HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.50

株式会社 日立システムズ

Human * IT

Hitachi Systems security Journal VOL.50

TABLE OF CONTENTS

●はじめに

本文書は、株式会社日立システムズ の公開資料です。バックナンバーは以下の Web サイトで確認できます。
https://www.hitachi-systems.com/report/specialist/index.html

セキュリティ専門家が履歴書レビューや模擬面接のワークショップを開催して業界への就職を積極的に支援

キンバー・ドウセット インタビュー

Kimber Dowsett

インタビューサポート＋通訳＝エル・ケンタロウ
取材＋記事構成＝吉澤亨史
文＝斉藤健一

キンバー・ドウセット氏は、連邦政府機関・民間企業でセキュリティ・エンジニアとして活躍する一方、コミュニティ内では技術分野への就職希望者を支援するワークショップも展開している。そのような彼女に、キャリアの築き方、仕事に対する考え方、就職支援活動などについて話を伺った。

米国と日本で企業の採用方針が異なるのは読者の方も容易に想像がつくだろう。日本の採用面接では学生時代に力を入れてきたことやプライベートなことも質問されるが、米国では、スキルや経歴に関する質問がメインとなっている。だからといって、今回の記事で紹介されていることが、日本では通用しないかといえば、そんなことはないはずだ。氏が提案するのは特別なことではなく、応募先の組織を調査・研究して対策を立てるということだ。これは国の違いや新卒・転職を問わず誰もが取り入れられる要素だろう。

キャリアを築くということ 仕事に対する姿勢を定めてスキルを磨く

吉澤（以下 Y）：今回はお時間をいただき、ありがとうございます。インタビューに先立ち、キンバーさんの経歴や執筆記事、過去のインタビューなどを調べてみました。非常にユニークなキャリアをお持ちだと感じました。まず、ご自身のキャリアについて簡単に振り返っていただけますか。

キンバー・ドウセット（以下 K）：大学院ではニューメディア論を専攻していました。私が在学していた 2000 年代初頭にはまだサイバーセキュリティの学位は存在していませんでした。卒業後は Apple に入社しました。Apple Store では、AdobeCreativeSuite などプロフェッショナル向けアプリケーションのトレーニング・プログラムを提供しているのですが、私はこのプログラムのトレーナーとして採用され、活動していました。

Y キャリアのスタートはセキュリティではなかったと。

K あるとき、Apple 本社でトレーナー向けの講習を受けていたのですが、隣の部屋でコンピューターを分解している人たちを見かけました。それ

キンバー・ドウセット（Kimber Dowsett）

VMware Tanzu Application Platform チームのセキュリティエンジニアリング責任者。以前はワシントン DC のセキュリティコンサルタント会社、Krebs Stamos Group でディレクター、Truss のセキュリティエンジニアリング担当ディレクター、そして NASA の上級ミッション情報スペシャリストなどを歴任。

プライバシー、暗号化、一般向けテクノロジーに対する情熱を持つ。専門技術分野でのキャリア開始をめざす社会的地位の低いコミュニティのメンターとして活動し、選挙の整合性とセキュリティについての講演を行なう。PCB ベースの電子プロジェクトの設計と構築が趣味で、コミックブックやビデオゲームも愛好している。

は、Mac Genius プログラムのトレーニングでした。とても面白そうに見えたので、こっそりと席について講義を受けていたところ、なんと Genius トレーニングを修了できてしまったのです。

Y 修了できるところが米国的なのかもしれません。

K この経験が技術に興味を持つきっかけとなりました。当時の Apple には技術認定資格が 3 つありましたが、私はそのすべてを取得した初の女性となりました。ですが、このときの Apple は販売に注力する方針を打ち出していましたので、技術の仕事に就きたいという私の志向とはズレが生じていました。

Y その後、新たな一歩を踏み出すこととなるわけですが、どのような職に就きたいか、何か考えていたことはありますか。

K 大学院でニューメディア論を学んだ経験から、「民主主義における技術」「技術と民主主義のバランス」などといったことを考えていました。これがきっかけとなり、とあるスタートアップ企業に参加したのです。その企業では、地方有権者の声を米国議会議員に届けるアプリケーションを開発していました。とはいえ、そのアプローチはかなりアナログなもので、有権者が Web フォームで入力した情報を、私たちが印刷してワシントン DC の議会へ届けるというものでした。

Y 有権者の声を議会に届ける仕組みを作った意義は大きいと思います。

K その後、別のスタートアップ企業にも参加しましたが、そこでは結果として企業倫理やプライバシー保護について深く学ぶこととなりました。その企業は、ラジオの聴取率調査を業務としており、聴取データを記録する機器を各家庭に配布、その後回収して調査を行なっています。しかし、ある時、調査を通じて不必要に多くの個人情報が収集されていることを知ったのです。職場環境や給与条件などは良かったのですが、自分の倫理観とは相反する状況だったため、結局その会社を辞める決断をしました。

Y 確かにプライバシー保護は重要ですね

K はい。その後、NASA（米航空宇宙局）に入ることとなりますが、その頃から「民主主義における技術」に関する取り組みを、より一層責任感を持って進めるべきだと強く感じるようになりました。その中にはもちろんプライバシー保護も含まれています。巨大テクノロジー企業は市民を守る義務があり、それは利益よりも優先されるべきだと私は考えています。そして私自身は、そのような価値観に合致した仕事を選ぶよう心がけています。

履歴書レビューと模擬面接に関するワークショップ

Y セキュリティ・コミュニティ内でキンバーさんが取り組んでいる、MIRR（Mock Interview and Resume Review：模擬面接と履歴書レビュー）について伺います。このワークショップを始めたきっかけにはどのような背景があったのでしょうか。

K きっかけはロビーコン（カンファレンス会場のロビーで参加者同士が意見を交わす私的な集会の通称）でした。確か、2016 年・2017 年くらいだと記憶しています。偶然にも私に履歴書のチェックを頼んできた人がいました。聞けば就職活動で苦戦しているとのこと。そこで、私が履歴書を見てアドバイスをしていると、次第に希望者が増えていきました。そこで、数人の仲間とともに非公式ではありますが、プロジェクトを始めることにしたのです。これまでにさまざまなカンファレンスで実施しており、中には正式なコンテンツとして採用してくれたところもあります。

Y 盛況ですね。

K はい。反響の大きさに自分たちも驚きました。ですが、次第にこのプロジェクトを自分たちだけで動かすことが難しくなってきたので、ワークショップのフレームワークを作り、GitHub で公開し、オープンソース化することとしたのです※1。今では、このフレームワークを使ってさまざまな人たちがワークショップを開いています。

Y キンバーさんが関わったワークショップでは何名くらいの方が参加されたのでしょうか。

K 私が関わったものだと 400 ～ 500 名ほどです。その中から 200 名ほどが何かしらの形で職務につくことができました。

※1 **MIRR Workshop** https://github.com/mzbat/mirr

キンバー・ドウセット氏は米国在住だが、このオンライン・インタビューは彼女の欧州への出張中に行なわれた。
さらに移動中の船内での対応となったそうだ

Y さきほど出た履歴書のチェックのお話ではどのようなアドバイスをされたのでしょうか。

K その人はセキュリティ業界に入って間もない方で、職務経歴書には、自分が重要だと考えている項目だけが簡潔に記述されていました。そこで、私は CTF 大会に参加した経験があるか尋ねてみました。新卒やセキュリティ業界でのキャリアを始めたばかりの段階では、どのように技術やセキュリティに興味を持ったのか、また、この業界を選んだ理由や背景を示す情報を履歴書に盛り込むことが重要です。というのも、面接官から見た場合、応募者がコミュニティとどのように関わりを持っているのかを知る手がかりにもなるからです。

Y 面接官の視点というのは自分の中にはありませんでしたから、とても新鮮に感じました。

K 多くの人が、履歴書を定型のテンプレートに基づいて作成していると思いますが、私自身、そうである必要はないと考えています。ひとそれぞれユニークなキャリア形成がありますから、それは履歴書にも反映するべきだと思っています。また、履歴書を書く時、多くの人に実践してほしいと思うのは、募集要項と履歴書をマッチングさせることです。私自身は応募の履歴書を 1 枚にまとめるようにしています。もちろん、すべての職務経歴や取得した認証資格、執筆した書籍などを含めると相当なボリュームになります。これを基に応募先の組織ごとに適切だと思われる情報をピックアップして履歴書を作成します。例えば 20 社に履歴書を送るのであれば、20 社分の履歴書はすべて異なった内容となります。

Y 履歴書をカスタマイズするということですね。

K 特に、大企業では応募者が多数となることから、事前に機械的な書類審査が行なわれることがあります。企業が応募要項で求めているキーワードが履歴書に反映されていないと、一次審査すら通過できませんから、調査して履歴書をカスタマイズするのです。

Y 同様に、模擬面接を受けた人にアドバイスしているポイントなどはありますか？

K 大切なのは面接の準備をすることです。多くの人は何の準備もしないまま面接を受けています。面接官がどのような職務を担当しているのか、どのような背景を持っているかなどを事前に調べておくだけでも、面接が進む方向を予測する手助けとなります。例えば、採用までに面接が 3 回～ 4 回行なわれる企業だとすれば、技術者・人事担当者・ライン統括マネージャーなどさまざまな職務の人が面接官となる可能性があります。それぞれの人がどのような質問をしてくるかなどを事前に考えておく必要があると思います。

Y 事前に準備していれば、予期しない質問にアタフタすることも減りますね。

K また、米国の話になりますが、過去 5 年間で面接において多様性に関する質問が増えてきまし

た。これは応募者の個性が企業文化と合っているかを探るための質問です。ただし、この「多様性」が指すものは、教育・社会経済・経歴・歴史・人種・宗教などさまざまな要素が含まれます。応募者は面接の際に、面接官が何を求めているのかを考える必要があります。先ほど述べた MIRR のフレームワークでは、このような多様性に関する質問の例などを提供しています。

Y 転職の場合だと、十数年ぶりに面接を受けるという状況も珍しくありません。その時にこうした社会的な質問をされると、どのように答えたらよいか分かりませんから、模擬面接は大切だと感じました。

K もう 1 つ、面接でよく見られる間違いについて紹介します。面接では最後に必ず「何か質問があるか」と尋ねられます。多くの人は「ない」と答えてしまいますが、これは実は適切な回答とは言えません。その企業で働きたいと真剣に考えているのなら、何かしらの質問はあるはずです。質問しないということは、面接官に対して、その人が組織や仕事について調査をしていないと思われる可能性があります。福利厚生などに関する質問ではなく、チーム構成や人数など、仕事に直結する質問をするべきです。

Y あらかじめ質問を用意するのがよさそうです。

K はい。参考になるかどうか分かりませんが私自身の話をします。私が面接を受けるのは管理職を募集しているケースですが、面接官に「最後に休暇を取得したのはいつか」と質問するようにしています。というのも、その回答から組織のワークライフバランスについて多くの情報が得られるからです。

Y 面白い視点からの質問です。

K 面接官の立場から考えると、応募者が質問を持っているか否かは、その人が実際に組織について調査を行なったのか、あるいは募集広告を見つけて応募しただけなのかを判断するための重要な指標となります。

Y MIRR の今後について考えていることがあれば教えてください。

K 私がワークショップ運営に直接関わっているのは、防御側の人たちを対象にした Blue Team Con のみです※ 2。このカンファレンスは毎年夏に開催されていますが、それ以外の時期、例えば春などにオンラインでワークショップを開催したいと考えています。ただ、オンライン開催は対面開催とは違った難しさがあるようにも感じています。他にもフレームワークの更新作業なども引き続き行なっていくつもりです。

成長に求められる 2 つの視点とメンターシップ

Y 最後になりますが、セキュリティ業界への就職をめざす人、あるいは業界内で転職して新たなスキルを習得したい人に向けて、アドバイスやメッセージがあればお願いします。

K 難しい質問です。セキュリティは非常に広範で、専門性は多岐におよびます。1 つの専門分野を深く掘り下げていく視点も重要ですが、それだけでは行き詰まる可能性もあります。そのため、全体を俯瞰する視点を持つことも大切だと私は考えます。手始めに自分が興味ある分野で働く人に「あなたの日常はどんな感じですか」と尋ねてみるところからはじめてみるのがよいと思います。

Y 2 つ視点を持つことは大切ですね。

K また、行き詰まったときに、相談したり助言を求めたりできるメンターの存在も重要です。私自身もメンターとして活動しています。多くの場合、メンティー（指導を受ける人）は具体的な答えを求めてきますが、私が示すのはあくまで答えにたどり着くまでの道筋です。このやりとりを続ける中で、メンティーは答えを見つけるやり方を学んでいくのだと思います。もちろん、メンターもメンティーと向き合う時間や気力といった覚悟が求められます。

Y まさに師弟関係ですね。本日は貴重な話を伺うことができました。ありがとうございました。

※ 2 **Blue Team Con** https://blueteamcon.com/

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

Hitachi Systems CSI（Cyber Security Intelligence）Watch 2023.06

文＝日立システムズ

Telegram を利用した サイバー犯罪の犯行声明増加に関する考察

【概要】

サイバー犯罪者からの犯行声明に、ロシア人技術者が開発した無料のインスタントメッセージアプリケーションである Telegram が使用される事例が増加している。例えば、DDoS 攻撃の犯行声明に Telegram が使用されるケースなどだ。これまでは Twitter などを介して声明が出されていたが、昨今、Telegram が犯行声明に利用される理由について考察する。

【【内容】

Telegram は無料のメッセージアプリであり、基本的な機能は LINE や Facebook、Messenger と変わらず、テキストチャットや音声・ビデオ通話、画像やファイルの共有などが可能である。また、2022 年 6 月の公式ブログによると、ユーザー数は 7 億人を突破しており普及率も増加している。

その一方で、Telegram は他のメッセージアプリに比べ犯罪で利用されるという負の側面も持つ。例えば日本の犯罪者による事例では、2023 年 2 月に逮捕された「ルフィ」をリーダーとするグループによる連続強盗・特殊詐欺事件で、犯行指示の連絡に Telegram が使われた。他にも、海外の犯罪者による事例では 2023 年 2 月 13 日に NoName057(16) が Telegram で日本の複数 Web サイトに対して DDoS 攻撃[※1] を行なったことを公表した（図）。また、2022 年 9 月 6 日には Killnet が、日本政府が運営する行政情報の総合窓口サイト「e-Gov」などへの攻撃を投稿している。

これまで DDoS 攻撃の声明には、Twitter などを介した攻撃対象の事前予告が多かったが、昨今は「実際に攻撃が成功した」という犯行声明が多い。これ

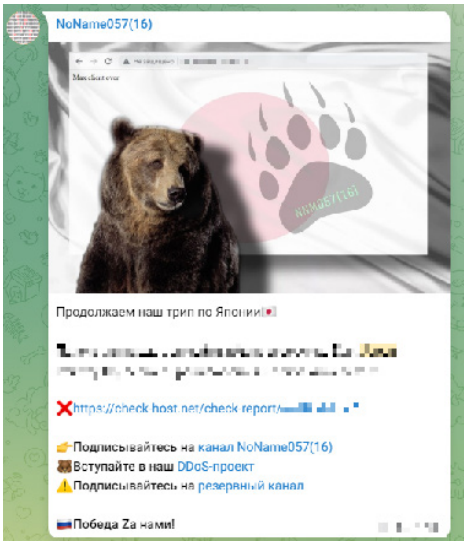


図 Telegram を使った攻撃声明の例
NoName057(16) が 日本の企業に対し DDoS 攻撃を行なったことを訴求したもの

は DDoS 攻撃への対策が広まったことで、攻撃が成功するかを事前に予測することが困難となり、明確な対象を事前に宣言しづらい状況になったことなどが理由に挙げられる。

Telegram が犯行声明に利用されやすい理由の 1 つとして匿名性の高さがある。LINE や Twitter などの登録では、電話番号による認証などが必要となり匿名性の確保は難しい。一方、Telegram は SIM カード（電話番号を含む識別情報）なしでもアカウント登録が可能である。これには Telegram 開発者が立ち上げた分散型オークションプラットフォーム「Fragment」で匿名番号（Anonymous Number）の購入が必須だが、SIM カード不要というのは、犯罪者にとって非常に好都合である。

また、サイバー犯罪に利用されるプラットフォームも変化している。従来、サイバー犯罪関連のフォー

ラムやマーケットなどはダークウェブでの運用が主だったが、法執行機関による摘発やフォーラムなどに対するサイバー攻撃といったサイバー犯罪者側にとっての課題も存在していた。一方、Telegram は登録・利用が容易であり匿名性が高いため、サイバー犯罪者にとって利用しやすい。

加えて、シークレットチャット機能を使えば、チャットを開始した端末のみにアクセスを制限することや、一定時間でのメッセージ自動消去、チャットの削除で相手の端末からも閲覧不可となるなど、非常に秘匿性の高いやりとりが可能である。このため、主要なサイバー犯罪のコミュニティがダークウェブから Telegram へと移行しており、それに伴って犯行声明で利用するプラットフォームが変化している可能性がある。

現時点では法執行機関による Telegram の通信履歴追跡や暗号化情報の復号は公表されていない。これらの点から、Telegram がサイバー犯罪者に好まれる理由と考えられる。

【情報源】

https://www.sompocybersecurity.com/column/column/shift_from_darkweb_to_telegram
https://telegram.org/blog/700-million-and-premium
https://www.bbc.com/japanese/64592167

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 HDD 保全！

1. 準備編

文＝日立システムズ

●はじめに

セキュリティ対応の現場ではさまざまな状況に直面します。それゆえに広範囲にわたる知見が必要となりますし、使用するツールも多岐にわたります。

本稿「レッツトライツール」は、各種の状況で使用されるセキュリティツールを実践的に紹介する連載です。

今号から 3 号にわたり「HDD の保全」について紹介します。セキュリティ・インシデントの調査において、元データがその後の分析に利用可能な状態で保たれていることが重要です。これが HDD の保全が必要となる主な理由です。

HDD の保全作業は図 1 のとおりです。1から6までの工程がありますが、今号では「準備編」として保全の事前準備となる1、2の作業を解説します。なお、本稿では保全対象を HDD としています。HDD 以外の対象には適用できない解説も含まれていますのでご注意ください。

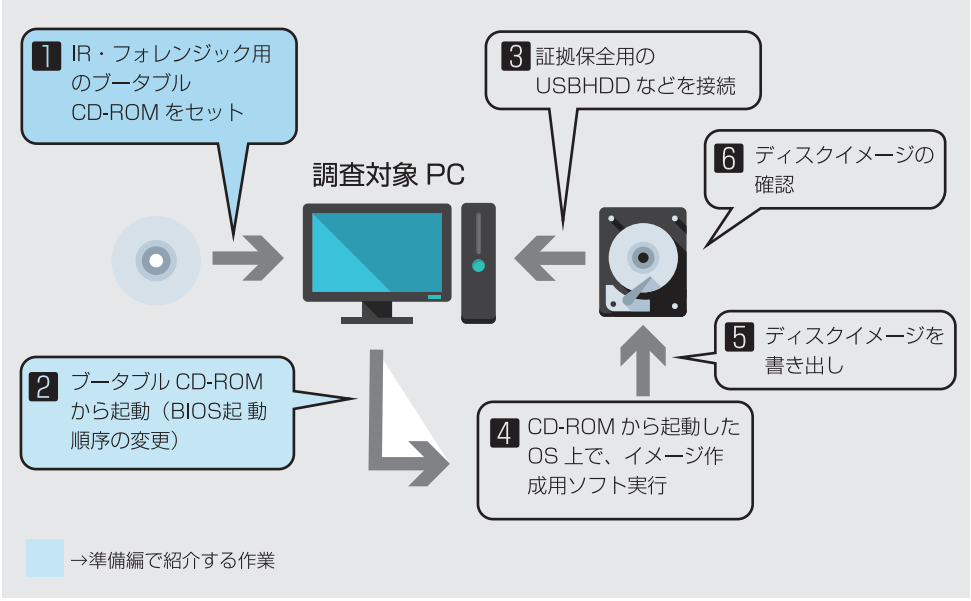


図 1 HDD 保全の工程と準備編で紹介する作業

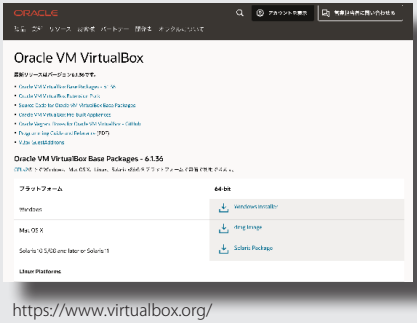
●環境の構築

●ゲスト OS（保全対象）作成の準備

保全の実習を行なうにあたり、保全を行なう対象のコンピューターが必要となります。今回は、保全を行なう対象のコンピューターとして、Oracle Virtual Box を利用し、CentOS がインストールされた仮想マシンを作成します。

① Oracle VirualBox のダウンロード

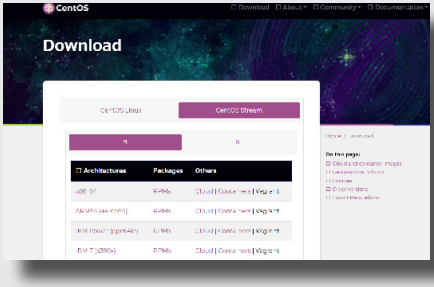
Oracle VirualBox は公式サイトから入手できます。なお、Virtual Box のインストールは基本的に初期設定で進めて問題ありませんので、手順などは省略します。



https://www.virtualbox.org/

② CentOS のダウンロード

また、CentOS の最新版も公式サイトから入手可能です。今回は、2023 年 4 月時点最新版の「CentOS Stream9」をダウンロードします。

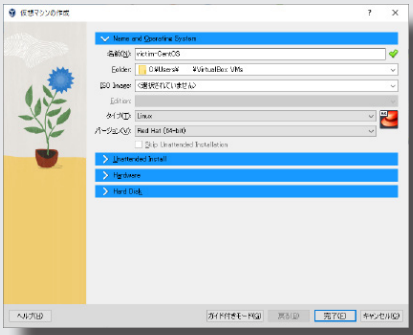


https://www.centos.org/download/

●ゲスト OS の作成と仮想マシンの起動

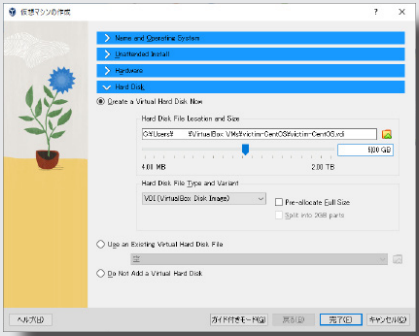
① 新規 VM イメージの作成

ダウンロードが完了したら、VirtualBox を立ち上げて、新規 VM イメージを作成します。VM イメージ作成する際は、OS 名を名称に入れると、VirutalBOX が OS 種別を自動認識する場合があるので便利です。



②ディスクサイズの設定

ここで、ディスクサイズを 5GB と設定しています。これは、CentOS9 を minimam インストールする（後述）ために必要な最小サイズです。あまり大きなサイズで作成すると、保全する際に時間がかかりますのでご注意ください。

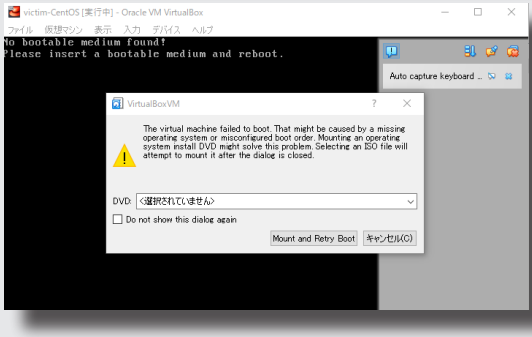


③ VM イメージの完成

VM イメージが作成できましたら、図のように追加されます。

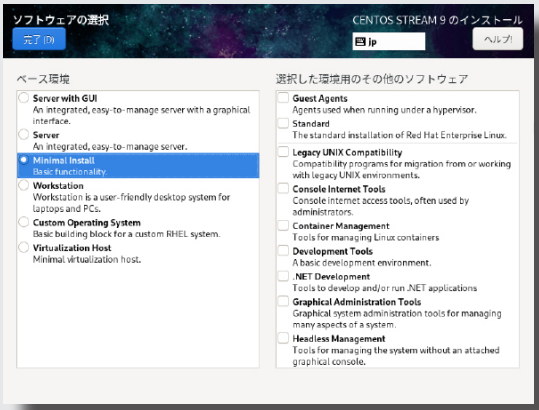
④ VM イメージの起動

「起動」ボタンをクリックして VM イメージを起動します。この時、OS がインストールされていませんので、図のように OS のインストール DVD を求められます。ダウンロードしておいた「CentOS Stream9」の ISO イメージを指定してください。ISO イメージを指定して起動すると、インストール設定画面が開きます。



⑤ CentOS のインストール

「CentOS Stream9」のインストール設定画面が開きましたら、まず、ソフトウェアから、最小インストール「Minimal Install」を選択してください。VM 作成時間、イメージの容量の節約にもなります。



TIPS

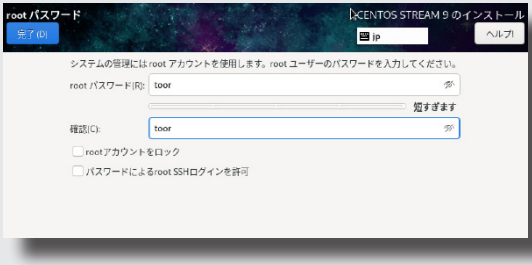
Linux OS をインストールする際は、まずは「Minimal Install」で作成し、必要なパッケージのみを追加する形を推奨します。これにより、余計なパッケージがインストールされず、攻撃の温床になる可能性を低くすることができます。

⑥ CentOS のインストール設定（インストール先）

今回は、ストレージの設定として「自動構成」を指定しました。お好みによって、パーティションを指定してください。

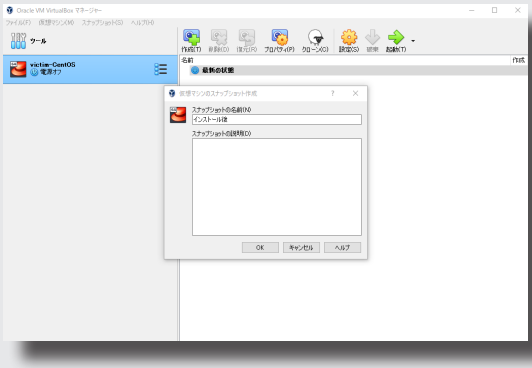
⑦ CentOS のインストール設定（パスワード）

root でログインするためのパスワードを設定します。記事では「toor」としていますが、読者の方は、それぞれのパスワードを設定してください。



⑧ CentOS インストール完了・スナップショットの作成

これらの設定が完了しましたら、インストールを開始します。「インストールが完了しました」と表示されれば作業は完了です。「システムの再起動」ボタンをクリックすると、CentOS が起動します。ただし、今回は、初期状態でスナップショットを取得するため、いったん電源をオフにします。CentOS がシャットダウンしたら、スナップショットを取得します。



TIPS

初期状態でスナップショットを取っておくと、さまざまな形で利用可能となり便利です。今後の本誌でも、また利用することもあるかと思いますので、是非、電源がオフになりましたら、スナップショットを取得しておきましょう。

⑨ CentOS に root ログイン・フラグの保存

スナップショットの作成が完了したら、CentOS を起動し、root と指定したパスワードでログインできることを確認してください。保全対象 HDD を確認するフラグ（目印）となるファイルを作成します。図のコマンドを用いて、確認用のフォルダー (/root/himitsu)、テキスト作成 (/root/himitsu/himitsu.txt) してください。

```
# mkdir /root/himitsu
# touch /root/himitsu/himitsu.txt
# echo himitsu > /root/himitsu/himitsu.txt
```

⑩ CentOS のシャットダウン

フラグとなるファイルの作成を終えたら、OS のシャットダウンします。シャットダウン後はあらためてスナップショットの取得をお勧めします。

```
# shutdown –h now
```

Tsurugi Linux

● Tsurugi Linux 起動の準備

「Tsurugi Linux」とは、オープンソースプロジェクトの、DFIR（Digital Forensics and Incident Response）向け Linux ディストリビューションです。保全に必要なツール類が初期状態でインストールされているなど使いやすいディストリビューションとなっています。

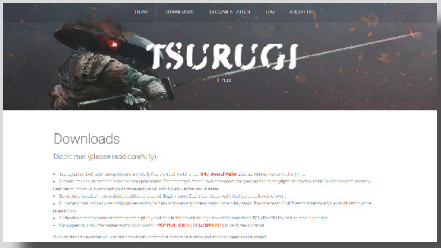
① Tsurugi Linux のダウンロード

「Tsurugi Linux」は、公式サイトからダウンロード、利用が可能です。

今回は、LIVE 起動が可能な下記の「Tsurugi Acquire」をダウンロード利用します。

Tsurugi Acquire [32-bit]
Filename: tsurugi_acquire_2021.1.iso
Release date: 09/04/2021

LIVE 起動とは、侵害された実機コンピューターを用いて、DVD や USB デバイスなど、外部メディアから、OS を起動する手法です。



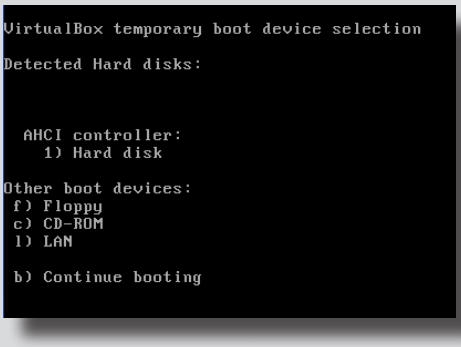
https://tsurugi-linux.org/downloads.php

TIPS

LIVE 起動を用いた保全は、実機 PC から HDD を取り出すことが困難な場合などに利用します。それ以外の方法として、以下の形で保全できます。状況に応じて、保全方法を検討してください。

・HDD などを取り外し、他のコンピューターに接続して保全
・HDD などを取り外し、専用機器を用いて複製して保全
・VMWare イメージをコピーして保全

② BIOS 設定の確認



「Tsurugi Linux」を Live 起動するにあたり、事前に BIOS 設定の確認が必要となります。一般的な PC では、BIOS 設定を通じて起動ドライブを選択できます。通常、PC は HDD から起動する設定となっていますが、マルウェア感染などの侵害を受けた場合、ログファイルが削除されるなどして PC の状態に変化が生じる可能性があります。このような問題を防ぐため、DVD や USB などの外部メディアから起動するように BIOS 設定を変更します。

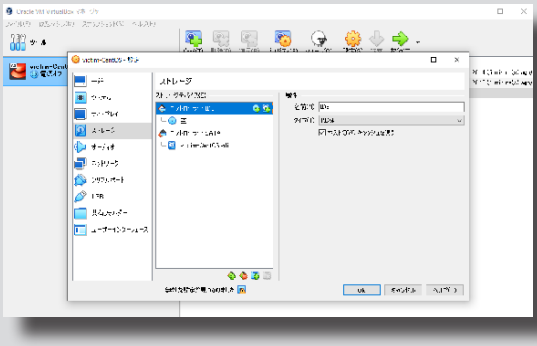
BIOS 設定画面の呼び出しや、起動メディアの設定方法は PC によって異なりますので、マニュアルなどでご確認ください。

VirtualBox では、起動時に F12 キーを押下する事で BIOS の設定画面を呼び出すことができ、通常の PC とは異なり単純なものとなります。なお、今回の記事で紹介する環境においては、この作業は必要ありません。

● Tsurugi Linux の Live 起動

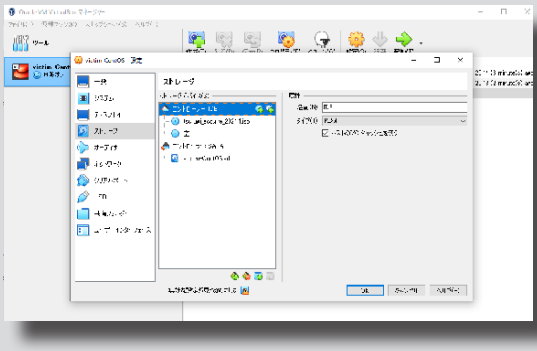
①ストレージ設定

VirtualBox の VM イメージを選択、設定ボタンを押下して、ストレージ設定を開きます。



② Tsurugi Linux の選択

コントローラ：IDE より、「Tsurugi Linux」イメージファイルをマウントします。この状態は、物理マシン（実機 PC）の DVD ドライブに「Tsurugi Linux」のメディアがセットされているのと同じ状況となります。



TIPS

今回は、VirtualBox において起動をする手順を紹介しましたが、実機 PC で Live 起動する場合は、CD/DVD などに保存するなどして準備しておきます。

なお、LiveCD/DVD を用いて起動する際には、BIOS の設定から以下の点に注意が必要です。

・起動順序

OS の読み込み順序を確認します。

具体的には、OS（今回の場合、CentOS）がインストールされているデバイスより、先に DVD Drive が読み込まれる設定となっていることを確認します。

・SecureBoot(Windows の場合)

SecureBoot が有効となっている場合、LiveCD/DVD での起動ができない場合があります。起動前に設定を確認します。

③ Tsurugi Linux の起動メニュー

「Tsurugi Linux」のブートローダーが起動します。今回は、Live で起動するので「Tsurugi Acquire Live（GUI mode）」で起動します。

④ Tsurugi Linux の起動

しばらくすると、「Tsurugi Linux」の起動が完了します。

●ファイルシステムの確認、保全 HDD の確認

①ファイルシステムの確認

OS の起動後、ターミナルを開き、ファイルシステムの状況を確認します。

```
#df -k
```

```
root@acquire:~# df -k
Filesystem     1K-blocks    Used Available Use% Mounted on
udev              996788       0    996788   0% /dev
tmpfs             206172     912    205260   1% /run
/dev/sr0         1185890 1185890         0 100% /run/live/medium
/dev/loop0        803840  803840         0 100% /run/live/rootfs/filesystem.squa
shfs
tmpfs            1030852   20076   1010776   2% /run/live/overlay
overlay          1030852   20076   1010776   2% /
tmpfs            1030848       0   1030848   0% /dev/shm
tmpfs               5120       0      5120   0% /run/lock
tmpfs            1030848       0   1030848   0% /sys/fs/cgroup
tmpfs            1030848       4   1030844   1% /tmp
tmpfs             206168      20    206148   1% /run/user/0
```

現段階では、作成した 5Gbyte の「CentOS」のファイルシステムは、「Tsurugi Linux」から確認できません。

②パーティション確認による保全 HDD の特定

次に以下の、fdisk コマンドで、デバイスの認識状況を確認します。

```
# fdisk -l
```

```
Device     Boot   Start      End Sectors Size Id Type
/dev/sda1  *       2048  2099199 2097152   1G 83 Linux
/dev/sda2       2099200 10485759 8386560   4G 8e Linux LVM



Disk /dev/loop0: 784.9 MiB, 823037952 bytes, 1607496 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/cs-swap: 512 MiB, 536870912 bytes, 1048576 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
                                                    保全対象
Disk /dev/mapper/cs-root: 3.5 GiB, 3753902080 bytes, 7331840 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

CentOS のパーティションと設定した物理デバイスは、/dev/sda と認識されています
今回は、CentOS の作成時に、ストレージを自動構成で作成しました。昨今の CentOS の初期状態では LVM を利用して論理的にパーティションを構成します。
そのため、詳細は割愛しますが、今回は、/dev/mapper/cs-root が、CentOS の root システムパーティションとなり、保全対象となります。

③保全 HDD のマウント

このパーティションを「Tsurugi Linux」でマウントして、読み込んでいきます。
この時、「-o ro」オプションを忘れずに付与し、" リードオンリーモード " でマウントしてください。

```
# mount -o ro /dev/mapper/cs-root /mnt/virtual1
```

実行結果は下記のとおりです。

```
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,mem
ory)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime
,perf_event)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hu
getlb)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blki
o)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,fr
eezer)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=27,pgrp=1,time
out=0,minproto=5,maxproto=5,direct,pipe_ino=11032)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,relatime)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=206136k,mode=700)
gvfsd-fuse on /run/user/0/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,us
er_id=0,group_id=0)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
/dev/mapper/cs-root on /mnt/virtual1 type xfs (ro,relatime,attr2,inode64,logbufs
=8,logbsize=32k,noquota)
```

保全対象

TIPS

リードオンリーモードマウントの必要性
OS からファイルを保存するだけでなく、ファイルを開く、ファイルの一覧を閲覧するだけでも OS が管理するファイルのタイムスタンプが更新される場合があります。タイムスタンプが更新されてしまっては、保全の本来の意味を成しません。そのため、リードオンリーモードでマウントすることで、オリジナルデータの改変を防ぎます。

df コマンドを利用してファイルシステムとしても認識されていることを確認します。

```
# df -k
```

実行結果は下記のとおりです。

```
root@acquire:~# df -k
Filesystem          1K-blocks    Used Available Use% Mounted on
udev                   996628       0    996628   0% /dev
tmpfs                  206140     912    205228   1% /run
/dev/sr0              1185890 1185890         0 100% /run/live/medium
/dev/loop0             803840  803840         0 100% /run/live/rootfs/filesystem
.squashfs
tmpfs                 1030692   20080   1010612   2% /run/live/overlay
overlay               1030692   20080   1010612   2% /
tmpfs                 1030688       0   1030688   0% /dev/shm
tmpfs                    5120       0      5120   0% /run/lock
tmpfs                 1030688       0   1030688   0% /sys/fs/cgroup
tmpfs                 1030688       4   1030684   1% /tmp
tmpfs                  206136      20    206116   1% /run/user/0
/dev/mapper/cs-root   3600384 1299488   2300896  37% /mnt/virtual1
```

保全対象

④フラグの確認

最後に、作成した himitsu.txt の存在を確認します。

```
# ls -la /mnt/virutal1/root/himitsu/himitsu.txt
```

これにより、保全対象の CentOS のディスクをマウントしたことを確認できました。
今回はここまでとなります。

●おわりに

今回は、保全対象となるコンピューターを作成し、DFIR に利用可能な「Tsurugi Linux」を用いた LIVE 起動方法を試行しました。また、起動した「Tsurugi Linux」から保全対象の HDD を確認しました。

次回、実践編では、LIVE 起動した「Tsurugi Linux」へ証拠保全用の USBHDD を接続し、DD コマンド、FTK コマンドを用いて、保全対象の CentOS 9 の HDD をイメージファイルとして保全する手順を学びます（図 2）。なお、本文書で保全に関する全ての手順は網羅していません。詳細については、デジタルフォレンジック協会が発行する「証拠保全ガイドライン」※を参考にしてください。

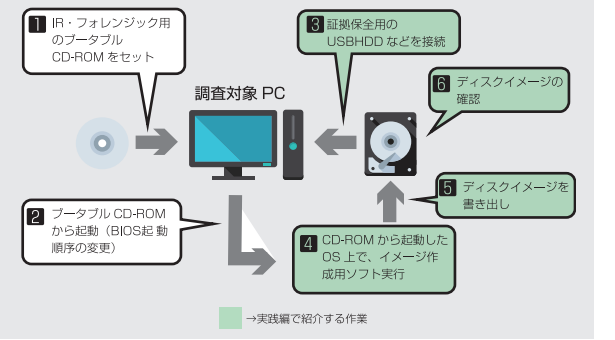


図 2 HDD 保全の工程と実践編で紹介する作業

※ **証拠保全ガイドライン**　https://digitalforensic.jp/wp-content/uploads/2023/02/shokohoznGL9.pdf

Human * IT

人と IT のチカラで、驚きと感動のサービスを。

Hitachi Systems Security Journal VOL.50

株式会社 日立システムズ
本社 〒141-8672 東京都品川区大崎 1-2-1