SHIELD Security Research Center

Hisys Security Journal

VOL.51

HITACHI
Inspire the Next

日立システムズ

Hisys Security Journal VOL.51

TABLE OF CONTENTS

サイバーセキュリティの幅広い領域をカバーをする 社会人向け教育プログラム「SECKUN」とは？
小出 洋 インタビュー …… 3

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 7 月号 …… 7

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！ 2. 実践編 …… 9

●はじめに

本文書は、株式会社日立システムズ 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/

サイバーセキュリティの幅広い領域をカバーする社会人向け教育プログラム「SECKUN」とは?

小出 洋 インタビュー

取材＋文＝谷崎 朋子
編集＝斉藤 健一

九州大学、情報基盤研究開発センターの情報システムセキュリティ研究部門で日々研究に没頭する小出洋教授。IPA 未踏ソフトウェア創造事業スーパークリエータで福岡県警サイバー犯罪対策アドバイザーでもある小出氏は、SECCON やセキュリティ・ティキャンプなどのサイバーセキュリティ人材発掘・育成の取り組みにも積極的に携わり、サイバーセキュリティ教育の最前線で活躍している。その同氏が現在注力するプロジェクトの 1 つが、九州大学の社会人向け教育プログラム「SECKUN（セッククン）」だ。インタビューでは、SECKUN の話を中心に、リカレント教育の意義などについて伺った。

社会人向けプログラム「SECKUN」の必要性と役割

谷崎（以下 T）：小出先生はどのようなきっかけでセキュリティ教育に携わるようになったのでしょうか。

小出（以下 K）：きっかけは、文部科学省の教育プログラム「enPiT」※1 です。当初は学生向けプログラムのみでしたが、のちに社会人のリスキリングやリカレント教育プログラムとして「enPiT-Pro」が開設されました。そのenPiT-Proで情報セキュリティ分野の教育を実施する「enPiT-Pro Security（ProSec）」というプログラムがあり、私が在籍する九州大学は連携校の 1 つです。enPiT 自体には初期の頃から関わっていまして、その頃はビッグデータ・AI 分野のクラウド技術教育を担当していました。より深くセキュリティ教育に携わるようになったのは、九州大学サイバーセキュリティセンターが厚生労働省の教育訓練プログラム開発事業で、のちの「SECKUN」を受託してからです。

T その SECKUN について教えてください。

小出 洋（こいで・ひろし）

1991 年電気通信大学工学部卒業、1993 年同大学院修士課程修了、1997 年同大学院博士課程修了。日本原子力研究所計算科学技術推進センター研究員や九州工業大学情報工学部人工知能工学科准教授などを経て、現在は九州大学教授。情報基盤研究センター 情報システムセキュリティ研究部門、大学院システム情報科学府（知能システム学専攻）、工学部 電気情報工学科（サイバーセキュリティ・プログラミング・並列分散処理）などを担当する。

プログラミングと天体観測と真空管が好き。未踏スーパークリエータでもある。SECCON やセキュリティ・ティキャンプなどのサイバーセキュリティ人材発掘・育成の取り組みにも積極的に携わっている。

※ 1 **enPiT** 成長分野を支える情報技術人材の育成拠点の形成。情報技術を高度に活用しながら社会課題を解決できる高度 IT 人材の育成機能強化を目的に始まったプログラム。ビッグデータ・AI、セキュリティ、組み込みシステム、ビジネスシステムデザインの 4 つの分野を主軸に、産学官共同で推進。

K SECKUN は、今年度で 4 回目を迎えます。テーマごとに講義を分類したモデルコースを選択する形式で、コースあたり平均 100 時間。土日を中心に開講されるので、受講期間は半年から 1 年くらいとなります。基本はオンラインですが、演習によってはオンサイトとのハイブリッドで行われるものもあります。受講生数は、初年度の令和 2 年（2020 年度）は厚生労働省の予算があったので無料開講し、82 名が集まり、67 名が修了しました。令和 3 年度（2021 年度）の 2 期生は、複数のコースを受講した方がいたので延べ 57 名。令和 4 年度（2022 年度）も同様で、延べ 59 名が受講しました。

T コース名を見ると、例えば令和 4 年度（2022 年度）では、「Human Element コース」「ビジネスイノベーションコース」「クライシスマネジメントコース」「リーガルエキスパートコース」「ProSec-IT-NEXT コース」と、技術系というよりはマネジメント系の科目が多い印象を受けます。

K ProSec-IT コースは大学院の履修科目として用意した技術寄りのコースですが、残りは法制度やセキュリティ心理学やルール形成戦略、机上演習、地政学・インテリジェンスなど、技術にとどまらない内容となっています。教育コンテンツを作成するとき、JNSA や日立システムズなどの IT 業界関係者や大学の先生方に検討委員として参加いただき、共に議論を深めました。その結果、コンテンツは技術だけでなく、法律、ヒューマンファクター、ビジネスなどの領域も網羅するという方向性でまとまりました。サイバーセキュリティは今やビジネス全体に影響を与える課題です。技術的な対策だけでなく、個人情報の取り扱いや法制度の遵守、インシデント発生時における組織としての対応方法といったソフト面での対策も講じる必要があります。つまり、技術者側は情報技術の知識のみならず、法律やビジネス戦略、リスク管理などの領域も知っておかなければならないということです。逆も然りで、IT 以外の領域の業務でもサイバーセキュリティ対策の観点を取り入れることは重要です。

T これまで大学・大学院の教育機関や enPiT などの取り組みでは求められるコンテンツがなかったということでしょうか。

K もちろん大学・大学院や enPiT でも良質かつ深い教育コンテンツが提供されています。しかし、あくまでも学術研究としての専門性を追求する内容であり、最新動向を取り入れた、実務に直結する実践的な内容とは方向性が異なります。そこを補完できるのが、SECKUN です。

T 社会人向けプログラムだというところも、コンテンツの違いがありそうです。

K 企業が求めるのは、自社の事業や業務を理解し、何を守るべきか、業務環境の安全性や事業継続性はどう担保するのかといった問題意識を明確に持ち、その上で情報システムの安全性を高める施策が打てるサイバーセキュリティ人材です。こうした問題意識や視点は、社会に出て実務を経験する中で生まれてくるものです。そういう意味で、学生に新しいことを覚えさせれば良いという既存の育成論では、人材不足はいつまでたっても解消されません。社会に出て働く中で課題に直面し、今の自分の知識だけでは解決が難しいと悩んだとき、その学びの受け皿として SECKUN のような社会人向けプログラムがあるのだと考えています。

演習中心の講義を支える実務経験豊富な講師陣

T 講師にはどのような方を迎えていらっしゃるのでしょうか。

K 専門分野の知見だけでなく、サイバーセキュリティと絡めた応用領域で実績のある方に講師の打診をしています。例えば、サイバーセキュリティ関連の裁判に関わったことがある裁判官や弁護士、サイバーセキュリティ基本法の策定に携わった議員といった具合です。

T 司法や立法の専門家で、かつサイバーセキュリティにも詳しい方は限られますから、そうした方々の講義は本当に貴重だと思います。

K もう 1 つは、演習中心に講義を組み立てられる方です。座学や教材ベースの学習はインターネット上でいくらでも見つかりますが、演習はなかなかありません。受講生も演習を希望する声が多く、大学の授業をそのまま展開したオンライン講座は、たとえ内容が良質であっても、受講生の集まり方が鈍い傾向にあります。

T 演習は環境の準備や内容の組み立てが大変なの

小出氏とのインタビューは、本年７月上旬にオンラインにて行われた

で、座学が増えるのもわかります。

K 例えばアーキテクチャや CPU の脆弱性を研究する大学の先生であれば、サイバー攻撃や防御を研究するための演習環境のようなものをすでに構築しています。そうした方に協力いただくことで、まさに最先端の演習環境で学べるというわけです。私も ProSec-IT コースで、ムービングターゲットディフェンスの最先端の研究成果などを教えています。ムービングターゲットディフェンスは、システムなどのパラメーターを動的に変化させることで攻撃されづらくする手法のことで、演習を交えて仕組みを学べるよう講義を作っています。こうした演習が、実務での応用やグローバルでの新規事業の開拓などを考えるきっかけになると嬉しいですね。

受講生が自発的に宣伝大使に
仲間同士のつながりも拡大中

T 受講者はどんな方がいらっしゃるのでしょうか。

K 全国各地から参加いただいており、30 ～ 40 代の方が多いです。ProSec-IT コースは単位がとれることもあって、九州大学の 20 代の大学院生が多くいます。これから就職や進学を考える学生たちが、社会人の技術系エンジニアなどとコミュニケーションをとれる場にもなっており、キャリアパスを考える良いきっかけになっていると感じます。

T 受講生の方々は、修了後に学びをどのように活かされているのでしょうか。

K 修了生からは、IT ベンチャーへの転職に成功した、CISO に抜擢された、社内のサイバーセキュリティ部門へ異動できたといった話を聞きます。福岡県警や佐賀県警の方も講座を受講しているのですが、サイバー犯罪対策の専門部署に異動した受講生もいるようです。

T リスキリングの成功事例ですね。

K あと、SECKUN の特徴とも言えるのが、リピーターが多いことです。例えば去年はクライシスマネジメントコースを受講したので、今年はリーガルエキスパートコースを受講するといったように、毎年受講する強者もいるほどです（笑）。

T すごいですね（笑）。他にはない、魅力的で満足度の高い講義が多いということなのでしょうね。

K おかげさまで、受講生の方々は「セキュリティ業界の 3 大温泉シンポジウム」※2 や SECCON、CODE BLUE などに参加した際に、SECKUN を積極的に宣伝してくれているようです。講師を引き受けていただいている AWS の松本照吾氏は元 SECKUN 受講生なのですが、「イベントで勝手に紹介してお

※2 **3 大温泉シンポジウム**：和歌山・白浜町の「サイバー犯罪に関する白浜シンポジウム」、新潟・越後町の「情報セキュリティワークショップ in 越後湯沢」、愛媛・松山市の「サイバーセキュリティシンポジウム道後」

いたよ」と言われました。非常にありがたいことです。

T 能動的に活動される方が多いのですね。

K そういえば CISSP の CPE ポイントなどについて、特に SECKUN で申請を代行しているわけではないのですが、受講生から「申請したら通った」と言われました（笑）。

T コミュニティも自主的に作られていそうです。

K はい。主催者側が用意しているのは、終業式に開催するシンポジウムくらいです。あとは、受講者による自主的な活動にお任せしています。実際、横のつながりを求めて受講される方は多いです。単発のセミナーやイベントではコミュニケーションの機会を作るのが難しいですが、SECKUN は長期間の講義や演習をともにすることでつながりを持つことができます。連絡先を交換し、コース終了後も連絡を取り合っている方は多いようです。また、オンサイト講義のあとに講師を交えて飲み会を開いたという話も聞きました。昨年度は大阪のセキュリティコミュニティと一緒にオンサイト講義を実施したところもあり、横のつながりがどんどん作られているようです。

2023 年度の出願開始！
10 月 1 日開講予定 !!

T 今年度の新規受講生募集は始まっているのでしょうか。

K はい。出願期間は 9 月 11 日までで、10 月 1 日に開講予定です。本年度はモデルコースを 5 つ用意し、他コースの講義を 1 コースあたり 15 時間まで受講可能になりました。受講中のコース以外の講義が気になるという声は以前からあって、ようやく要望に応えられるようになりました。受講料は 1 コース 50 時間程度で 6 万円、ProSec-IT コースは 120 時間で 12 万円という料金設定にしています。

T 業界関係者であれば、最先端かつ高度な内容を取り上げながらこの受講料は良心的すぎると驚きますね。ちなみに、ProSec-IT コースは社会人でも受講できるのでしょうか。

K 以前は受講に大学の卒業証明書や成績証明書などが必須でしたが、厚生労働省のプロジェクト期間が終了したこともあり、ProSec-IT の主要な技術演習科目を大学卒業資格なしで受講できるコースを 2022 年度に新設しました。2023 年度は、ProSec-IT-SECKUN コースとして選択できます。

T 最後に、SECKUN の受講を迷っている人にメッセージをお願いします。

K 社会人向けの講座って、ギブアンドテイクが成り立つんですよね。自分には技術力がないから不安と思う方も、他の人から見れば他領域の知見や専門性を持った人物です。自分では当たり前にできることも、アウトプットしてみると他の人にとって価値ある情報になることもある。だから、悩むくらいなら一歩踏み出して参加してみてはいかがでしょうか。講義のレベル感を知りたければ、SECKUN 第 1 期生が開発した教材が厚生労働省のホームページで公開されているので、参照してみてください※3。また、SECKUN は講義の見学が可能で、気に入ったら途中参加することもできます。まずは気になる講義を見学するところから始めるのはいかがでしょうか。問い合わせ先からご相談も受け付けています。参加をお待ちしています。

T 改めて素晴らしい取り組みと感じました。お話いただき、ありがとうございます。

※ 3 https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/jinzaikaihatsu/program_development.html
上記ページの「6.　情報システムを守る高度なサイバーセキュリティ技術に関する教育訓練プログラム」で参照

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 7月号

文＝ SHIELD Security Research Center

共通脆弱性評価システム CVSS の現状とこれから

【概要】

ソフトウェアの脆弱性の特性と重大度を伝達するためのオープンフレームワークとして、共通脆弱性評価システム CVSS（Common Vulnerability Scoring System）がある。現在業界標準として利用されているのは CVSS バージョン 3.1 であるが、2023 年 9 月には CVSS バージョン 4.0 が正式リリースされる。そこで本稿では CVSS の作成された背景や今後の実装について概説する。

【内容】

現在の脆弱性対策の仕組みは、2001 年 9 月 11 日の米同時多発テロ事件を契機に、米政府が 2002 年に電子政府法の一環として連邦情報セキュリティ管理法を成立させた事に端を発している。

脆弱性を定義し、それぞれに固有の番号を付与する辞書である CVE（Common Vulnerabilities and Exposures）は、CVSS よりも早い、1999 年に誕生した。それ以前は、同じ脆弱性であってもベンダーごとに異なる名称を付けており、脆弱性情報の共有が困難であった。しかし、CVE の導入により異なるベンダーの脆弱性情報であっても統一的に扱えるようになった。

脆弱性情報における次の課題は、特性の共通化であった。2005 年には、ソフトウェアの脆弱性の特性と重大度を伝達するためのオープンフレームワークとして CVSS が定義された。現在では脆弱性の指標として CVSS 以外の観点から作成された指標も出てきているが CVSS は依然として業界標準である。

CVSS は①基本評価、②現状評価、③環境評価の 3 つの評価基準で構成される（図 1）。①基本評価は脆弱性そのものの特性（システムの機密性、完全性、可用性に対する影響）を評価する。②現状評価は脆弱性の現在の重大度（攻撃コードの存在や対策情報の有無など）を評価する。この 2 つの基準は主に製品ベンダー・セキュリティベンダーや組織が評価を行う。③環境評価はユーザーが各自の利用環境や使用状況も含め、最終的な脆弱性の重大度を評価する。この 3 つの評価を含めて最終的な CVSS の評価値が得られる。

現在、主流となっている CVSS は 2019 年に定義されたバージョン 3.1 であるが、近年では、評価指標が不足している部分も出てきている。例えば、近年拡大している IoT 環境における課題として、人命に対する影響やセーフティに関する明確な評価指標がないことが挙げられている。これを受け、CVSS は新バージョンであるバージョン 4.0 が 2023 年 9 月に正式リリース予定となっている（図 2）。

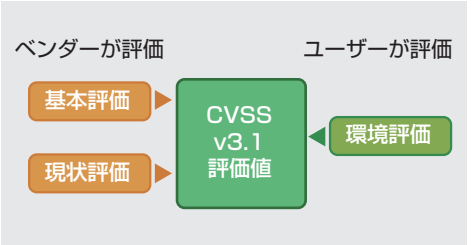


図 1 CVSS 3.1 評価値を構成する基準

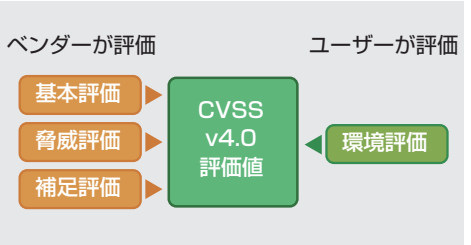


図 2 CVSS 4.0 評価値を構成する基準

CVSS バージョン 4.0 では、攻撃が自動化可能か否か、攻撃からの回復の難易度、攻撃者が一度に悪用できるリソースの密度、ユーザーの特定の操作が必要か否か、安全性に関する項目などが追加される予定である。評価基準も、現在の 3 種類から、基本評価、環境評価、脅威評価、補足評価の 4 種類に変更されるなど大幅な変更が予定されている。これにより、脆弱性の評価が厳格に行われる一方で、対象システムの環境や構成に合わせた複雑な対応作業が必要となり、作業コストの増加が考えられる。

CVSS バージョン 4.0 がリリースされたとしても、必ずしも即時採用されるとは限らない。現在、脆弱性情報の提供は公開から 10 年以上経つバージョン 2.0 も併記されていることが多いが、徐々にバージョン 3.1 のみの提供になりつつある。利用するバージョンの選択には CVSS の活用目的と各バージョンのメリット・デメリット（表）とを照らし合わせて採用するとよいだろう。

表 CVSS のバージョンとそれぞれのメリット・デメリット

バージョン	メリット	デメリット
CVSS2.0	簡易性が高い	評価に現実との乖離
CVSS3.1	詳細な評価が可能	専門知識要、IT のみ適用
CVSS4.0	適用範囲が拡大	専門知識要、コスト増

【情報源】

https://www.first.org/cvss/v4.0/specification-document
https://www.jpcert.or.jp/present/2010/20100125_IPA_Terada-sama.pdf

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！

2. 実践編

文＝ SHIELD Security Research Center

はじめに

前号より、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」が開始となりました。企画第一弾として「HDD 保全」を学びます。マルウェアなどの感染が認められ、後の解析のために HDD の現状保全が必要となる場面などで使われています。

前号は「準備編」として、保全を行う対象の作成や保全対象 HDD の確認などを行いました（図 1 ❶～❷）。今号は「実践編」として、保全対象 HDD をイメージファイルとして実践に保全します（図 1 ❸～❺）。

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。

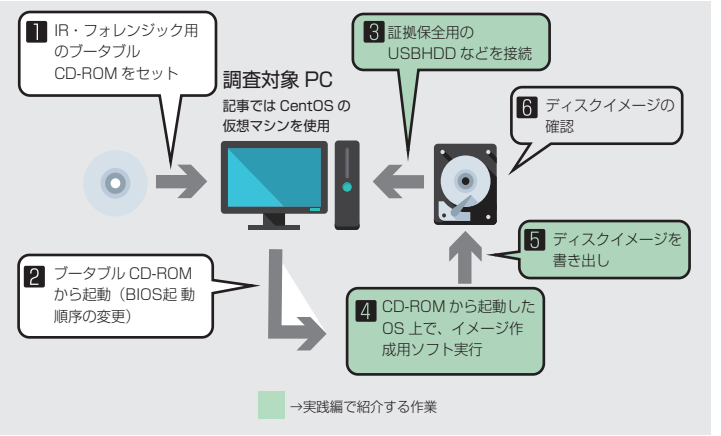


図 1 HDD 保全の工程と実践編で紹介する作業

証拠保全用の USB HDD などを接続

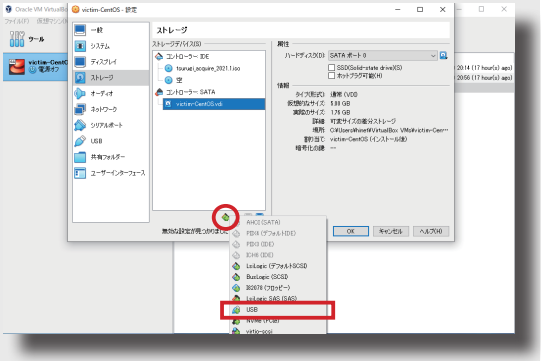
HDD の保全を行うためには、まず、HDD サイズを確認します。そして、保全対象の HDD と同じサイズ以上の外付け HDD などのリムーバブルメディアを準備します。

● VirtualBox での USB ディスクの追加

ここでは「準備編」で作成した保全対象の CentOS9（HDD:5GB）を保全するために必要なリムーバルメディアを仮想的に準備します。

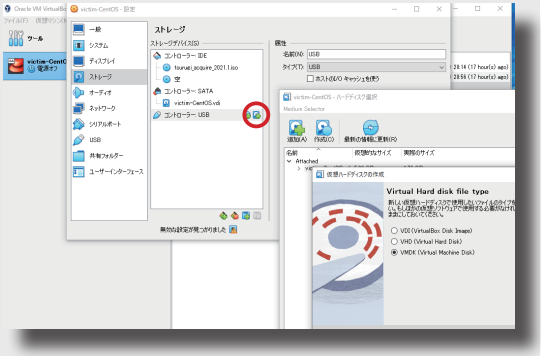
① USB コントローラーの追加

仮想マシン (CentOS9) を選択し、[設定] → [ストレージ] を選択します。枠で囲ったコントローラーの追加ボタンより、USB を追加します。ストレージデバイスに「コントローラー：USB」が追加されます。



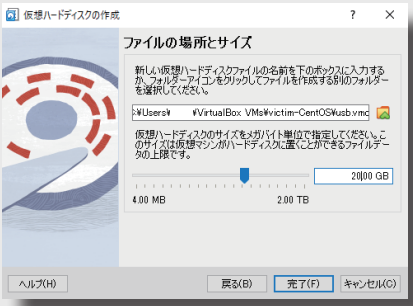
②仮想 HDD の追加

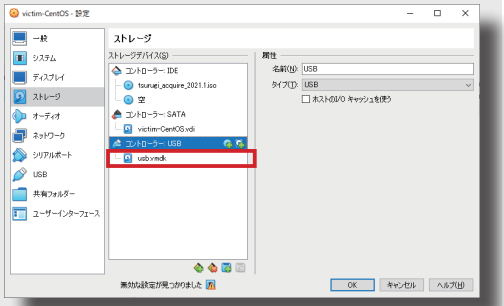
「コントローラー：USB」に HDD を接続します。枠で囲ったボタンを押下したのちに、作成ボタンを押下します。これにより、仮想ハードディスクの作成ウインドウが起動します。



③仮想 HDD の作成

基本的な設定は初期設定のままで構いませんが、HDD サイズを 20GB 程度設定し、完了ボタンを押下してください。なお、今回ファイルタイプとして、VMDK を指定していますが、何を指定しても構いません。これにより、当該 CentOS のマシンに USB HDD(20GB) が接続された状態となります。





● USB HDD のフォーマット

ここでは、保全対象機器（CentOS9）に接続した USB HDD をフォーマットしていきます。
まず、準備編と同様の手順で「Tsurugi Linux」を起動します。

① USB HDD の認識状況の確認

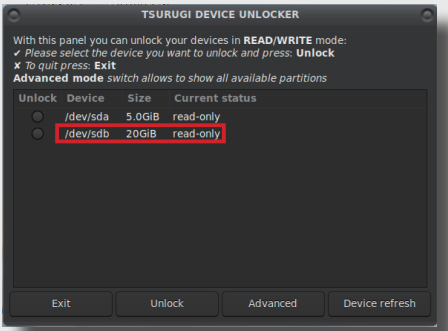
起動が完了しましたらターミナルを立ち上げて下記のコマンドで USB HDD の認識状況を確認します。すると、図のように、/dev/sdb として、20GB の HDD が認識されていることが確認できます。

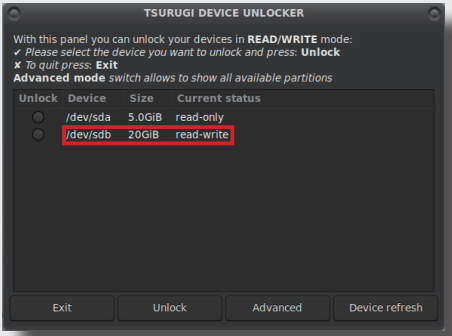
```
# fdisk -l
```

```
Disk /dev/sdb: 20 GiB, 21474836480 bytes, 41943040 sectors
Disk model: HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

② read-only モードのアンロック

parted コマンドでパーティションを作成したいのですが、「Tsurugi Linux」を利用している場合、すぐにパーティションを作成できません。この理由は、「Tsurugi Linux」が外部ディスクをすべて read-only モードでロックしているためです。これは、データの改ざん保護といった意味では有効な機能ですが、保全作業もできません。そこで、今回は、/dev/sdb の read-write モードとしてアンロックします。
デスクトップ上の「TSURUGI DEVICE UNLOCKER」を起動します。
/dev/sdb が read-only であることが確認できますので、/dev/sdb にチェックを入れ、Unlock ボタンを押下します。実行後、/dev/sdb が read-write モードであることを確認してください。





③パーティションの作成

parted コマンドでパーティションを作成します。
パーティション作成コマンドは以下の通りです。ここで、mklabel コマンドで「gpt」を指定していますが、名称は任意のもので構いません。実行後、Partition Table に　gpt がセットされたことを確認します。

```
# parted /dev/sdb
(略)
(parted) mklael gpt
(略)
(parted) p
```

```
(parted) p
Model: VBOX HARDDISK (scsi)
Disk /dev/sdb: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start  End  Size  File system  Name  Flags
```

③フォーマット（ext2）

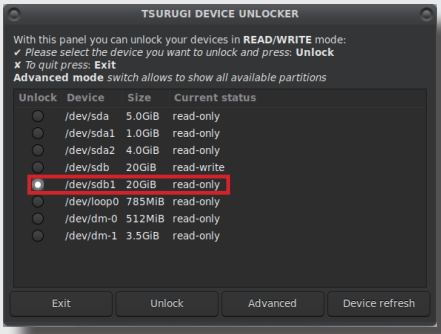
mkpart コマンドを用いて、フォーマットします。ここでは、Start 0%、End100%を指定し、全体を ext2 でフォーマットします。今回は、フォーマットが完了後、/dev/sdb1 として認識されました。なお、ext2 を選択したのは、先に利用した parted コマンドが exFAT に対応していないためです。次の工程で exFAT で再フォーマットします。

```
(parted) mkpart
Partition name?  []?
File system type?  [ext2]?
Start? 0%
End? 100%
(parted) p
Model: VBOX HARDDISK (scsi)
Disk /dev/sdb: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system  Name  Flags
 1      1049kB  21.5GB  21.5GB  ext2
```

④ read-only モードのアンロック

デスクトップ上の「TSURUGI DEVICE UNLOCKER」を起動して、/dev/sdb1 にチェックし、Unlock ボタンを押下します。



⑤フォーマット（exFAT）
/dev/sdb1 を exFAT でフォーマットします。

```
# mkfs.exfat /dev/sdb1
```

⑥マウントと状況の確認
保全先としてマウントします。

```
# mkdir /media/usbhdd
# mount /dev/sdb1 /media/usbhdd
```

最後にディスクのマウント状況を確認します。コマンド実行結果に、/dev/sdb1 on /media/usbhdd の記述があれば、保全先の準備は完了です。

```
# mount
```

```
/dev/sdb1 on /media/usbhdd type fuseblk (rw,nosuid,nodev,relatime,user_id=0,grou
p_id=0,default_permissions,allow_other,blksize=4096)
root@acquire:~#
```

CD - ROM から起動した OS 上で イメージ作成用ソフト実行

次に、HDD の保全作業を実施します。HDD の保全作業には、物理的に同じ HDD にコピーする方法などもありますが、今回は、「Tsurugi Linux」に収録されているコマンドを用いて、イメージファイルを作成します。イメージファイルとは、記録されたデータを、ファイルやフォルダ構造を保ったまま複製・保存したデータファイルのことです。

● dd コマンドを使ったコピー
dd コマンドを使って､イメージファイルを作成します。dd コマンドはファイルを指定されたブロックサイズでコピーします。cp コマンドは、ファイルをコピーするだけですが dd コマンドは、デバイスからデバイスへコピーしたりすることができます。dd のコマンド利用例は下記の通りです。

```
# dd if=[ 入力 ] of=[ 出力 ] bs=[ ブロックサイズ ]
または
# dd if=[ 入力 ] bs=[ ブロックサイズ ] > [ 出力 ]
```

記事では、以下のように入力して実行しています。conv オプションのパラメーターとして noerror（不良セクタによるエラーがあってもコピーを継続）と、sync（エラーの分を 0 パディング）を指定しています。なお、このコマンドの完了までにはかなりの時間がかかります。

```
# dd if=/dev/mapper/cs-root of=/media/usbhdd/victim-CentOS-root.dd
bs=64k conv=sync,noerror
```

● FTK Imager を用いたイメージファイルの作成

FTK Imager を用いた、イメージファイルの作成を実施します。FTK Imager は、Exterro 社 (旧：AccessData 社) が権利を保有するフォレンジックツールです※。
さまざまなフォレンジック機能がありますが、今回は、この FTK Imager を使ってイメージファイルの作成も体験します。FTK Imager のコマンド利用例は下記の通りです。詳細はコマンドのヘルプを参照してください。

```
# ftkimager 入力 [ 出力 ] [Option]
```

記事では、以下のように入力して実行しています。なお、コマンドの完了までにはかなりの時間がかかります。

```
# ftkimager /dev/mapper/cs-root /media/usbhdd/ftk-victim-CentOS-root.img
```

●取得イメージファイルの存在確認

最後に、今回取得したイメージデータ「victim-CentOS-root.dd」「ftk-victim-CentOS-root.img(.001)」のファイル存在、ファイルサイズが同じであることを確認してください。

```
root@acquire:/media/usbhdd# ls -la
total 10997824
drwxrwxrwx 1 root root      32768 Jan  1  1970 .
drwxr-xr-x 1 root root         60 May 15 06:54 ..
-rwxrwxrwx 1 root root 3753902080 May 11 09:46 ftk-victim-CentOS-root.img.001
-rwxrwxrwx 1 root root        599 May 11 09:46 ftk-victim-CentOS-root.img.001.tx
t
-rwxrwxrwx 1 root root 3753902080 May 11 08:33 victim-CentOS-root.dd
```

ここで、イメージデータの中身を確認したいところですが、このタイミングで実施することはやめておきます。その理由については、次回ご説明させていただきます。

おわりに

今回は、Live 起動した「Tsurugi Linux」へ証拠保全用の USB HDD を接続し、dd コマンド、ftkimager 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した。

次回は、USB HDD が接続できない環境の場合に、ネットワーク越しにイメージファイルを取得する手順を実践します。また、取得したイメージファイルの確認、確認の際の注意点を確認します。

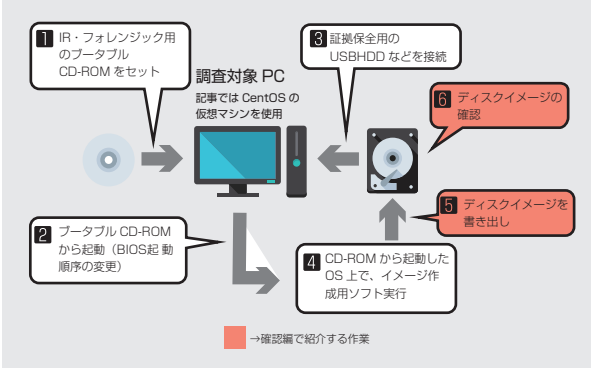


図 2 HDD 保全の工程と確認編で紹介する作業

※ https://www.exterro.com/forensic-toolkit