SHIELD Security Research Center

Hisys Security Journal

VOL.53

HITACHI
Inspire the Next

日立システムズ

Hisys Security Journal VOL.53

TABLE OF CONTENTS

マツダが取り組むサプライチェーン・セキュリティの強化 …… 3
部品サプライヤー約 20 社のセキュリティ担当者と対話した松本 正宏氏

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 2023.09 …… 9

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！ 1. 自動起動プログラム確認編 …… 11

●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/

●ご利用条件

本文書内の文章等すべての情報掲載に当たりまして、株式会社日立システムズ（以下、「当社」といいます。）と致しましても細心の注意を払っておりますが、その内容に誤りや欠陥があった場合にも、いかなる保証もするものではありません。本文書をご利用いただいたことにより生じた損害につきましても、当社は一切責任を負いかねます。
本文書に記載した会社名・製品名は各社の商標または登録商標です。
本文書に掲載されている情報は、掲載した時点のものです。掲載した時点以降に変更される場合もありますので、あらかじめご了承ください。
本文書の一部または全部を著作権法が定める範囲を超えて複製・転載することを禁じます。

© Hitachi Systems, Ltd. 2023. All rights reserved.

Human * IT

マツダが取り組む サプライチェーン・セキュリティの強化

部品サプライヤー約 20 社のセキュリティ担当者と対話した松本 正宏氏

聞き手＝丹京 真一（日立システムズ）
構成・原稿・撮影＝斉藤 健一

近年、ランサムウェアを用いたサイバー攻撃の被害が多く報じられている。その大部分がサプライチェーン企業のセキュリティ対策の不備を突いたものだと言われてる。企業にとって、サプライチェーンのセキュリティ強化は喫緊の課題だ。

このような状況の中、自動車メーカーのマツダでは、セキュリティ担当者が部品サプライヤー各社を訪れ、現場の技術者と対面でヒアリング調査などを行ったという。今回は、この取り組みの責任者である松本 正宏氏（写真右）に話を伺った。聞き手は弊社の丹京 真一（写真左）。ヒアリング調査で集めた現場の声は自動車業界だけに限らず、幅広い業界で参考になるはずだ。

また、対談を通じて国際社会や自動車業界が一丸となって進めている自動車のセキュリティの取り組みの一端を垣間見ることができるだろう。

開発の期間短縮から品質向上、さらに「価値創造」までを担う MDI

丹京（以下 T）：松本さんとは普段から「協働の会」※1 などでご一緒させていただいており、毎回興味深い話を伺っています。特に、MDI（MAZDA DIGITAL INNOVATION）や、サプライチェーン・セキュリティの取り組みなどは、ぜひとも本誌読者にもお伝えしたいと考えています。そこで私が聞き手となり、自動車業界の事例を IT 業界に活かすことができないか、そのような視点も交えながら話を進めて行きたいと思います。よろしくお願いします。

松本（以下 M）：わかりました。よろしくお願いします。それではスライドを使って話を進めます。マツダでは、合理化を目指して生産領域にコンピューターをいち早く導入していましたが、1996 年に商品企画から生産まで、ものづくり領域全体を通して、三次元 CAD データをフル活用する取り組みを開始しました。理論上、コンピューターの中で自動車を組み上げることができれば効率的なはずです。当時コンピューターの処理能力も向上してきたので、機は熟したと判断し、導入に踏み切ることとしました。

T 社内での反響はいかがでしたか。

M 当時は、バブルがはじけた危機の中で生き残りをかけた開発期間短縮プロジェクトとして全社横断的に取り組みました。その結果、データの一元管理、各工程のコンカレント（同時並行）化などのメリットを活かすことができ、デザイン決定から量産開始までの期間を、取組み前の 27 ヵ月から約半分の 15 ヵ月まで短縮することができたのです（次頁 図 1）。ここでキーとなるのが「デジタルモックアップ」でした。

T コンピューター上で自動車を組み上げるにはすべ

丹京 真一（たんきょう・しんいち：写真左）
株式会社 日立システムズ セキュリティリスクマネジメント本部 主管技師長
国内外のグループ会社も含め、全社のセキュリティを統括し、統制、技術、セキュリティインシデント発生の対応、人材育成全般に関わる。2022 年広島県警サイバー犯罪対策テクニカルアドバイザーに就任。APWG(Anti Phishing Working Group) の Steering Committee Member。

松本 正宏（まつもと・まさひろ：写真右）
マツダ株式会社 MDI 業務設計部主査
1991 年入社。CAD/CAM の社内開発に携わる。その後、フォードグループ内の CAD/CAM ツール開発のため米国勤務を経験。マツダ・メキシコ工場の設立にも携わる。2015 年の帰国後は IT インフラ担当となり、セキュリティとの関わりを深めるようになる。現在は IT に限らず、全社の情報セキュリティを担当。R&D・生産・サービス領域と IT 領域との間のセキュリティプロセスの作成や、CSIRT でインシデント対応などを行い、経営に報告を行っている。

※1 **協働の会**：JNSA、IPA、JPCERT/CC、JASA 連携による情報交換会。国内外のサイバーセキュリティ問題に関して、業界・分野を越えた交流の場を提供している。運営は JNSA 脅威を持続的に研究する WG。

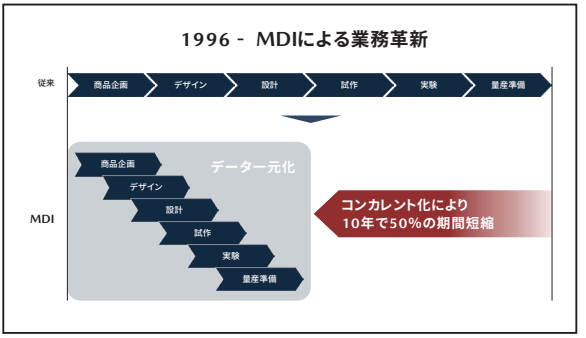


図 1 MDI による製品開発の期間短縮

てのパーツをデジタル化する必要があると思いますが、実際にはどれくらいの点数なのでしょうか。

M 約 3 万点になります。当然、マツダだけでは実現できません。部品サプライヤーにもご協力いただいてはじめて可能となりました。引き続き 2010 年には MDI は「価値創造」のフェーズへと移行します。デジタルを活用したマツダらしいクルマ作りを行うもので、その事例の 1 つが、デザインテーマ「魂動（こどう）」※2 の実現です。デザイン画やデジタルモデルから実車へと作り上げる工程をデジタル化したのです。具体的には、効率を重視しながらも、魂動デザインの実現を目指し、金型切削の CAM データと、デジタルモデルの一致性を、各段に向上させ、「匠の技の量産化」を実現しました。

T マツダの自動車はヨーロッパ車のようなデザインの一貫性がありますが、これも「魂動」の一環なのですね。

M はい。また、衝突試験をコンピューター上で再現しました。衝突試験というのは、試作車を作って壊すわけですから、そのコストは大きなものとなります。MDI に取り組む前までは、何度か試験を行わなくてはなりませんでしたが、衝突時に、乗員が受けるダメージのメカニズムの解明と、モデル化により、衝突実験をコンピューター上で、CAE により再現できるようになりました。いまでは、すべての衝突形態を 3 週間以内でシミュレーションできるまでになっています。

T お話を伺っただけで大幅なコストダウンが予想できます。

M 次がエンジンです。内燃機関の燃料噴射や、化学反応による燃焼特性をモデル化し、コンピューター上で検証しながら、走りと燃費、排ガスの相反を、高い次元で両立させました。これにより、走行性能も環境性能の高いエンジン（SKYACTIV）を提供できるようになったのです。

T 開発の期間短縮だけでなく品質向上にもデジタル化が役立っているのですね。

M 現在、MDI の取り組みは、より広く・より横断的に展開しています。モデルベースの考え方を用い、ロボットや治具を動かす設備信号など、全てをバーチャル空間で統合し、プロセス全体を可視化しました。いわゆる「デジタルツイン」です。最近では、販売プロセスの管理も可視化しています。一見すると簡単そうに見えるのですが、なかなか大変でした。物流倉庫・工場・販売店などそれぞれの在庫は、これまですべて縦割りで管理されていました。これを一元的に管理して可視化したのです。取り組みの背景にはコロナ禍がありました。売れる場所に売れる自動車をどのように持って行くかを日々検討したのです。

T お話を伺い、IT 業界のわれわれも見習うべき点が多々あると痛感しました。データベース化やシステム化が遅れていますし、個人のノウハウや属性によらない体制を作りたいのですが、なかなかうまく行きません。

M 自動車がコネクテッドになり品質情報や利用状況のデータを収集・分析して迅速に対応できるようになりました。ですが、コネクテッドになるとセキュリティ対策にも力を入れなくてはなりません。MDI ではセキュリティにも取り組んでいます。自動車向けサイバーセキュリティでは、適切なソフトウェアアップデートを確保するためのプロセス整備が法規によりレギュレーション化されています。各メーカーは自動車のライフサイクルにわたりセキュリティを保証することになっています。

※ 2 **魂動（こどう）－ SOUL of MOTION**：クルマをただの鉄の塊ではなく、生き物のように生命感を感じさせるものにする。まるで意志を持って動き出しそうな緊張感と、体温を持ち呼吸しているかのような温かみをもった、生命感をカタチにするデザインコンセプト。

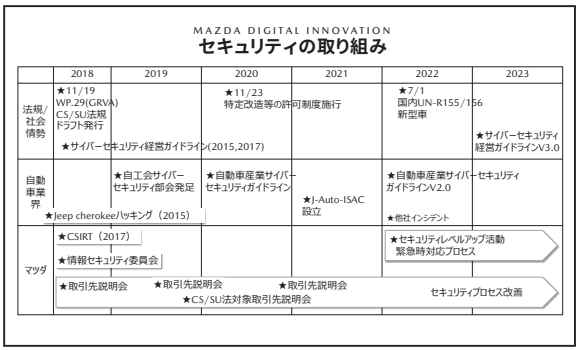


図 2 自動車のセキュリティに関する社会・業界・マツダの取り組み

サプライチェーン・セキュリティ強化の取り組み

T 引き続き、サプライチェーンのセキュリティについて伺いたいと思います。

M まず、背景にある社会情勢や自動車業界の動きから説明します（図 2）。社会情勢では 2015 年にサイバーセキュリティ基本法が施行され、2018 年には WP29（自動車基準調和世界フォーラム）が CS（サイバーセキュリティ）と SU（ソフトウェアアップデート）の法規策定に乗り出し、それぞれ「UN-R155」と「UN－R156」として採択され、日本国内においても 2022 年 7 月から新型車への適用が開始されています。また、2015 年には経済産業省よりサイバーセキュリティ経営ガイドラインも発表され、2023 年には Ver.3.0 に改訂されています。

T サイバーセキュリティ経営ガイドラインには、インシデント発生に備えた体制構築の 1 つとして「サプライチェーンセキュリティ対策の推進」が挙げられています。

M 自動車業界では、2015 年のジープ・チェロキーのハッキングが大きな転機となりました。日本自動車工業会（自工会）による「自動車産業サイバーセキュリティガイドライン」の制定や、業界内での情報共有や連携の推進を図る J-Auto-ISAC の設立などが相次ぎました。マツダとしては、まず CSIRT を設立し、CS/SU 法規に対応するための委員会を立ち上げ、取引先の企業とともに取り組みを続けています。

T 自動車業界が、サイバーセキュリティへの関心が高いとは認識していましたが、その背景には、業界内部の横のつながりの強さがあるという印象を持ちました。

M はい。横のつながりについては後ほどあらためてお話しします。前述した MDI では「デジタルモックアップ」を活用しています。これには部品サプライヤーの協力が不可欠です。ですから、部品サプライヤーがサイバー攻撃の被害に遭うと、自動車の生産だけではなく、設計もストップしてしまうのです。昨年、大手自動車メーカーの部品サプライヤーがランサムウェアに感染するというインシデントが発生しました。マツダとしてもサプライヤーの企業、1 社 1 社を直接回ってヒアリングし、緊急対応時プロセスを作ることにしたのです。

T 直接回られたのは何社ですか。また、部品サプライヤーは全体で何社あるのですか。

M 約 20 社です。国内部品サプライヤーは約 800 社になります。

T 20 社を選ばれた基準はあるのでしょうか。

M はい。前述の自工会が作成したガイドラインにはチェックリストがあり、サプライチェーンの多くがすでに回答を寄せている状況でした。また、中には複数の自動車メーカーに部品を供給している企業もあり、他社が先んじて対応してくれたところもありました。マツダがピックアップしたのは、広島を地盤に活動する部品サプライヤーで、自動車の製造に大きな影響を与える企業です。

T ピックアップの基準がわかるのと同時に、業界の横のつながりを垣間見ることができました。

M 駆動装置系、ボディシャーシ系、内装・外装部品などさまざまな企業を回りました。チェックリストに定めてある対策状況をヒアリングするのと同時に、サイバー攻撃を受けたときの緊急対応時プロセスがあるか確認したり、インシデント発生時にはマツダ側に報告するようお願いしたりしました。

T その結果はいかがでしたか。

M 結論を先に言うと、サイバーを起点とした緊急対応時プロセスがある企業はほとんどありませんでした。企業によっては火災や地震を想定したも

のがありましたが、サイバーと火災とでは対応が異なります。火災は気づいた時に消火できる可能性もありますが、サイバーでは気づいた時点で被害が大きくなっていることもあります。故に早め早めの対応が必要です。

部品サプライヤーの現場の声

T 製造業と IT 業界での違いはありますが、サプライチェーンのセキュリティはわれわれも取り組まなくてはならない喫緊の課題です。参考のためいくつか質問をさせてください。インシデント発生時の報告ですが、もう少し具体的にお話いただけますか。

M 例えば、マルウェアに感染したけれど駆除できた場合は報告の必要がなかったり、反対に拡散の恐れがあるマルウェアの場合やネットワークへの侵入、さらに警察等外部からの指摘があった場合は報告するといった具合です。

T 報告することによって部品サプライヤー側には何かメリットがあるのでしょうか。

M 報告が上がれば、われわれが支援するつもりです。ヒアリングでは各社の体制だけでなく、端末台数やシステム構成をお聞きしているので、報告から状況を推察することもできます。

T ヒアリングというと、部品サプライヤー側からは警戒されませんか。

M 警戒というか、われわれのような自動車会社の IT 部門の人間が部品サプライヤーを訪問することは、今までになかったことなので、最初は気まずい雰囲気でした（笑）。ですから、まず「監査に来たわけではない」ということを強調します。そのうえで、自動車業界で発生したインシデントなどをお話していると、こちらが訪れた意図などを理解し、協力していただけるようになります。

T 対面での真摯な話し合いが信頼に結びつき協力を得られたのですね。

M さきほども触れましたが、自動車業界では自工会が独自のチェックリストを作成し、部品メーカーなどに協力を要請していました。また、部品メーカーによっては、複数の自動車メーカーのサプライチェーンを兼ねています。例えば、マツダと他社でガイドラインに違いがあると困るわけです。ですから統一しようという流れになりました。こうした状況が、自動車業界全体のコンセンサスを生む背景になっているのだと思います。

対談は終始なごやかな雰囲気の中で行われた

T IT 分野だと IPA などがガイドラインを提供していますが、受け取る側が自分ゴトとして捉えていないように思います。皆が関わらなくてはならない仕組みを作る必要がありそうです。そういう形できちんと足並みを揃えないと全体の安全を担保するのは難しいかもしれません。

M 教科書的なガイドラインでは一般論が前提となっており「あれもやりましょう」「これもやりましょう」と書かれています。ですが、部品サプライヤーそれぞれの担当者から話を伺うと、いろいろと工夫されていることがわかりました。

T それは人員や予算の話でしょうか。

M はい。予算や人員が限られているからこそ、今のメンバーでできることに注力し、それ以外は利便性を捨ててセキュリティ優先の運用をしていたりします。教科書的なガイドラインに沿っているわけでもありませんし、ユーザーからすれば非常に不便なのですが、セキュリティ対策としては有効なケースも数多くあります。

規範の遵守性と対策の有効性のジレンマ

M 今の話題を端的に示している図があります（次頁 図 3）。高橋正和氏の著作※3 に掲載されてい

※ 3「**CISO のための情報セキュリティ戦略 - 危機から逆算して攻略せよ**」（技術評論社 2023 年 1 月刊）
図は著者の許諾を得た上で転載

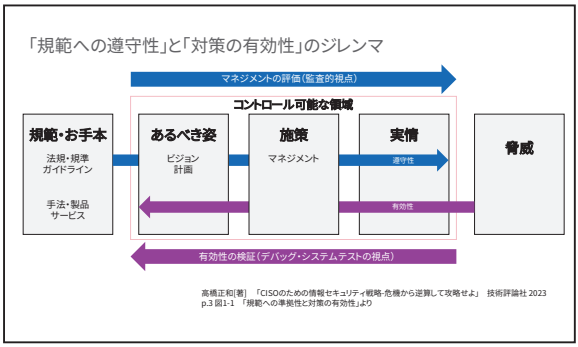


図 3 規範の遵守性と対策の有効性のジレンマ

るものです。ちなみにこの書籍には私も協力しており、高橋氏より謝辞をいただいています（笑）。図の右から左への矢印は、現実の脅威に日々対処している現場の技術者の視点です。一方で、左から右への矢印は、経営者の視点となります。

T はい。業種にかかわらず、経営層は規範やガイドラインなどの話題を好みますね。

M 仕事柄、部品サプライヤーの経営者の方ともお話する機会があるのですが、「現場をよく見てください」とお伝えしています。現場の技術者の方々は本当に頑張っておられます。それがよくわからないという経営者がいらっしゃれば、間をつなぐ役割の人を立てることをお勧めしています。それがセキュリティ体制づくりなのだと思います。

T まさに橋渡し人材ですね。「現場から経営」「経営から現場」どちらの話も理解でき、それぞれを通訳できる存在です。経営と技術者との間のコミュニケーションは本当に難しいと思います。技術者からすると、経営に事実を報告しているつもりでも、実は伝わっていないということも多いのです。経営がわかる言葉に変換しつつも、事実は事実として歪曲なく伝えなくてはなりません。経営の意向を現場に伝える時も同様です。そして、松本さんご自身もマツダ社内でそういう存在として活躍されているのだと思います。

IT の世界においてベンダーは どこまでサービスを提供すべきなのか

T IT 業界では、システムを開発・納品までが仕事で、保守については別途というのが、これまでの考え方だったと思います。ですが、この考え方をアップデートすべき時期が来ているように思えます。例えば、問題が発生したときにパッチを出して終わりでよいのか。また、システム構築時には想定されていなかった問題が発生した場合、それは納品後のことなので知りません、と言い切れるのか。システムの安全な稼働という根本に立って考えるべきだと思います。

M 従来の自動車はハードウェアとしての「モノ」を売るというビジネスだったと思います。販売後のサービスは部品のメンテナンスなどが主でした。一方、自動車の中のソフトウェアは、エンジン制御に始まり、自動運転へと発展しています。こうしたソフトウェアをサイバーセキュリティ法やソフトウェアアップデート法により、自動車のライフサイクルを通じて維持しなくてはなりません。加えて、コネクテッド・サービスによってさまざまな価値を提供するようになりました。

T ソフトウェアやサービスの比重が増していますね。

M はい。ユーザーに使い続けてもらう中で、ソフトウェアは常に進歩していかなくてはならないと思います。もはや「納品して終わり」の世界ではないのです。今、われわれは自動車のソフトウェアをメンテナンスしながらサービスを続けることにチャレンジしています。

T まさしく、時代の変革期にいることを実感しました。これまでのお話を伺い、自動車業界の取り組みは非常に興味深く、今後の IT 業界が参考にすべき点が多々あったと感じています。本日はありがとうございました。

マツダ広島本社のエントランスロビーにて撮影

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 2023.09

文＝ SHIELD Security Research Center

セキュリティインシデント対応能力の向上について

【概要】

サイバー攻撃を完全に防ぐことは困難であり、攻撃を受けることを前提に被害を軽減するための対応能力の向上が求められている。本稿では、対応能力の向上のために事業者等がサービス提供している演習や自組織で行う演習について、その目的や対象者、内容の違い、組織の環境を踏まえた訓練の重要性について解説する。

【内容】

さまざまな組織からインシデント対応に関する演習が提供されており、組織によって「サイバー演習」や「インシデント訓練」など名称や内容が異なる。これらの演習は大きく実働演習（Field Training Exercise「以下､FTX」）と机上演習（Table Top Exercise「以下、TTX」）に分けられる。FTX は実際のシステムなどを使用して演習を行うものである。一方、TTX は単に机の上で実施するという意味ではなく、FTX のような実際のシステム等を使用せずに模擬演習することを意味する。

TTX を大きく 2 つに分類したものを図に示す。1 つは図の左上「技術習得型 TTX」である。主に IT 部門を対象としてインシデントの原因調査等の技術習得を目的としたものである。もう 1 つは図の右下「問題検証型 TTX」である。インシデント発生時にその組織のインシデント対応計画などに従った適切な対応ができるか検証することを目的としたものである。

また、それぞれの内容も異なる。技術習得型 TTX は一般的なインシデント対応の流れを学びながら、その中で証拠保全やログ解析などの技術的要素も習得するものである。一方、問題検証型 TTX はその組織独自のインシデント対応計画などのルールに従った組織的対応のシミュレーションを行うとともに、インシデント対応計画などに問題がないかを検証するものである。さらに、問題検証型 TTX においては、複数部署にまたがるインシデント対応を模擬体験することで、組織の横断的対応の観点についても検証を行う。これらの検証結果から判明した問題を踏まえてインシデント対応計画などの見直しを行い、その見直し結果を次の演習に反映するというサイクルを繰り返すことにより組織の総合的な対応能力の向上を図っている。上述の通り、その組織の環境を踏まえているかどうかという点で一般的な演習より有益であるが、特定の組織を想定した演習であるため汎用的に利用できるものではないというデメリットがある。

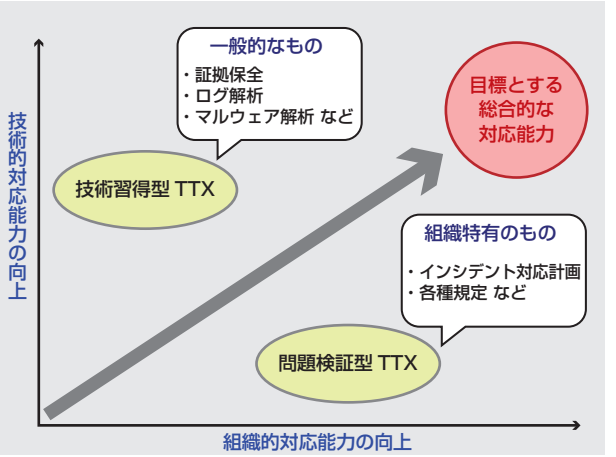


図 TTX の種類と位置づけ

技術習得型 TTX の代表として NICT（国立開発研究法人 情報通信研究機構）が主催する CYDER（実践的サイバー防御演習）がある。CYDER では仮想組織を演習舞台とし、セキュリティ関連規程の抜粋や演習環境を準備して、受講者はその規程類を確認しつつ実際に演習環境を操作しながら原因調査等を行う。このような外部組織が提供する技術習得型 TTX は受講者が所属する組織の環境を踏まえたものではなく、一般的なインシデント対応能力の向上を目的としたものである。

［情報源］
https://cyder.nict.go.jp/

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！

1. 自動起動プログラム確認編

文＝ SHIELD Security Research Center

1. はじめに

各種セキュリティツールを実践的に紹介する連載企画、「レッツトライツール」が Vol.50 よりスタートしました。第一弾では「HDD 保全」の工程を 3 回にわたり紹介してきました。今回からは「Windows システム確認」と題して 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確認します。

「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、「1. 自動起動プログラム確認編」として、Windows 起動時に自動的に起動するプログラムの登録例、Autoruns での確認方法を確認します。マルウェアが自動起動登録する可能性が高いといった特徴をもとにした、マルウェアの感染確認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、安全を保障するものではありません。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、推奨します。

2. Windows サンドボックスの準備

本稿では、Windows 標準で提供されている軽量なサンドボックス環境である「Windows サンドボックス」を使用します。「Windows サンドボックス」とは、「Windows 10 May 2019 Update」で追加された Windows の新機能です。Windows　OS の中に仮想的なコンピューター (Windows OS) を作り出すことができ、安全にソフトウェアの検証などを行うことが可能です。

Microsoft 社のドキュメントによると「Windows サンドボックス」の前提条件は下記の通りとなっています※。

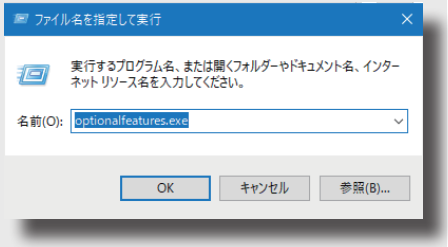
- Windows 10 Pro または Enterprise ビルド バージョン 18305 または Windows 11 を使用していること（Windows Home エディションはサポート対象外）
- ARM64 (Windows 11 バージョン 22H2 以降) または AMD64 アーキテクチャ
- BIOS で有効化された仮想化機能
- 少なくとも 4 GB の RAM (8 GB 推奨)
- 空きディスク領域 1 GB 以上 (SSD を推奨)
- 少なくとも 2 つの CPU コア (ハイパースレッディングを使用した 4 コアを推奨)

2.1 Windows サンドボックスの有効化

Windows サンドボックスは以降の手順で利用可能となります。すでに設定をしている方は不要となります。また、前期前提条件を満たしていない方は、「Windows サンドボックス」は利用できませんので、通常の Windows 上で実施してください。

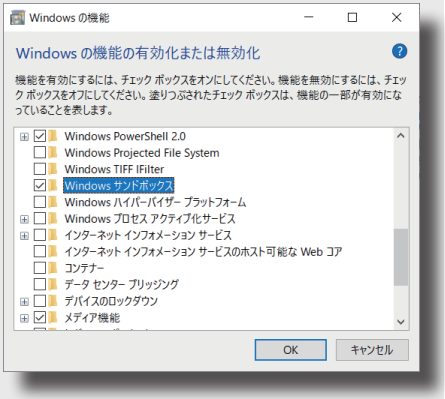
① optionalfeatures.exe の実行

Windows ロゴ キー＋R キーで「ファイル名を指定して実行」ダイアログボックスを起動し、「optionalfeatures.exe」を入力します。
もしくは、Windows 左下の Cortana(コルタナ) に「optionalfeatures.exe」と入力しても起動できます。



② Windows サンドボックスの有効化

Windows の機能ダイアログボックスが立ち上がるので、「Windows サンドボックス」にチェックを入れ、「OK」を押下します。「Windows サンドボックス」のインストールが始まりますので、インストールが完了しましたら再起動します。



※ **Windows サンドボックス**　https://learn.microsoft.com/ja-jp/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-overview

3. Autoruns の実行

3.1 Autoruns の準備

「Autoruns」とは、「Sysinternals Suite」に含まれる、Windows 起動時に実行されるプログラムを確認するためのツールです。

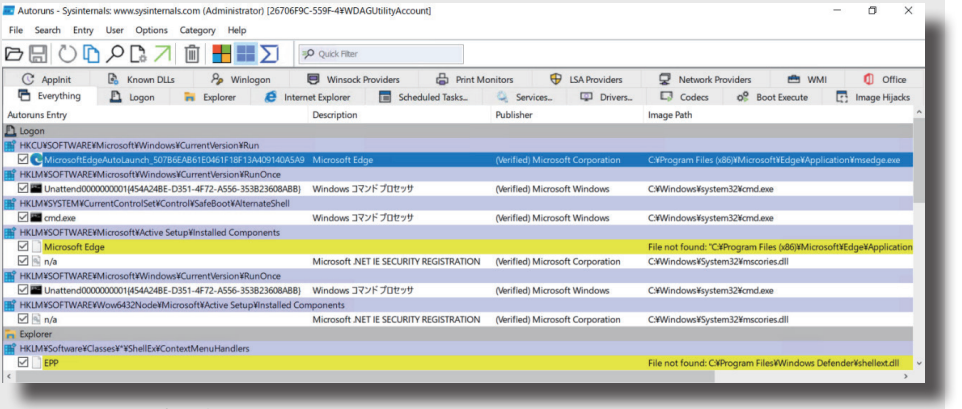
「Autoruns」および「Sysinternals Suite」は下記などから、ダウンロードすることができます。

- 「Autoruns」
  https://learn.microsoft.com/ja-jp/sysinternals/downloads/autoruns
- 「Sysinternals Suite」
  https://learn.microsoft.com/ja-jp/sysinternals/downloads/sysinternals-suite

今回は、Windows v14.1 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。今回は、筆者は Autoruns64.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。

3.2 自動起動プログラム確認

Autoruns を起動します。初回起動時には、利用規約の確認が入ります。内容を確認して、「Agree」を押下します。起動すると、自動起動するプログラムの登録状況などが確認できます。



自動起動するプログラムの登録箇所として以下の項目が挙げられます。

【レジストリ】

レジストリとは、Windows のシステムやソフトウェアの設定情報です。レジストリには、自動起動を設定するための箇所がいくつか存在します。代表的な自動起動に関するレジストリは下記の通りです。

[HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run]
[HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥RunOnce]
[HKCU¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run]
[HKCU¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥RunOnce]

HKLM は、コンピューターにログオンした際に実行されます。この場合は、ログオンした際に登録されているプログラムが自動実行されます。HKCU は、現在ログオンしているユーザーがログオンした際にのみ実行されるといった違いがあります。なお、RunOnce は、一度だけ自動実行され登録されているキーは削除されるといった特徴があります。

Autoruns では、【Logon】タブで確認できます。

「Windows サンドボックス」を利用した今回の例では、Microsoft Edge が登録されていることが確認できます。

【スタートアップ】

スタートアップは、格納されているプログラムを起動時に実行するフォルダーです。起動したいプログラムのショートカットなどを保存しておくことで、起動時にプログラムを実行できます。
Autoruns では、【Logon】タブで確認できます。

「Windows サンドボックス」を利用した今回の例では、何も登録されていません。

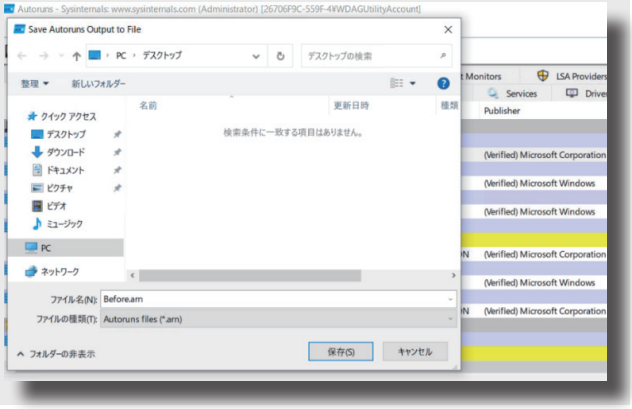
【タスク】

定例の作業を自動化するなどの目的で、Windows には「タスクスケジューラ」が標準で用意されている。「タスクスケジューラ」を活用することで、プログラムを起動時に実行することができます。
Autoruns では、【Scheduled Tasks】タブで確認できます。

「Windows サンドボックス」を利用した今回の例では、何も登録されていません。

3.3 状態の保存

次に、現在の自動実行プログラムの登録状況を保存します。メニューバーの「File」→「Save」より、自動実行プログラムの登録状況を保存してください。保存したファイルは「5.1 自動起動プログラムの差分確認」で利用します。



4. 自動起動するプログラムの設定

4.1 レジストリから自動起動するプログラム

Autoruns の機能を確認するにあたり、ここではサンプルとして自動起動設定がなされる Microsoft 社の Teams をインストールしてみます。

① Teams（サンプルとなるプログラム）のインストール

下記より、Teams をダウンロードしてインストールしてください。

https://www.microsoft.com/ja-jp/microsoft-teams/download-app

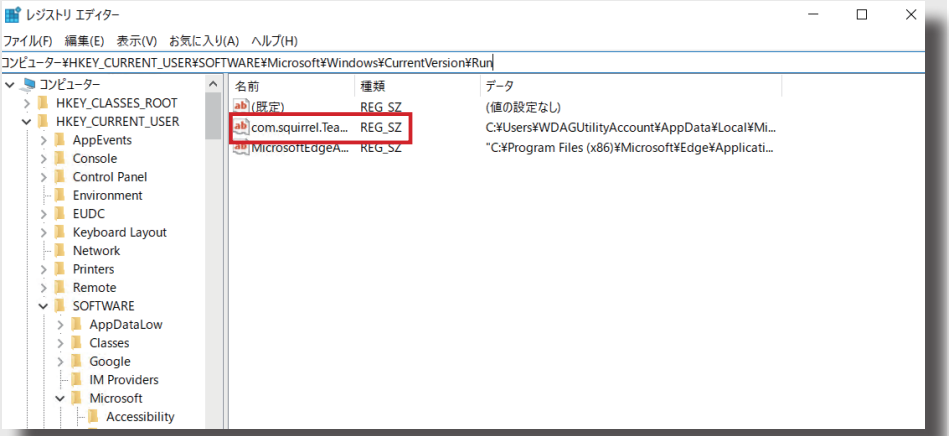
インストールする Teams は下記どちらの Temas でも問題ありません。環境に合わせてご選択ください。また、アカウントを利用してログインをする必要はありません。

②レジストリエディターの起動

インストールが完了したら、レジストリーキーの登録状況を手動で確認してみます。Windows ロゴ キー + R キーで「ファイル名を指定して実行」から「regedit.exe」を起動してください。「レジストリエディター」が起動したら、

HKEY_CURRENT_USER → SOFTWARE → Microsoft → Windows → CurrentVersion → Run

の順でフォルダーを開きます。「com.squirrel.Teams.Teams」といった Teams に関するキーが登録されていることを確認します。

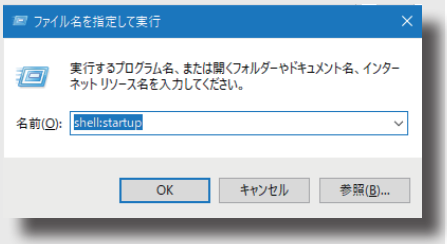


4.2 スタートアップフォルダーから自動起動するプログラム

①スタートアップフォルダーの確認

スタートアップフォルダーは、Windows ロゴ キー + R キーで「ファイル名を指定して実行」ダイアログボックスを起動し、「shell:startup」を入力することで確認できます。

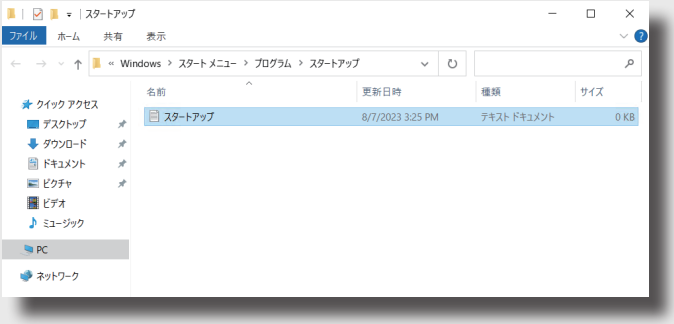
もしくは、「%AppData%¥Microsoft¥Windows¥Start Menu¥Programs¥Startup」で当該フォルダーを確認できます。



②サンプルファイルの追加

フォルダが開いたら、「スタートアップ」という名称のテキストファイルを保存します。

これで、スタートアップフォルダーを利用して「スタートアップ .txt」というテキストファイルが起動時開くように登録できました。

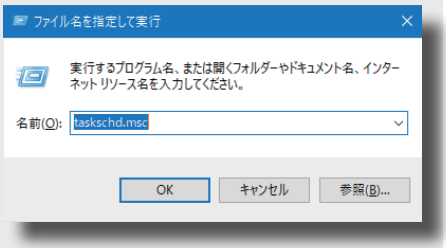


4.3 タスクから自動起動するプログラム

①タスクスケジューラの起動

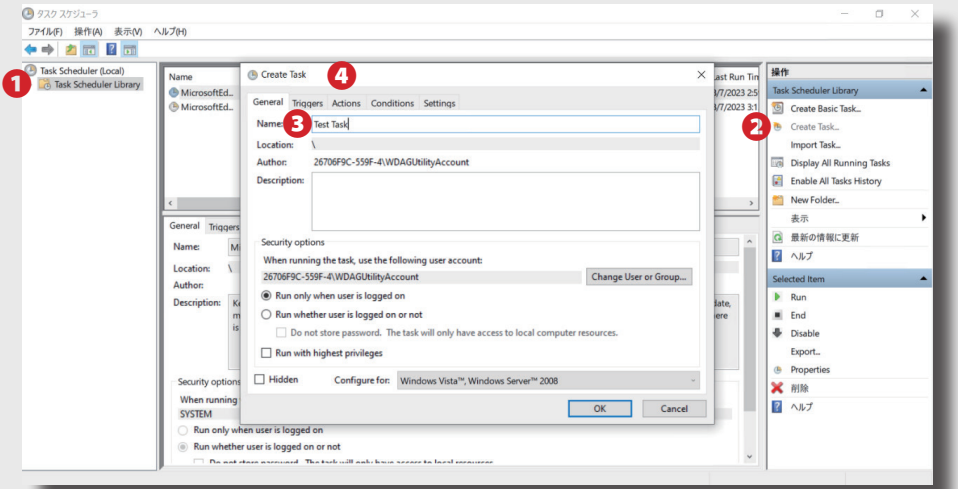
Windows ロゴ キー + R キーで「ファイル名を指定して実行」から、「taskschd.msc」を入力することで確認できます。

もしくは、Windows 左下の Cortana(コルタナ) に「タスクスケジューラ」と入力しても起動できます (Cortana(コルタナ) から、「taskschd.msc」でも可)。



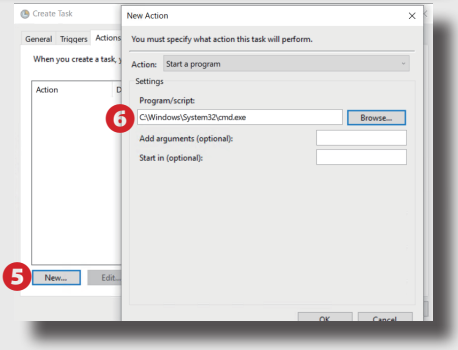
②タスクの作成（その 1）

タスクスケジューラが起動したら、左タブの「Task Scheduler Library」(❶) を選択し、右タブの Create Task(❷) をクリックします。Create Task ウインドが開いたら、Name に「Test Task」を (❸) を入力し、「Actions」タブをクリック (❹) します。



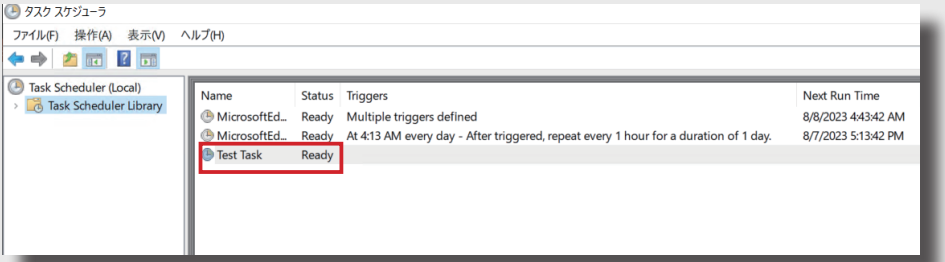
②タスクの作成（その 2）

「Actions」タブが開いたら、「New」をクリックし（❺）、「Program/script」に「C:¥Windows¥System32¥cmd.exe」を指定（❻）して登録します。



②タスクの確認

タスクスケジューラに「Test Task」が登録されましたら、登録完了です。Windows のユーザーログオン時に「cmd.exe(コマンドプロンプト)」が起動するように登録ができました。



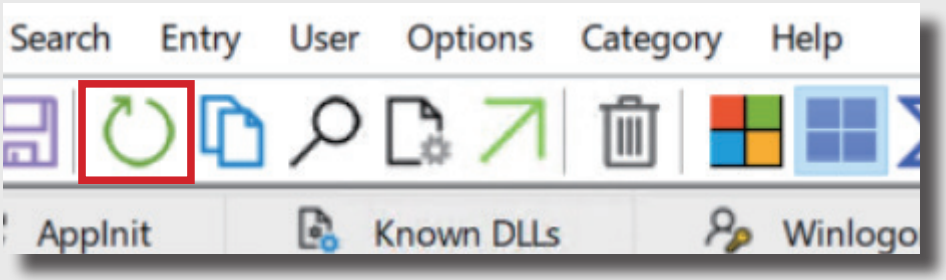
5. Autoruns を活用した調査方法

5.1 自動起動プログラムの差分確認

Autoruns では、保存していた自動実行プログラムの登録状況を用いて、新たに自動起動設定がなされたプログラムを確認可能です。

① Autoruns の更新

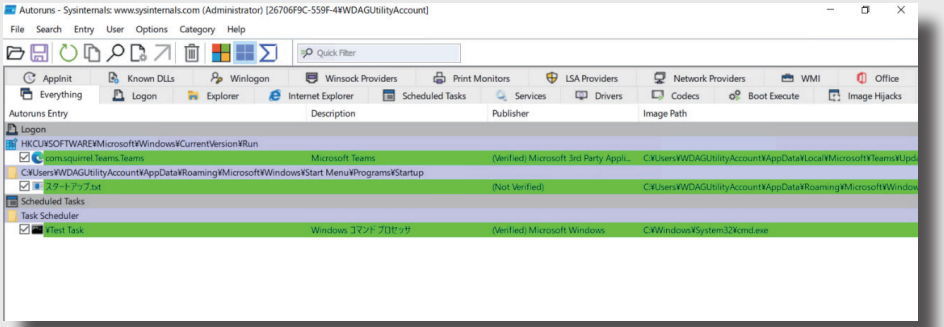
あらかじめリフレッシュボタンを押下して最新の状態に更新してください。



②差分の確認

次に、「File」->「Compare」より、「3.3 状態の保続」で取得した自動起動の設定する前のファイル(拡張子：arn) を選択してください。

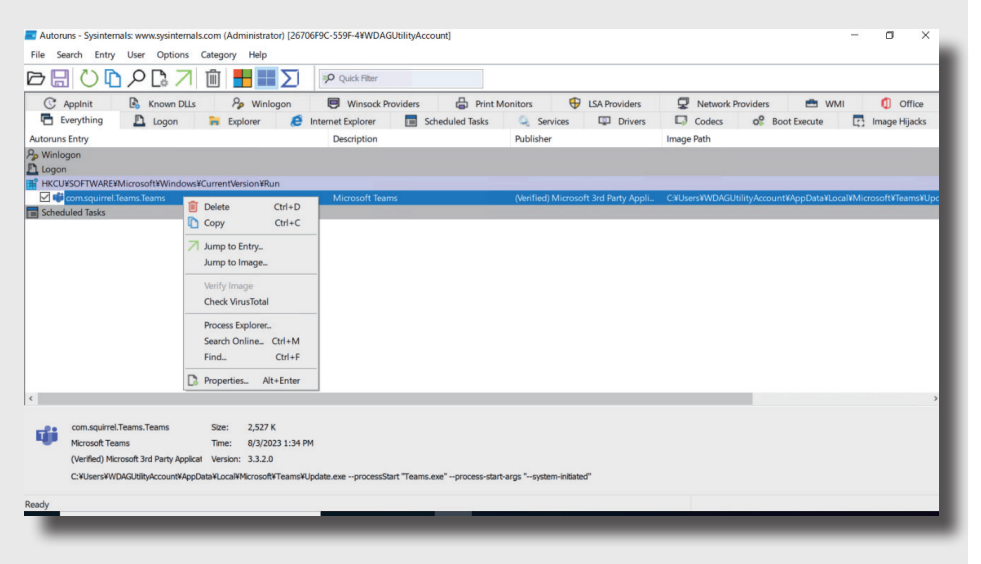
Compareを実行すると下記の通り、変更が加えられた箇所のみを表示(緑色の行) します。今回は、「4. 自動起動するプログラムの設定」で解説した、自動起動設定各種を Autoruns で確認することができました。



5.2 VirusTotal を用いた自動起動プログラムの安全性確認 (参考)

マルウェアはコンピューターに常駐するため、しばしば自動起動に設定されていることがあります。Autoruns を活用し、登録されているプログラム 1 つ 1 つのハッシュ値等を確認していくことで安全性を確認できますが、Autoruns ではハッシュ値を VirusTotal で確認、結果を表示する機能を有しています。

確認したいプログラムの行を右クリックし、「Check VirusTotal」より、安全性を確認することができます。



6. おわりに

今回はここまでとなります。

今回は、「1. 自動起動プログラム確認編」として、Windows 起動時に自動的に起動するプログラムの登録例として、レジストリ、タスク、スタートアップの登録方法を確認しました。

また、これらの登録状況について、「Sysinternals Suite」に含まれる「Autoruns」での確認方法を確認しました。

マルウェアが自動起動登録する可能性が高いといった特徴をもとにした、マルウェアの感染確認などに利用可能です。

次回は、同「Sysinternals Suite」に含まれる「Process Monitor」を用いて、Windows 上で起動しているプロセスの動きを確認します。