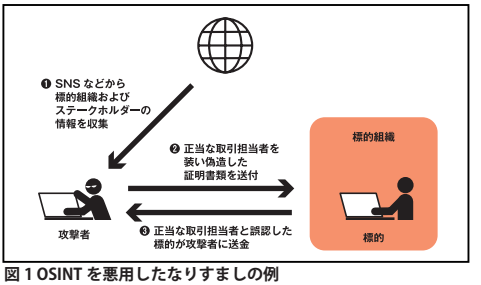


図 1 OSINT を悪用したなりすましの例

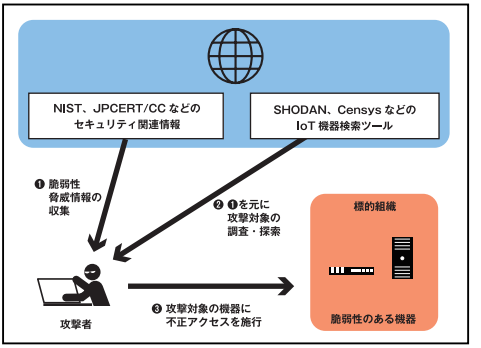


図 2 OSINT を悪用した不正アクセスの例

その他、攻撃者が OSINT の情報源そのものを改ざんしたり、正規の情報源であるかのように装った虚偽の情報源になりすましマルウェアを仕込むなど OSINT の活用者を混乱させるといった事例も考えられ、悪意の攻撃者にとっても OSINT の活用は極めて有効な手段のひとつとなっている。

このように、OSINT が攻撃者にも活用されている可能性があることを踏まえ、サイバー攻撃から自組織を防衛する手段のひとつとして OSINT を活用するには注意が必要である。

【情報源】https://blog.kaspersky.co.jp/osint-open-source-intelligence/34626/
https://www.hitachi-systems.com/solution/s003/johoteikyou/

セキュリティツールを実践的に紹介する連載企画

Let's Try Windows システム確認！

3. ネットワーク状況確認編

文＝ SHIELD Security Research Center

1. はじめに

本稿は、各種セキュリティツールを実践的に紹介する連載企画です。前々号（Vol.53）より第二部「Windows システム確認」と題し、Microsoft 社が提供する「Sysinternals Suite」として利用可能な、いくつかのツールの使い方を紹介しています。

「Sysinternals Suite」は、多数のトラブルシューティング ユーティリティをまとめたバンドルです。誰でも無償で利用することができ、Windows マルウェアの動的解析などにも利用可能なツールです。

「Sysinternals Suite」を有効活用することで、コンピューターに感染した Windows マルウェアを見つけ出したり、Windows マルウェアの挙動を確認したりすることができます。

一方、「Sysinternals Suite」が動作するコンピューターでは、活動を停止する Windows マルウェアも存在します。

「第二部　Windows システム確認」は次の 3 部構成となっています。

1. 自動起動プログラム確認編
   Autoruns を利用して、Windows の自動起動プログラム設定を確認します。

2. プロセス確認編
   Process Monitor を利用して、Windows 上で起動するプロセスの動きを確認します。

3. ネットワーク状況確認編
   TCPView を利用して、Windows 上でのネットワーク状況を確認します。

今回は、「3. ネットワーク状況確認編」として、Windows 上でのネットワーク状況の確認方法を解説します。マルウェアの挙動確認、マルウェアの感染確認（ロードされる DLL として）などに利用可能となります。

なお、本稿の安全性には留意していますが、安全を保証するものではございません。

OA 端末（社内ネットワーク接続機器）で実施するのではなく、分離された回線内および機器を利用することを推奨いたします。

2. 準　備

2.1 TCPView の準備

「TCPView」とは、「Sysinternals Suite」に含まれる、Windows でネットワーク状況を確認するためのツールです。OS 標準で利用可能な「netstat」と比べて高機能となっています。「TCPView」および「Sysinternals Suite」は下記などから、ダウンロードすることができます。

・「TCPView」
https://learn.microsoft.com/ja-jp/sysinternals/downloads/tcpview
・「Sysinternals Suite」
https://learn.microsoft.com/ja-jp/sysinternals/downloads/sysinternals-suite

今回は、「TCPView」の v4.19 をダウンロードしました。ダウンロードした zip ファイルを、アクセス可能なフォルダーにて展開します。フォルダー構成は、以下の通りとなっています

名前	更新日時	種類	サイズ
Eula.txt	2023/10/04 14:38	テキスト ドキュメント	8 KB
tcpvcon.exe	2023/10/04 14:38	アプリケーション	198 KB
tcpvcon64.exe	2023/10/04 14:38	アプリケーション	245 KB
tcpvcon64a.exe	2023/10/04 14:38	アプリケーション	232 KB
tcpview.chm	2023/10/04 14:38	コンパイルされた HT...	16 KB
tcpview.exe	2023/10/04 14:38	アプリケーション	923 KB
tcpview64.exe	2023/10/04 14:38	アプリケーション	1,062 KB
tcpview64a.exe	2023/10/04 14:38	アプリケーション	1,020 KB

今回は、筆者は tcpview64.exe を利用します。皆様は、利用されている環境に合わせて、選択をしてください。

2.2 Putty の準備

「Putty（パティ）」は、Simon Tatham が MIT License（オープンソースソフトウェアライセンスの一種）で開発・公開しているリモートログオンクライアントです。後ほど、「Putty」を使った確認手順がありますので、準備をしておきます。ソフトウェアは以下の URL よりダウンロードできます。

・「Putty」
https://putty.org/

筆者は下記、64-bit x86 binary file をダウンロードしました。ご自身の環境に合わせてダウンロード、ご準備してください。

Alternative binary files

The installer packages above will provide versions of all of these (except PuTTYtel an

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

putty.exe (the SSH and Telnet client itself)

64-bit x86:　putty.exe　(signature)

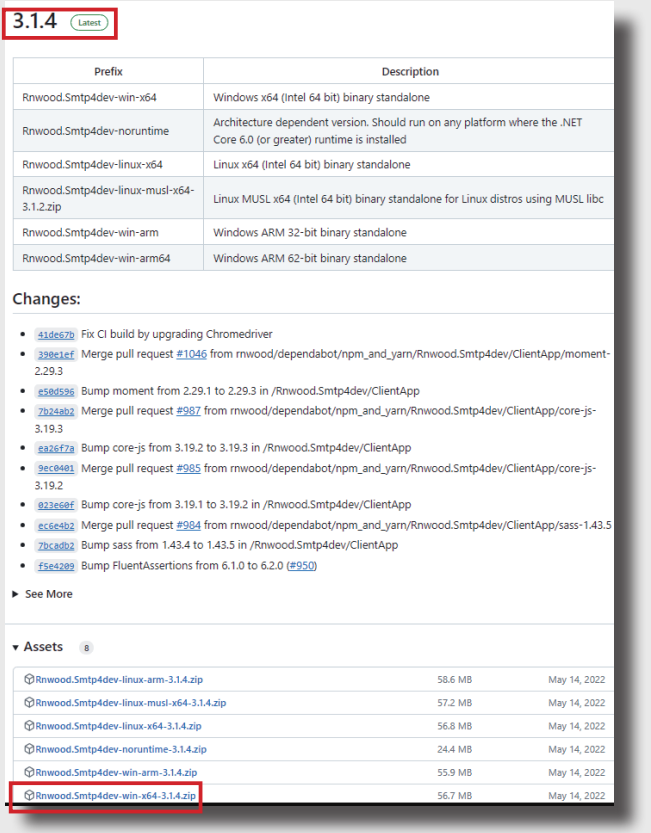
2.3 Smtp4dev の準備

Smtp4dev は、ダミーの SMTP サーバを立てるアプリケーションです。BSD-3-Clause license で配布されています。Smtp4dev は、以下からダウンロードできます。

・「Smtp4dev」
https://github.com/rnwood/smtp4dev/releases

ダウンローページのいちばん上に表示されているものは、本誌執筆時点 (2023 年 10 月) では、「Pre-release」でしたので利用には注意してください。

筆者は、本誌執筆時点 (2023 年 10 月) の最新リリース版 (Latest) である、v3.1.4 をダウンロードしました。ファイル名は「Rnwood.Smtp4dev-win-x64-3.1.4.zip」です。



3.1.4 Latest

Prefix	Description
Rnwood.Smtp4dev-win-x64	Windows x64 (Intel 64 bit) binary standalone
Rnwood.Smtp4dev-noruntime	Architecture dependent version. Should run on any platform where the .NET Core 6.0 (or greater) runtime is installed
Rnwood.Smtp4dev-linux-x64	Linux x64 (Intel 64 bit) binary standalone
Rnwood.Smtp4dev-linux-musl-x64-3.1.2.zip	Linux MUSL x64 (Intel 64 bit) binary standalone for Linux distros using MUSL libc
Rnwood.Smtp4dev-win-arm	Windows ARM 32-bit binary standalone
Rnwood.Smtp4dev-win-arm64	Windows ARM 62-bit binary standalone

Changes:

- 41de67b Fix CI build by upgrading Chromedriver
- 390e1ef Merge pull request #1046 from rnwood/dependabot/npm_and_yarn/Rnwood.Smtp4dev/ClientApp/moment-2.29.3
- e50d596 Bump moment from 2.29.1 to 2.29.3 in /Rnwood.Smtp4dev/ClientApp
- 7b24ab2 Merge pull request #987 from rnwood/dependabot/npm_and_yarn/Rnwood.Smtp4dev/ClientApp/core-js-3.19.3
- ea26f7a Bump core-js from 3.19.2 to 3.19.3 in /Rnwood.Smtp4dev/ClientApp
- 9ec0401 Merge pull request #985 from rnwood/dependabot/npm_and_yarn/Rnwood.Smtp4dev/ClientApp/core-js-3.19.2
- 023e60f Bump core-js from 3.19.1 to 3.19.2 in /Rnwood.Smtp4dev/ClientApp
- ec6e4b2 Merge pull request #984 from rnwood/dependabot/npm_and_yarn/Rnwood.Smtp4dev/ClientApp/sass-1.43.5
- 7bcadb2 Bump sass from 1.43.4 to 1.43.5 in /Rnwood.Smtp4dev/ClientApp
- f5e4209 Bump FluentAssertions from 6.1.0 to 6.2.0 (#950)

▸ See More

▾ Assets 8

Rnwood.Smtp4dev-linux-arm-3.1.4.zip	58.6 MB	May 14, 2022
Rnwood.Smtp4dev-linux-musl-x64-3.1.4.zip	57.2 MB	May 14, 2022
Rnwood.Smtp4dev-linux-x64-3.1.4.zip	56.8 MB	May 14, 2022
Rnwood.Smtp4dev-noruntime-3.1.4.zip	24.4 MB	May 14, 2022
Rnwood.Smtp4dev-win-arm-3.1.4.zip	55.9 MB	May 14, 2022
Rnwood.Smtp4dev-win-x64-3.1.4.zip	56.7 MB	May 14, 2022

ダウンロードが完了しましたら、ファイルを展開します。

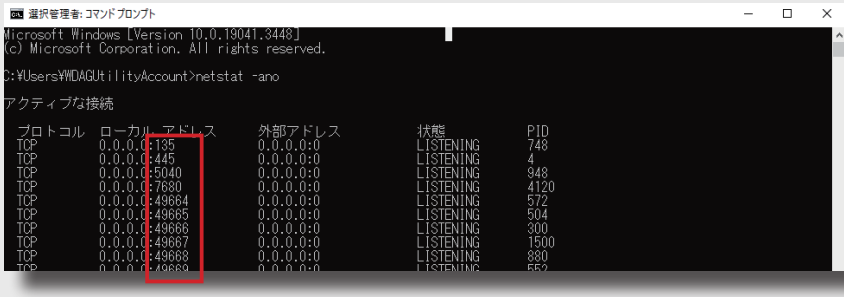
3. ネットワーク状況の確認

3.1 初期状態の確認

初期状態のネットワーク状況を確認します。
Cortana に「cmd.exe」を入力し、コマンドプロンプトを起動します。
コマンドプロンプトが立ち上がりましたら、以下のコマンドを入力します。

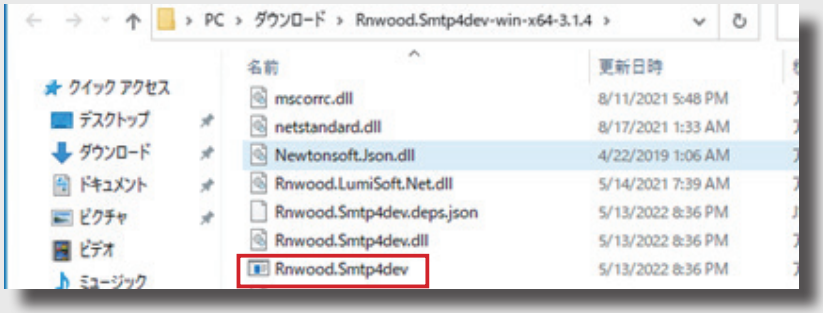
```
netstat -ano
```

実行結果を以下に示します。ポート 25 番でリッスンしているプログラムがないことを確認してください。

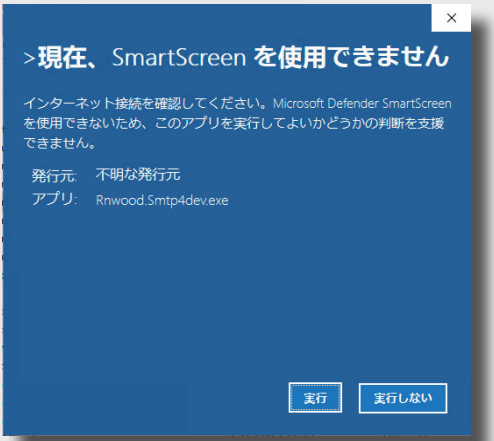


3.2 ポートリッスン状態の確認

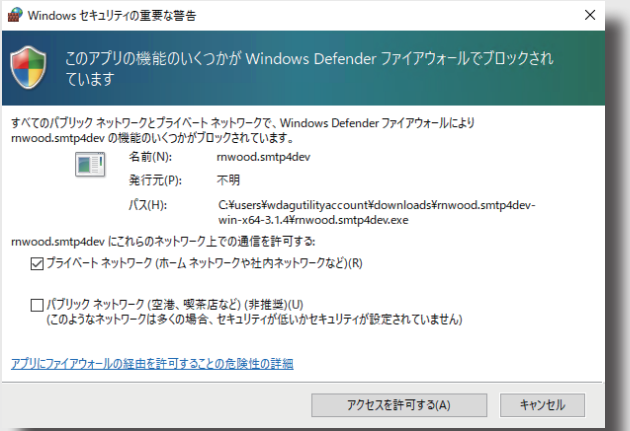
Smtp4dev フォルダ内には、実行に必要な沢山のランタイムファイルなどが含まれますが、Smtp4dev を実行する際は「RnwoodSmtp4dev（.exe）」の実行ファイルを利用します。



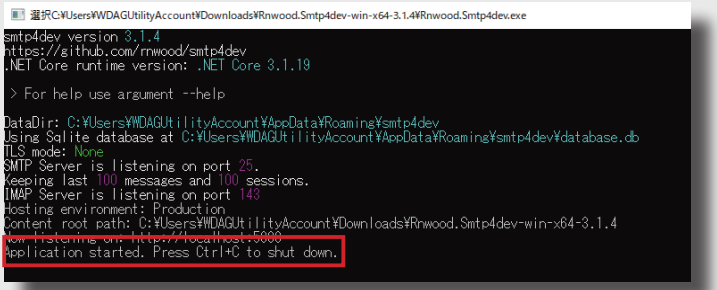
Smtp4dev を実行すると、Windows sandbox 等ご利用の環境によっては、次頁の図のように警告が出る場合があります。ここでは、「実行」を押下してください。



また、初回は以下の警告が出てきます。初期状態で「パブリックネットワーク」にチェックが入っていることもありますが、むやみにアクセスを許可しないようにしましょう。ここでは、プライベートネットワークを選択します。



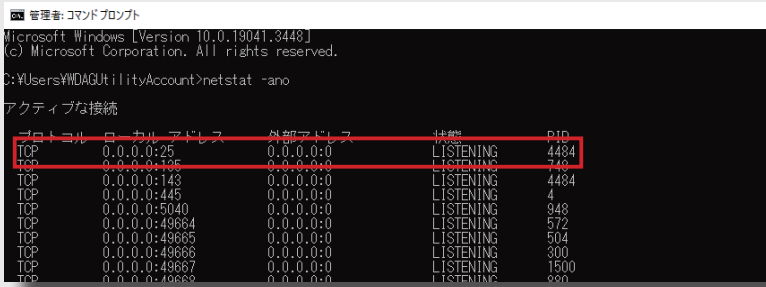
最終的に下の図のように表示されましたら起動は完了です。



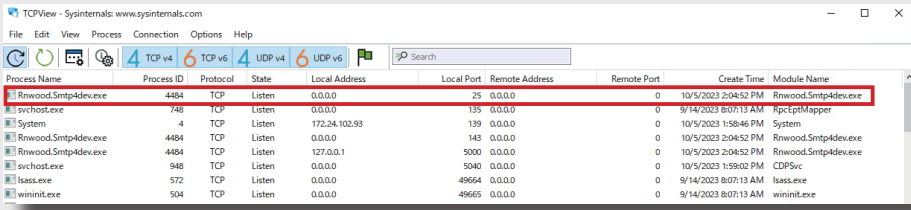
次に、前述の手順と同様、netstat コマンドを実行します。

```
netstat -ano
```

実行結果を以下に示します。ポート 25 番でリッスンしているプログラムが存在していることを確認してください。この PID4484 で立ち上がっているサービスが Smtp4dev です。



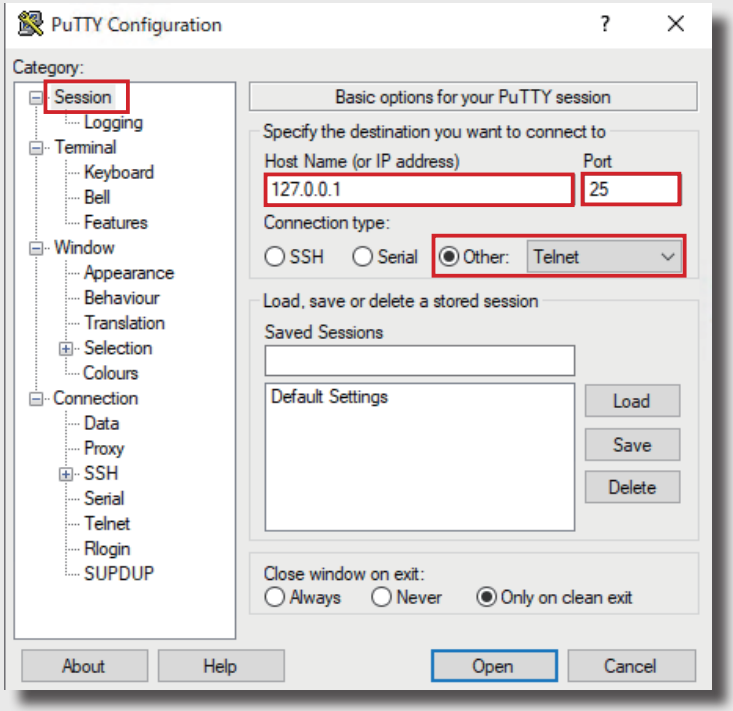
同様に、「TCPView」で確認します。
「TCPView」の起動結果は下の図の通りです。



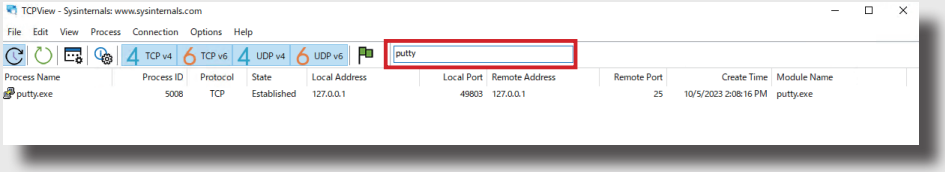
netstat コマンドでの実行結果に加えて、PID 4484 で起動しているプロセス名およびプロセスが起動した時刻を確認することができます。
これで、ダミーの SMTP サーバーである Smtp4dev が起動していることを確認できました。

3.3 サービス接続状態の確認

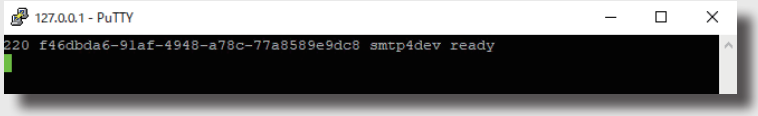
Smtp4dev が起動しましたので、SMTP 接続を行います。
「Putty」を起動し、次頁の図の通り、Session タブの Host Name に「127.0.0.1」、Port に「25」を入力し、Connection Type を Other で「Telnet」を選択し、Open ボタンを押下します。



この状況で、「TCPView」を確認してみます。検索窓に「putty」を入力し、検索します。
その結果、プロセス「putty」が送信元ポート「49803」から送信先ポート「25」に接続している状況が確認できます。



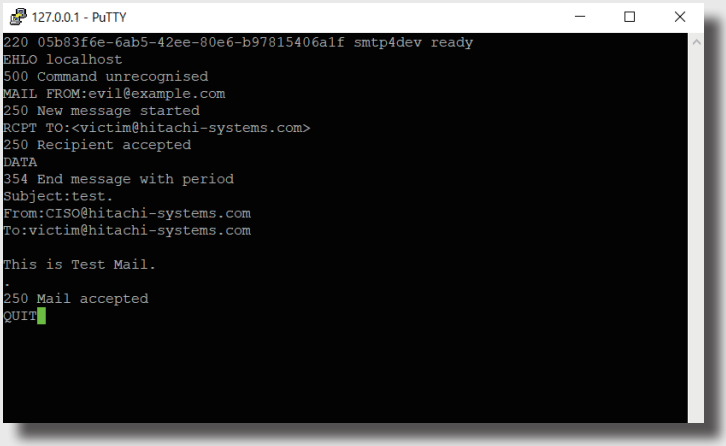
「Putty」で SMTP サーバーへ接続を行うと、下の図のような画面が表示されます。
なお、前述の「TCPView」を確認している間に、セッションが切れている場合には再度、「Putty」で接続をしてください。



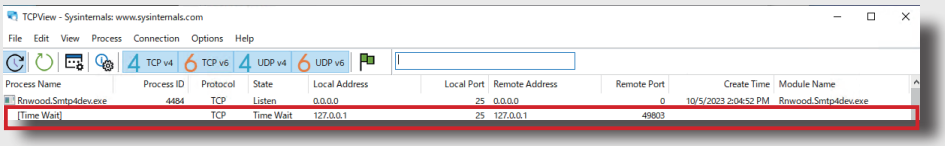
Putty 画面が表示されたら、（最初に ENTER を押下したのち）、以下の内容を入力（番号については後述）して、SMTP サーバーに送信し、メールを送信します（実際には送信されません）。

```
EHLO localhost                                  ❶
MAIL FROM:evil@example.com                      ❷
RCPT TO:<victim@hitachi-systems.com>            ❸
DATA                                            ❹
Subject:test.                                   ❺
From:CISO@hitachi-systems.com                   ❻
To:victim@hitachi-systems.com                   ❼

This is Test Mail.                              ❽
.                                               ❾

QUIT                                            ❿
```

SMTP サーバーへの送信が終わると、コマンドプロンプトが終了（または、1 回の Enter で終了）します。

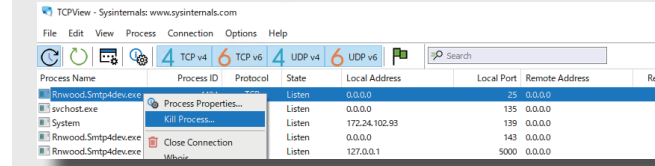


「TCPView」で確認すると、送信元ポート「49803」から送信先ポート「25」への接続、つまりメールサーバーへの接続は終了しており、ステータスが「Time Wait」になっていることが確認できます。

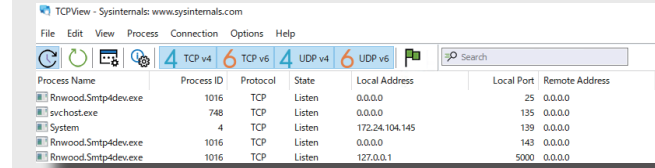


3.4 プロセスを Kill（強制終了）する

ここまで確認してきたように、「TCPView」は、GUI（Graphical User Interface）で利用な可能な netstat と表現しても遜色はないものです。一方、「TCPView」は、ネットワーク状況、プロセスを確認しながら、プロセスを Kill できる点では便利です。
今回立ち上げた、Smtp4dev プロセスを「TCPView」より、Kill します。
Kill したい Smtp4dev プロセス (PID 4484) を右クリックし、「Kill Process」を選択します。

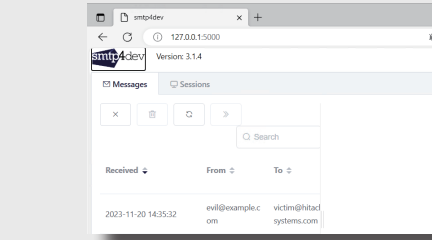


警告が表示されたら内容を確認し、「OK」ボタンを押下します。
これで、Smtp4dev を Kill できました。「TCPView」上で、Kill した Smtp4dev プロセス（PID 4484）が終了していることを確認します。

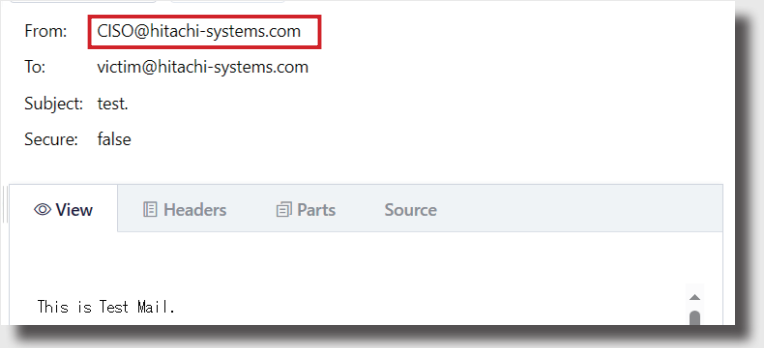


3.5［参考］メールアドレスの偽装

Smtp4dev は、ダミーメールサーバですので、実際にはメールの送信は行いませんが、Web インタフェース上で送信したメールの内容を確認できますので、念のため、実際のメールの内容も確認します。
Smtp4dev が起動した状態でブラウザを起動して、以下のアドレスにアクセスしてください。
http://127.0.0.1:5000/
Smtp4dev のメール管理画面上で送信したメール一覧を確認することができます。



こちらは実際のメーラーで見える画面です。



From に表示されているメールアドレスは、実際の送信元と異なるメールアドレス（コマンド❷のアドレスでなく、コマンド❻のアドレス）が表示されていることが確認できます。サイバー犯罪者はこのように、送信元アドレスを偽装する場合があります。

4. おわりに

今回は、「3. ネットワーク状況確認編」として、「Sysinternals Suite」に含まれる「TCPView」を用いた、Windows ネットワーク状況を確認しました。
マルウェアによる不審な通信が発生していないか、攻撃者などによる不審な接続がないか、などネットワーク状況を確認する際に利用します。

次回からは第三部「IoT 検索エンジンを用いたサーバ確認手法」となります。Shodan、Censys などを用いて外部公開しているサーバーなどがどのように見えているかついて解説します。