SHIELD Security Research Center

Hisys Security Journal

VOL.52

HITACHI
Inspire the Next

日立システムズ

Hisys Security Journal VOL.52

TABLE OF CONTENTS

超巨大組織が取り組むセキュリティ対策とガバナンス強化
村山 厚 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 2023.08 …… 8

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！ 3. 確認編 …… 10

●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/

Human * IT

超巨大組織が取り組むセキュリティ対策とガバナンス強化

村山 厚 インタビュー

日立製作所 情報セキュリティリスク統括本部 副統括本部長

取材＋文＋撮影＝斉藤健一

グローバルでの従業員数は約 37 万人、連結子会社も 853 社という日立グループ。この超巨大組織はセキュリティ対策やガバナンスにどのように取り組んでいるのだろうか。今回は日立製作所 情報セキュリティリスク統括本部 副統括本部長の村山厚氏に話を伺った。同社ではセキュリティ対策の取り組みを外部に向けて公開しているが、今回のインタビューは、公開情報の行間が垣間見える一歩踏み込んだものとなっている。

2000 年代初頭から続く セキュリティとの関わり

斉藤（以下 S ）：まず経歴を簡単に教えてください。

村山（以下 M ）：1986 年、日立情報システムズ（現日立システムズ）の前身である日立情報ネットワークに入社し、その後、2006 年に日立製作所へ転属しました。日立情報ネットワークでは、ネットワークの仕事に従事していました。主に内線電話網やデータ交換網などの設計を行ったり、そうした設備を工場に導入したりするなどの仕事を 14 ～ 15 年ほど続けていました。

S セキュリティと関わるようになったきっかけは何でしたか。

M 2001 年に相次ぎ登場して世間を騒がせた Code Red II ※1 や Nimda ※2 といったインターネットワームがきっかけです。われわれも大きな損害を被りました。当時、ビジネスでのインターネットへの依存は現在ほど高くなく、社内では専用線を引いていました。ところが、各所がワームに感染した影響で帯域が逼迫し、ほとんどのネットワークが麻痺して使えなくなるという状況に陥りました。こうした時期にセキュリティを担当することとなったのです。Nimda が登場したのは、Code Red II の 1 ヵ月後だったのですが、こちらも感染を防ぐことはできず、何日も対応に追われることになったのを覚えています。当時は感染の端緒もわかりませんでしたし、ウイルス・ワームとはどんなものか、というところから始まりました。再発防止策の検討や従業員の啓発、定常的なセキュリティパッチの適用など、すべてをゼロから始めました。

S 日立製作所のインシデントレスポンスチーム HIRT（ハート）に関わるようになったのはいつ頃ですか。

M その後の事です。当時、HIRT はすでに発足していましたが、社内チームとの連携が活発ではありませんでした。しかし、社内のインシデントとあわせて HIRT を活性化していきたいという考えから、日立製作所に在籍し、HIRT 発足に携わった寺田真敏氏（現 東京電機大学教授）と積極的に連携するようになりました。HIRT が FIRST（the

※1 **Code Red II（コードレッド 2）**：2001 年 7 月に大流行したネットワークワーム。それ以前に流行した Code Red と同様に Microsoft の IIS サーバーの脆弱性を利用して感染を広げるが、Code Red と Code Red II はプログラムとしては全くの別物。

※2 **Nimda（ニムダ）**：2001 年 9 月に感染を広げたネットワークワームで、ファイルに感染するコンピューターウイルスでもある。名称は「admin」を逆から綴ったもの。Windows の脆弱性や Code Red などのワームによるバックドアを利用など、複数の感染方法があり、短期間にインターネットへの感染が広まった。

Forum of Incident Response and Security Teams）※3 に加盟した 2005 年の頃のことはよく覚えています。当時から、HIRT は社内の IRT（Incident Response Team）、製品の IRT（現在でいうところの PSIRT）、そして SIer としての IRT という性質を持っていました。寺田氏とは 2000 年代初頭から、組織活性化に向けて尽力してきました。

S 現在は、日立製作所 情報セキュリティリスク統括本部に所属されていると伺っています。この部署は 2017 年の WannaCry 事案の後に発足した部署とのことです。WannaCry 事案に関しては、日立評論の「サイバー攻撃事案の教訓と社内堅牢化の取り組み」※4 という文書で取り上げられています。この文書では、感染の状況・影響範囲・セキュリティ対策・ガバナンスの強化などが、技術面・統括面からまとめられており、大変参考になりました。ちなみに、情報セキュリティリスク統括本部には何名の方が在籍されているのでしょうか。

M 全体で 34 名です。業務範囲としては、情報セキュリティのガバナンス、情報セキュリティ対策だけでなく、個人情報の取り扱いやプライバシーに関わる個人情報データ保護も担当しています。

S「サイバー攻撃事案の教訓と社内堅牢化の取り組み」によると、日立グループの情報セキュリティガバナンスを統括する部署とのことでしたので、予想していた人数よりも少ないと感じました。

M 日立グループのガバナンス構造はピラミッド型であり、われわれが直接統制する範囲はその上部にあたる、それぞれのビジネスユニット（日立では事業ごとに独立した事業計画などを行う）やグループ企業のトップになります。また、それぞれの組織にはセキュリティ責任者が配置され、下部組織の統制を担当しています。人数に関して言えば、前述の 34 名が担当しているのは、各ビジネスユニットやグループ企業のセキュリティ責任者数百名で、これらの責任者が連絡窓口となっている担当者は海外も含むグループ全体で数千名となります。

S ありがとうございます。情報セキュリティのガバナンスについては、後ほどお話を伺いたいと思います。

サイバーレジリエンス強化の取り組み

S 村山さんは以前、「日立社内におけるサイバーレジリエンス強化の取り組み」をテーマに講演されています。また、同テーマの文書が日立評論にも掲載されています※5。今回のインタビューにあたり、この文書を拝見しました。文書の前段では、情報セキュリティ対策の変遷について触れられています。2011 年の標的型攻撃への対応を目的とした境界面の情報窃取対策や、2017 年の WannaCry 事案を受けたシステム破壊対策の強化、そしてセ

村山 厚（むらやま・あつし）

2001 年より日立グループにおける IT セキュリティの実装および日立グループ CSIRT である Hitachi Incident Response Team（HIRT）でサイバーセキュリティインシデント対応業務を担当。その後、情報セキュリティ全般の戦略・マネジメント業務やサイバーセキュリティ対策、監視業務を担当し、2017 年 10 月に情報セキュリティリスク統括本部サイバーセキュリティ技術本部長に就任。現在は同統括本部副統括本部長として情報セキュリティ戦略およびサイバーセキュリティ技術の統括業務に従事。

※ 3 **FIRST（the Forum of Incident Response and Security Teams）**：世界中の CSIRT (Computer Security Incident Response Team) 同士の情報交換やインシデントレスポンス業務の協力関係を構築する目的で 1990 年に設立されたフォーラム。政府機関・民間企業・学術機関をはじめとする、多種多様なセキュリティチームが結集している。

※ 4 **日立評論 2018 vol.100 No.3「サイバー攻撃事案の教訓と社内堅牢化の取り組み」**
https://www.hitachihyoron.com/jp/archive/2010s/2018/03/05b02/index.html

※ 5 **日立評論 2021 vol.103 No.6「日立社内におけるサイバーレジリエンス強化に向けた取り組み」**
https://www.hitachihyoron.com/jp/archive/2020s/2021/06/06b02/index.html

キュリティガバナンスの強化などです。文書の背景には、コロナ禍に伴うリモートワークの導入や働き方の変化が影響しており、それによってネットワークの使用方法が大きく変化していることが挙げられます。今回の取り組みは、過去の重要な取り組みと比較してどのような位置づけになるのでしょうか。

M 業務システムを自組織で開発・運用していた時代には、従来の境界型セキュリティが有効でした。しかし、システムが急速にクラウドに移行していく中、その効果は限定的になってきました。また、人間の心理として「境界のセキュリティが強固だから安全だろう」と考えがちですが、現在のサイバー攻撃の手法を見ると、侵入後のネットワーク内で横展開するものが非常に多くなっています。このような状況を考慮し、従来の境界型セキュリティを包含するハイブリッドなゼロトラストセキュリティ対策の実装を開始しました。

S お話を伺って感じたのは、今回の取り組みが2011年や2017年のものと同様に大きな役割を果たしているということです。また、文書の方は、セキュリティ対策の取り組みに『統制』『協創』『自分ゴト化』という新たな視点を取り入れたことがとても印象的でした。それぞれの要素を見ていくと、『統制』ではゼロトラストセキュリティを実現する上で重要な要素である「認証」「エンドポイントのセキュリティ」「サイバー統合監視」の強化が挙げられています。『協創』については日立グループにおいても使われていると認識しています。この言葉について簡単に説明していただけますか。

M セキュリティ活動における『協創』は、社内だけでなく、社外の各分野とセキュリティエコシステムを共に創出するということで考えています。2017年のWannaCryの事案を経験してわかったことは、セキュリティはIT部門のみの課題ではなく、広報・法務・渉外などの多岐にわたる部署との情報共有や連携が不可欠であるということです。これは、日立グループの内部に限らず、国や他の企業を始めとしたさまざまな社会組織との関係をしっかり確立することも含まれています。

S 日立評論での文書掲載やセミナーなどで積極的に発表していくことも、外部とつながるという意味では『協創』の一環なのではないかと思いました。

M まさしくそう考えています。セミナーでの講演以外にも、お客様から「日立はセキュリティやガバナンスに対してどのように取り組んでいるのか？」などと質問を受けることがあります。きっかけはWannaCryの事案です。当該事案が発生した際の対応策や遭遇した困難について、可能な限り正直に情報共有するようにしています。こうして情報共有を行った企業は180社ほどになります。

S サイバー攻撃事案という秘匿しておきたい情報をあえて開示したからこそ情報共有の輪が広がったのだと思います。

M『協創』に取り組む背景には、日立が経験した事案を他社には経験してほしくないという思いを強く持っているというのはありますね。

S 次に『自分ゴト化』について伺います。背景にはコロナ禍によって働き方が大きく変化し、テレワークの導入が進む中でのセキュリティ意識の向上があるように思うのですが。

M この取り組みについてはやや話が長くなります。2000年代以降、情報セキュリティの事故にはUSBメモリやノートPCなどの紛失や盗難、あるいは電子メールの誤送信などの、いわゆるヒューマンエラーに起因するものが圧倒的に多かったのです。当時、データの暗号化技術もあまり普及していなかったため、ノートPCを紛失すると、その被害は大きかったのです。

S 確かに。個人情報保護法が施行された2000年代前半から、多くの組織が紛失を公表するようになりました。

M こうした事故が増えると「PC持ち出し禁止」などの「××するべからず」の規則が増えることとなります。当然、セキュリティ対策により業務の進行に制限がかかるため、従業員には不評となります。統計的に見れば、セキュリティ対策のルールを守らずに重大事故につながるケースはほんのわずかですから、従業員の不満も理解できます。とはいえ、事故を起こしてお客様にご迷惑をおかけするリスクを無視するわけにはいきません。

S セキュリティ対策の強化と利便性の低下にどう折り合いをつけるかは難しい問題です。

M「××するべからず」だけでは従業員も納得し

ません。「なぜ禁止するのか」という前段階の理由を周知することが重要だと感じました。これが2008年ごろの話です。

S そこからかなりの時間が経過していますね。

M はい。これまで人員の都合で十分に対応できなかったのですが、メンバーが徐々に増えてきたのを機に、改めて取り組むこととしました。しかし、多くの従業員は「セキュリティは面倒」と感じているため、従来の教育方法やeラーニングなどでは効果が出るとは考えにくいとも思っていました。そこで、まったく別の方向からアプローチしてみようという試みが「自分ゴト化」なのです。

S 具体的にはどのように取り組まれたのですか。

M これまでのeラーニングの教材を見返してみると、一般ユーザーには必要のない深い技術的内容まで解説されているなどがあり、この教材で共感を得るのは難しいと思いました。そこで今回の取り組みでは、意識改革としてセキュリティに興味を持ってもらうことから始めました。Harry（ハリー）というキャラクターを登場させて身の回りのセキュリティを意識してもらうことに努めました。

S キャラクターを使った親しみやすさは大切ですね。

M また行動改革としてGREEN AEGISという社内コミュニティ活動もスタートさせています。こちらはどちらかというと『協創』に近い取り組みで、セキュリティに興味を持った人たちが自発的に集まり、自由に意見交換できる場を提供しています。本来は対面でのイベントなどを行いたかったのですが、コロナ禍でオンライン中心の活動となりました。

S オンラインでは具体的にどのような活動をされたのですか。

M 大規模なリモートイベントも企画しました。セキュリティに興味のない人にも参加してもらおうと、基調講演にはセキュリティの難しい話ではなく、一見するとセキュリティとは無縁に思えるのですが、講演を読み替えると実はセキュリティの話になっているなど、テーマ選びを工夫しました。また、サイバー脅威インテリジェンスの専門家の講演や若手社員によるセキュリティ技術のセッションなども設けました。任意参加ですが800名ほどの参加がありました。

S 文書では簡単にまとめられていた事柄も、実際に話を伺ってみるととても興味深いものだと感じました。

超巨大組織の情報セキュリティガバナンス

S 2022年度の情報になりますが、日立グループの従業員数は約36万8000名で、日本国内が15万7000名、海外が21万1000名。連結子会社数は853社で、国内が157社、海外が696社となっています。この超巨大組織の統制を情報セキュリティリスク統括本部の34名の方々が担当されているわけで、さまざまな苦労があるのではないかと思います。特にグローバルの取り組みについて伺いたいと思います。

M 先ほどお話ししたとおり、情報セキュリティリスク統括本部が担当するのは、日立製作所（以下コーポレート）を頂点とした組織のピラミッド構造の上部にあたる、それぞれのビジネスユニットやグループ企業のトップです。グローバルのガバナンスでは、情報セキュリティエキスパート（以下ISE：Information Security Expert）を各地域（米州・欧州・アジア・中国・インド）に設置して、現地法人のガバナンス強化支援を行っています。

S ISEとはどのような組織なのでしょうか。

M ピラミッド構造の中にはさまざまな会社が含まれています。そこで、ピラミッド構造のタテの指示系統とは別に、現地法人をサポートする部隊がISEです。いわば各地域をヨコ方向からサポートする存在になります。

S 各地域でのISEの人数はどれくらいなのですか。また、日立グループ内に各地域のISEをサポートする部署は存在するのでしょうか。

M ISEは各地域ともに数名です。各地域でセキュリティに特化した人材などによる兼務であり、コーポレート所属となります。したがって、ISEをサポートする部署は存在しませんが、各地域のISE間での連携やセキュリティの情報共有などはコーポレート主体で行っています。

S 地域ごとに仕事のやり方に違いなどありますか。

M やはり地域ごとに異なります。

S 他にもサプライチェーンのガバナンスもあります。こちらについて何かお話いただけることがあればお願いします。

M サプライチェーンを対象としたサイバー攻撃により、工場の生産ラインが停止するなど、グループ全体に影響を及ぼした事例は数多く存在します。サプライチェーンのセキュリティに関する議論は、もはや避けることはできません。セキュリティ対策の実現には多くの課題があることも理解しています。

S 例えばセキュリティ対策の費用などでしょうか。

M それも 1 つの要因ですね。サイバーセキュリティは奥が深いというか、どれだけ対策を講じてもキリがない部分があります。そうした中で、サプライチェーンの企業の方々に対してこちらが親身になって対応していかなくてはならないということです。これはサプライチェーン企業の方々との『協創』とも言えます。

セキュリティ人材育成の取り組み

S 最後にセキュリティ人材育成について、取り組まれていることなどを教えてください。

M サイバーセキュリティの技術分野における人材育成は、長らく取り組んできました。HIRT のメンバーなどもその一例です。加えてもう 1 つ、これも WannaCry の事案がきっかけになっているのですが、現場の中心者としてリーダーシップを発揮できるセキュリティ人材が必要とされています。実際、セキュリティ事故というのは、ビジネスユニットや各社の現場で発生しています。検知は SOC でできたとしても、検知した内容を伝えて理解してもらい、初動対応をお願いするのは現場でセキュリティを取りまとめているメンバーです。そのメンバーが適切に動けないと、事故対応に遅れが生じてしまいます。この観点から、そうした対応ができる人材を育成する必要があると思います。

S 経産省のいう「プラスセキュリティ人材」ですね。

M はい。では具体的に人材育成にどう取り組むかと考えると、生産・製造現場で働く技術者の方にセキュリティを学んでもらうか、IT セキュリティの技術者に生産・製造の現場を学んでもらうかという問題にいきつきます。当然、前者の方が早いわけです。これは生産・製造現場に限りません。エリアごとに即したセキュリティプログラムを作成・配布して人材育成に取り組んでいるところです。

S ありがとうございます。

M 他にも足りないと言われているのが、いわゆる「橋渡し人材」です。セキュリティの技術がわかっていないと話ができませんから、コーポレートだけではなく、各ビジネスユニットやグループ企業にも必要なのです。こうした人材の育成も今後のポイントになると思います。

S 本日はありがとうございました。

【参考資料】情報セキュリティ報告書 2022 https://www.hitachi.co.jp/sustainability/download/pdf/securityreport.pdf

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 2023.08

文＝ SHIELD Security Research Center

ランサムウェアによる名古屋港システム障害について

【概要】

2023 年 7 月 4 日、国内有数の貿易港である名古屋港でランサムウェア攻撃によるシステム障害が発生した。障害発生時は、ターミナルへのコンテナ搬出入作業が停止され、物流にも影響がおよんだ。しかし、障害から復旧までの時間は約 2 日半と名古屋港の BCP（Business Continuity Plan：事業継続計画）の想定内に収まり、当港の災害に対する BCP 対策の堅ろうな体制がうかがえる。各関連機関との連携体制や行動計画をもとに考察する。

【内容】

7 月 4 日、名古屋港のコンテナターミナルで運用されている統一ターミナルシステム（Nagoya United Terminal System 以下 NUTS）でランサムウェアによる障害が発生した。感染したランサムウェアは、ロシアを拠点とするサイバー犯罪集団「Lockbit」によるものとみられている。NUTS は、コンテナ船積卸作業、プランニング、コンテナ保管・搬出管理、ヤード作業管理、保税管理などコンテナターミナルで必要とされる各種業務を効率化するシステムとして採用されている。さらに、このシステムを通じて、各ターミナル内の端末機器や港内のコンテナターミナル、中央管理ゲート、税関や NUTS-Web が連携している。

障害発生当日、協会職員はコンテナ重量の計測機器の不具合をきっかけにシステム障害を認識した。当日の時系列を見ると、障害の把握、外部への情報公開、復旧計画の開示、復旧までの時間は約 2 日半だった（表）。警察庁の統計情報によると、日本国内でランサムウェアによる攻撃を受けた組織の内、復旧を 1 週間以内で実施できた組織は 20%程度である。これと比較すると、NUTS の対応は、多様なシステムと連携しているにも関わらず迅速な対応であったことがわかる。また、名古屋港の BCP には、おおむね 72 時間で応急対応が完了する計画が記載されており、今回の 2 日半での復旧は想定内だったと言える。

なお、ランサムウェアの感染原因は現時点では公表されておらず、5 ヵ所あるターミナル事務所の PC の他、協会に加盟する一部の事業者からマ

表 ランサムウェアによる名古屋港システム障害の時系列

日時		出来事
7 月 4 日	6:30 頃	ランサムウェアによるシステム障害が発生
同日	朝	職員が出社し、システム障害を把握
同日		プリンターから約 100 枚の脅迫文が印刷される
同日		名古屋港におけるコンテナ搬出入の停止発表
7 月 5 日	昼頃	5 日の終日コンテナ搬出入停止を発表
同日	昼過ぎ	ランサムウェア感染を公表
7 月 6 日	7:00	NUTS システムの復旧作業完了
同日	15:00	TCB(飛島コンテナ埠頭株式会社) でコンテナ搬出入再開
同日	17:30	NUCT(名古屋ユナイテッドコンテナターミナル) でコンテナ搬出入再開
同日	18:15	飛島東側の 3 ターミナルでコンテナ搬出入を開始し全面復旧

ルウェアが侵入した可能性もあるとして調査中である。

名古屋港では以前から BCP が綿密に整備され、訓練も実施されていた。同港は日本有数の国際港湾であり、中部圏の経済活動を支えていることから、災害時における機能維持を重視してきた背景がある。

同港の BCP には、各関連機関との連携・協働体制が示されており、官民含めた役割分担も確立されている。また同港では、以前から愛知県警のアドバイスに従い、事前にデータのバックアップも取得していた。バックアップデータを保存していたサーバーからも一部ランサムウェアが検出され、駆除に時間を要したものの復旧は成功した。

県警との連携・協働体制を活かしたことで、身代金を支払わずにシステム復旧できたと言える。また、2022 年 4 月に発足されたサイバー警察局による捜査指導、解析、情報集約・分析、対策などの一元的な所掌を背景に、県警の支援の下、障害の把握から情報開示までの初動対応も迅速に行うことができたと考えられる。

今回の障害はランサムウェア感染によるものであったが、障害発生から復旧までの時間は 2 日半と迅速で、最終的には同港の BCP の想定内での復旧となった。サイバーセキュリティを考える上で災害対策や訓練の重要性を改めて示した事例と言える。

一方、バックアップからの復元には課題があった。BCP の観点から早期復旧には、バックアップのシステム化と定期的なリストアなどの訓練が改めて必要だと言える。

【情報源】

https://www.port-of-nagoya.jp/_res/projects/default_project/_page_/001/001/723/kowanbcp202203.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！

3. 確認編

文＝ SHIELD Security Research Center

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（前々号）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。

第 3 回目となる今回は、「確認編」として、リムーバブルメディアが接続できないなど、ネットワーク越しにイメージファイルを取得する手順と、保全したイメージファイルを確認する方法を学びます（図 1 ❺～❻）。

保全対象の HDD の確認などを行った「準備編」や、保全対象 HDD のイメージファイルをとして実際に保全した「実践編」については、本誌バックナンバーに掲載していますので、必要に応じてご参照ください※。

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。

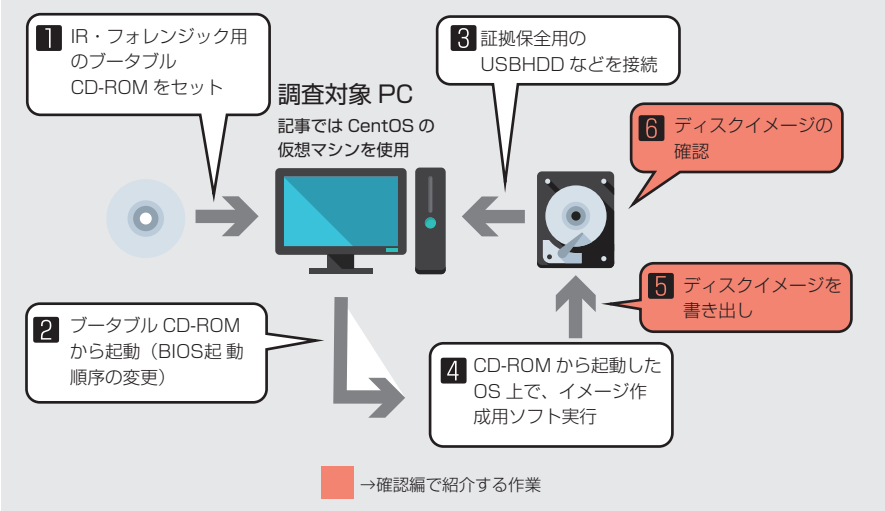


図 1 HDD 保全の工程と確認編で紹介する作業

※ 1 **準備編** https://www.shield.ne.jp/ssrc/document/doc/SSRC-HJ-202306.pdf
確認編 https://www.shield.ne.jp/ssrc/document/doc/SSRC-HJ-202307.pdf

ディスクイメージを書き出し

実践編では、USBメモリなど外部メディアを保全対象PCに接続し、そのUSBメモリなどにddコマンド、FTK Imagerを使って、イメージファイルの取得、保管を行いました。しかし、保全対象がレンタルサーバーなど、USBメモリなどを接続できない場合があります。その場合には、ネットワーク越しにイメージファイルの取得をすることを検討します。

●ネットワーク越しのイメージファイル取得

本稿では、ネットワーク越しのイメージファイル取得の1つとして、nc(netcat)コマンドを活用します。今回は、コンピューターなどの性能を鑑みて、ローカル環境からローカル環境へncを使って試行します。

保全対象CentOSに「Tsurugi Linux」、をセットして、DVDブートを実施してください(準備編を参照)。また、USB HDDを接続して起動してください。「Tsurugi Linux」が起動したら、USB HDDをRead Writeモードに変更し、/media/usbhdd/にマウントしてください(準備編を参照)。

①待ち受けポートと出力ファイルの指定

USB HDDのマウントが終わりましたら、ncでネットワーク越しに送信されるイメージファイルの待ち受けを行います。下記のコマンドを実行してください。

```
# nc -lv -p 12345 | dd of=/media/usbhdd/nc-victim-CentOS-root.dd
```

②待ち受けポートの確認

コマンドを実行しましたら、別のターミナルを起動して、下記のコマンドを実行、ポート12345で待ち受けしていることを確認してください。

```
# netstat -an
```

実行結果は、以下の通りです。

```
root@acquire:~# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:12345           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
tcp6       0      0 ::1:25                  :::*                    LISTEN
udp        0      0 0.0.0.0:68              0.0.0.0:*
```

③入力ファイルとポートの指定

ポート12345で待ち受けしていることを確認したら、以下のコマンドを実行してください。

```
# dd if=/dev/mapper/cs-root bs=64k | nc 127.0.0.1 12345
```

今回はローカル(127.0.0.1)の12345ポートで待ち受けているncへ、ddコマンドで取得したデータを同じくncを使って送信しています。これと同様に、保全データ保管用PCでコマンド①を実行、保全対象PCでコマンド③を実行し、IPアドレスを保全データ保管用PCに指定することで、リモート越しに、イメージファイルの取得が可能となります。なお、リモート越しにイメージファイルの取得を行う際には、ファイアーウオールの設定などアクセス制御を見直すことになりますが、不用意に不特定多数相手にポート開放を行うことがないように注意してください。

ディスクイメージの確認

●保全したイメージファイルのハッシュ値確認

本項では、同一性の検証を目的として、ハッシュ値を確認します。詳細については、デジタルフォレンジック研究会が公開している「証拠保全ガイドライン 第 9 版」6-2-3 同一性検証機能を参照してください※2。

ここでは、証拠保全ガイドラインに記載があるとおり、2 種類のハッシュアルゴリズムを用いて、ハッシュ値を確認していきます。

```
# sha224sum /media/usbhdd/*
# sha256sum /media/usbhdd/*
```

sha224sum の確認結果を以下に示します。sha256sum についても同様にご確認ください。なお、ハッシュ値は、それぞれの環境（取得したデータ）により異なります。

```
root@acquire:~# sha224sum /media/usbhdd/*
f3b726e0c57ec930cbd652f49c985779a02490ab0cad46aec80e5431  /media/usbhdd/ftk-vict
im-CentOS-root.img.001
646073bb9fd8fcaa300e952e4f859a66fc6d2420df92687652289917  /media/usbhdd/ftk-vict
im-CentOS-root.img.001.txt
f3b726e0c57ec930cbd652f49c985779a02490ab0cad46aec80e5431  /media/usbhdd/nc-victi
m-CentOS-root.dd
f3b726e0c57ec930cbd652f49c985779a02490ab0cad46aec80e5431  /media/usbhdd/victim-C
entOS-root.dd
root@acquire:~#
```

●保全したイメージファイルのバックアップ

次に保全したイメージファイルのバックアップを作成します。このあと、保全したイメージファイルの中身を確認しますが、誤って書き込み可能モードでマウントしてしまい、データに変更を加えてしまった際に、即座にバックアップから元に戻すことを目的としています。複数取得しておくことをお勧めします。バックアップが作成できたら、前項と同様にハッシュ値を確認します。

```
# mkdir /media/usbhdd/backup
# cp -a /media/usbhdd/ftk-victim-CentOS-root.img.001 /media/usbhadd/
backup/
```

●保全したイメージファイルの内容確認

①イメージファイルをマウントする

まずは、保全したイメージファイルを確認します。以下のコマンドを実行して、ディスクイメージをマウントします。なお、mount に関する解説は「実践編」で行っていますので、必要に応じて参照してください。

```
# mount -o ro /media/usbhdd/victim-CentOS-root.dd /mnt/virtual2/
```

②ファイルの確認

以下のコマンドを実行して、himitsu.txt の存在 (CentOS9 の HDD である事) を確認してください。

```
# ls - la /mnt/virtual2/root/himitsu/himitsu.txt
```

※ 2 https://digitalforensic.jp/wp-content/uploads/2023/02/shokohoznGL9.pdf2

●保全したイメージファイルの確認失敗の事例

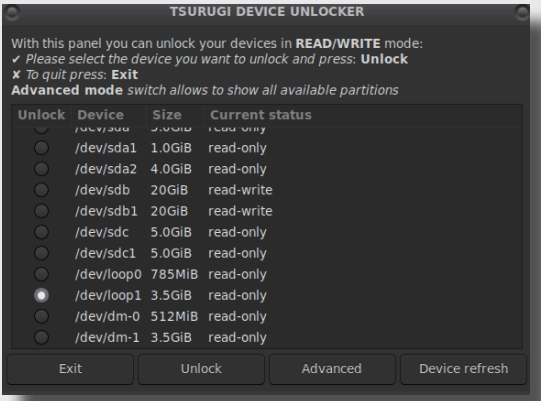
本項では、保全したイメージファイルの確認失敗を体験してみます。
以下のコマンドを実行して、ディスクイメージをマウントしてください。なお、ここではあえて、「-o ro」オプションがないことに注目してください。

```
# mount /media/usbhdd/ftk-victim-CentOS-root.img.001 /mnt/virtual3/
```

マウントしましたら、rw モードでマウントできていることを確認してください。

```
# mount
```

今回の例では、Tsurugi Linux が、loopback device としてマウントするようですので、/dev/loop1 の Unlock が必要となります。
デスクトップ上の「TSURUGI DEVICE UNLOCKER」を起動し、/dev/loop1 にチェックを入れ、Unlock ボタンを押下します。



次に、以下のコマンドを実行してください。

```
# echo test > /mnt/virtual3/root/himitsu/test.txt
# rm /mnt/virtual3/root/himitsu/test.txt
```

このコマンドは、誤ってファイルを作成してしまい、急いで削除したことを想定しています。この時のファイルの状況はどうなるのでしょうか？
以下のコマンドを実行してみてください。

```
# ls -la /media/usbhdd/ftk-victim-CentOS-root.img.001
# sha224sum ftk-victim-CentOS-root.img.001
```

```
root@acquire:~# ls -la /media/usbhdd/ftk-victim-CentOS-root.img.001
-rwxrwxrwx 1 root root 3753902080 May 18 10:42 /media/usbhdd/ftk-victim-CentOS-r
oot.img.001
root@acquire:~# sha224sum /media/usbhdd/ftk-victim-CentOS-root.img.001
9715c71762b25b807491b17152cd9c5a091524fc46a37ddd6c83be78  /media/usbhdd/ftk-vict
im-CentOS-root.img.001
root@acquire:~#
```

イメージファイルのタイムスタンプが変更され、ハッシュ値も変わっていることが分かります。そのため、当該イメージファイルは改ざんされているとみなされるなど、イメージファイルは、正しく保全されたファイルと見なされなくなってしまう可能性があります。
実践編でイメージデータの中身を確認しなかった理由はこのためです。Tsurugi Linux には、誤った変更を防ぐ機能があり問題がないように見えますが、他の OS で作業する際には特に注意が必要です。保全したファイルを閲覧する際には、先にバックアップを取得し、加えて特段の理由がない限りは、リードオンリーモードで閲覧するように心がけましょう (今回は、バックアップが複数あるため戻すことも可能です)。

おわりに

これまで 3 回にわたりお届けした「HDD 保全」はここで終了です。記事では、対象を HDD に限定するなど、保全に必要な作業の一部を紹介したにすぎません。詳細については、デジタルフォレンジック研究会が公開し、本稿 P12 でも参照している「証拠保全ガイドライン 第 9 版」をご覧ください。

次回からは、「Windows システム調査」と題して、Sysinternals Suite を用いた調査手法を解説します。本稿が、みなさんがセキュリティツールに興味を持ち試してみるきっかけになれば幸いです。