5-3　Co-Nexus S: 高度 SOC 人材育成及び国産脅威情報の生成と共有

5-3　Co-Nexus S: Advanced SOC Analyst Training and Generation & Sharing of Threat Information

久保 正樹　神宮 真人　piyokango
KUBO Masaki, JINGU Masato, and PIYOKANGO

NICT では、これまでにサイバー攻撃の観測・解析を行う様々なシステムを研究開発し、それらを運用してきた。サイバーセキュリティ研究室／ CYNEX のサイバー攻撃解析チームでは、アナリストがこれらのシステムを用いて日々観測されるサイバー攻撃の脅威分析及び対処を行うとともに、分析結果を定期レポートやブログ、SNS といったメディアを通じて外部に発信している。また、共同研究先の組織や政府をはじめとするセキュリティ関連組織と脅威情報の共有も行っている。CYNEX では、このような活動に従事するために必要な知識や経験、技術を持つアナリストを「高度 SOC 人材」と位置付け、その育成や成果の共有を推進している。

本稿では、Co-Nexus S において実施する高度 SOC 人材育成及び脅威情報の生成・共有に関する活動を概説する。

At NICT, we have researched, developed, and operated various systems for observing and analyzing cyberattacks. The Analysis Team at the Cybersecurity Laboratory/CYNEX leverages these systems for daily threat analysis and response. We disseminate our findings through regular reports, blogs, and social media. Additionally, we share threat intelligence with partner organizations, government agencies, and other security-related entities. CYNEX identifies analysts with the necessary knowledge, experience, and skills as “advanced SOC analyst” and is committed to their training and the dissemination of their achievements. This paper provides an overview of our efforts in training advanced SOC analyst and generating and sharing threat intelligence within Co-Nexus S.

1　はじめに

NICT ではダークネット分析基盤、ライブネット分析基盤、標的型攻撃基盤、各種セキュリティアプライアンス群、サイバー攻撃統合分析基盤、各種ハニーポットといった様々な分析基盤を保有し、これらの運用を通じて得られたサイバー攻撃に関する各種の実データをアナリストが日々分析し、脅威の検出、インシデント対応に関わる組織と連携した対処支援、結果の共有や情報発信といったセキュリティオペレーションを行っている（図 1）。

サイバー攻撃が増加し、その被害に遭う組織が後を絶たない今日、セキュリティインシデントの未然防止や、攻撃を早期に検知して対処することが求められている。そのためには、脅威インテリジェンス、あるいは脅威情報と呼ばれるサイバー攻撃情報を対策に活用することが重要である。

脅威インテリジェンスの一部として IoC 情報（Indicator of Compromise）と呼ばれるものがある。IoC 情報とは、観測されたサイバー攻撃通信の送信元の IP アドレス、マルウェアなどの不正プログラムによる攻撃の被害を受けたコンピュータが攻撃者からの指令を受ける先の IP アドレス、攻撃に悪用された不正プログラムから生成したハッシュ値など、侵害の痕跡を示唆する情報である。これらの情報は、ファイアウォールをはじめとするセキュリティ対策製品に遮断対象リストとして直接利用できることから、サイバー攻撃対策に広く利用されている。

攻撃を検知した組織やセキュリティベンダが早期に他の組織と情報を共有することで、これらの情報は更に広く利用可能になる。対策を必要とする他の組織がこの情報を活用することで初めて情報共有に意味が生まれる。

このように、脅威インテリジェンスにおいては、情報の共有と活用によってその価値が見出される。

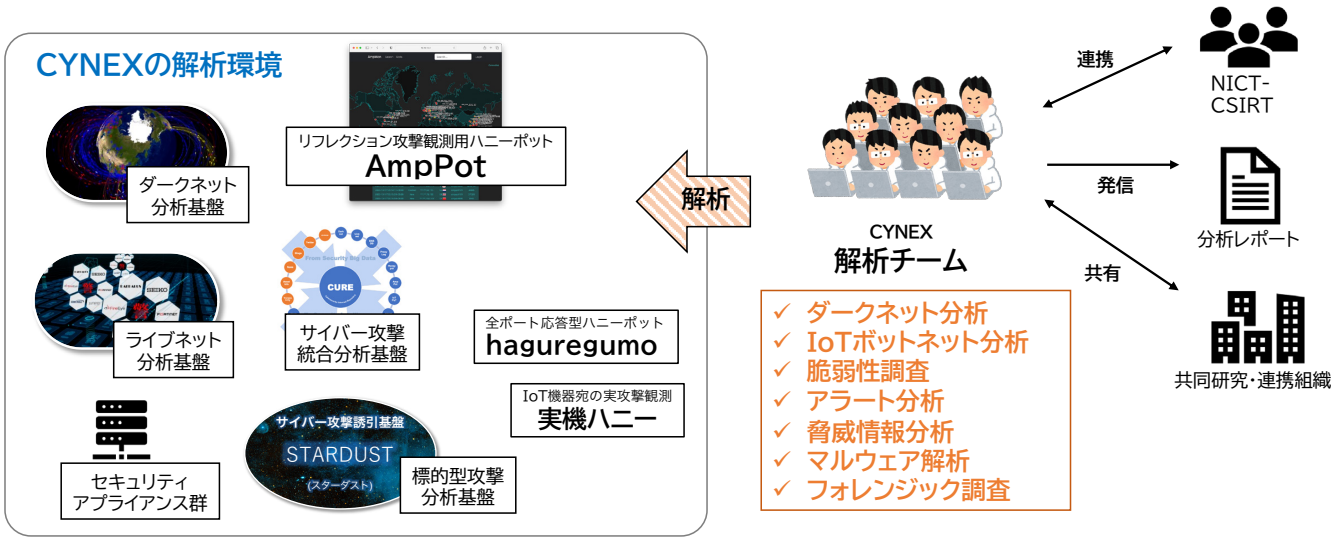


図 1　CYNEX 解析チームのオペレーション

コース名		期間	内容
オンラインコース		半年	• Infinity Chamberによるオンライン自己学習 • 学習した知識を使った調査実施(解析チームでサポート) • 成果発表
OJT	ダークネット分析コース	1,2年～	• ダークネット分析の概要説明 • 攻撃通信に関する各種分析 • 分析アプローチの検討と分析実施 • 成果発表
	ライブネット分析コース		• ライブネットオペレーションの概要説明 • 機構内セキュリティオペレーション • 分析アプローチの検討と分析実施 • 成果発表
	アーティファクト分析コース		• マルウェア解析の概要説明 • 解析環境構築 • マルウェアの表層/動的/静的解析 • 成果発表

図 2　Co-Nexus S 高度 SOC 人材育成プログラムのコース概要

図 3　Co-Nexus S 受講の流れ

サイバー攻撃は、国や地域を問わず世界全体で発生するグローバルな問題であるが、攻撃の傾向は地理的要因や政治経済状況、企業の規模や業種といった特性によって異なる。そのため、日本で有効なセキュリティ対策を検討するには、日本という国及び日本の各業種において観測されるリアルなサイバー攻撃の実データに基づく分析が必要であり、分析結果の共有と活用を進める必要がある。

グローバルにサイバーセキュリティのソリューションを提供するベンダが提供する脅威情報だけに頼るのではなく、日本国内で多くの組織が自ら攻撃観測や分析、脅威情報の発信や共有を行うことが重要である。さらに、得られた知見を持ち寄り、対策技術を開発できる好循環を作ることが求められる。

Co-Nexus S では、NICT において実施しているセキュリティオペレーションをモデルとしつつ、自組織で攻撃の観測や観測データの調査分析、脅威情報の発信や共有といったセキュリティオペレーションを担える人材、すなわち高度SOC人材を育成することを目標に、人材育成を行っている。

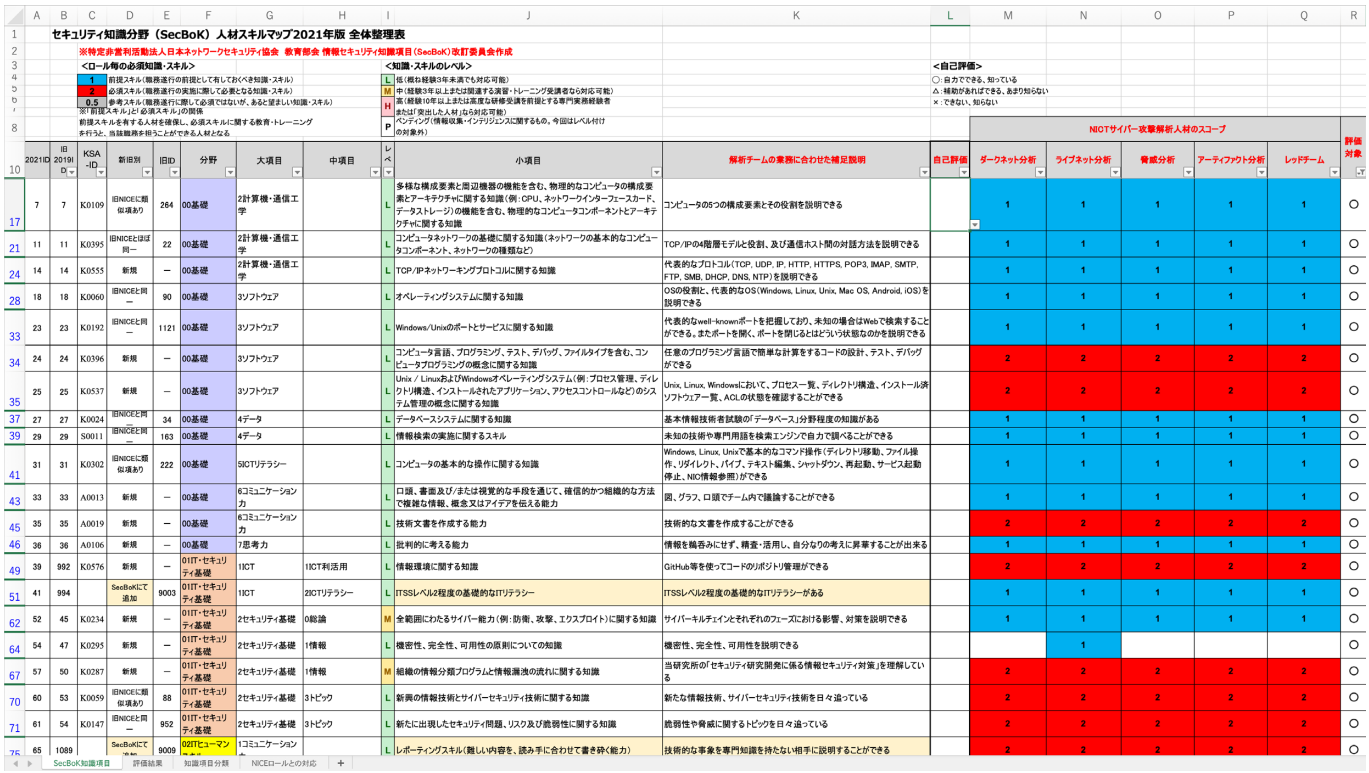
本稿では Co-Nexus S で実施する高度 SOC 人材育成及び脅威情報の生成・共有に関する活動について紹介する。

2　高度 SOC 人材育成

2.1　人材育成プログラムの概要

Co-Nexus S において提供する人材育成プログラムは、オンラインコースと OJT コースの 2 つに大別される（図 2）。

これらのプログラムはいずれも図 3 に示す流れで進められる。まず受講生は、育成前の自身のスキルを客観的に把握し、また選択するプログラムへの適性を評価するために（OJT コースの場合）スキルマップを使ったスキルの自己評価を行う。次に、オンラインコースでは自己学習プラットフォームを使って自分のペースでオンライン学習をすすめる。OJT コースでは、受講生の希望やスキル評価結果に基づくプログラムへの適合度を考慮し、ダークネットコース、ライブネットコース、アーティファクト分析コースのいずれかのコースを選択し、各コースに配属。アナリストとしての実務経験を積む。いずれのコースも学習の終盤では、学んだ知識やスキルをより深めるオリジナルの調査分



セキュリティ知識分野（SecBoK）人材スキルマップ2021年版 全体整理表

※特定非営利活動法人日本ネットワークセキュリティ協会 教育部会 情報セキュリティ知識項目（SecBoK）改訂委員会作成

2021ID	旧2019ID	KSA-ID	新旧別	旧ID	分野	大項目	中項目	レベル	小項目	解析チームの業務に合わせた補足説明	自己評価	ダークネット分析	ライブネット分析	脅威分析	アーティファクト分析	レッドチーム	評価対象
7	7	K0109	IBNICEに類似項あり	264	00基礎	2計算機・通信工学		L	多様な構成要素と周辺機器の機能を含む、物理的なコンピュータの構成要素とアーキテクチャに関する知識（例：CPU、ネットワークインターフェースカード、データストレージ）の機能を含む、物理的なコンピュータコンポーネントとアーキテクチャに関する知識	コンピュータの5つの構成要素とその役割を説明できる		1	1	1	1	1	○
11	11	K0395	IBNICEとほぼ同一	22	00基礎	2計算機・通信工学		L	コンピュータネットワークの基礎に関する知識（ネットワークの基本的なコンピュータコンポーネント、ネットワークの種類など）	TCP/IPの4階層モデルと役割、及び通信ホスト間の対話方法を説明できる		1	1	1	1	1	○
14	14	K0555	新規	―	00基礎	2計算機・通信工学		L	TCP/IPネットワーキングプロトコルに関する知識	代表的なプロトコル（TCP, UDP, IP, HTTP, HTTPS, POP3, IMAP, SMTP, FTP, SMB, DHCP, DNS, NTP）を説明できる		1	1	1	1	1	○
18	18	K0060	IBNICEと同一	90	00基礎	3ソフトウェア		L	オペレーティングシステムに関する知識	OSの役割と、代表的なOS（Windows, Linux, Unix, Mac OS, Android, iOS）を説明できる		1	1	1	1	1	○
23	23	K0192	IBNICEと同一	1121	00基礎	3ソフトウェア		L	Windows/Unixのポートとサービスに関する知識	代表的なwell-knownポートを把握しており、未知の場合はWebで検索することができる。またポートを開く、ポートを閉じるとはどういう状態なのかを説明できる		1	1	1	1	1	○
24	24	K0396	新規	―	00基礎	3ソフトウェア		L	コンピュータ言語、プログラミング、テスト、デバッグ、ファイルタイプを含む、コンピュータプログラミングの概念に関する知識	任意のプログラミング言語で簡単な計算をするコードの設計、テスト、デバッグができる		2	2	2	2	2	○
25	25	K0537	新規	―	00基礎	3ソフトウェア		L	Unix / Linux及びWindowsオペレーティングシステム（例：プロセス管理、ディレクトリ構造、インストールされたアプリケーション、アクセスコントロールなど）のシステム管理の概念に関する知識	Unix, Linux, Windowsにおいて、プロセス一覧、ディレクトリ構造、インストール済ソフトウェア一覧、ACLの状態を確認することができる		2	2	2	2	2	○
27	27	K0024	IBNICEと同一	34	00基礎	4データ		L	データベースシステムに関する知識	基本情報技術者試験の「データベース」分野程度の知識がある		1	1	1	1	1	○
29	29	S0011	IBNICEと同一	163	00基礎	4データ		L	情報検索の実施に関するスキル	未知の技術や専門用語を検索エンジンで自力で調べることができる		1	1	1	1	1	○
31	31	K0302	IBNICEに類似項あり	222	00基礎	5ICTリテラシー		L	コンピュータの基本的な操作に関する知識	Windows, Linux, Unixで基本的なコマンド操作（ディレクトリ移動、ファイル操作、リダイレクト、パイプ、テキスト編集、シャットダウン、再起動、サービス起動停止、NIC情報参照）ができる		1	1	1	1	1	○
33	33	A0013	新規	―	00基礎	6コミュニケーション力		L	口頭、書面及び/または視覚的な手段を通じて、確信的かつ組織的な方法で複雑な情報、概念又はアイデアを伝える能力	図、グラフ、口頭でチーム内で議論することができる		1	1	1	1	1	○
35	35	A0019	新規	―	00基礎	6コミュニケーション力		L	技術文書を作成する能力	技術的な文書を作成することができる		2	2	2	2	2	○
36	36	A0106	新規	―	00基礎	7思考力		L	批判的に考える能力	情報を鵜呑みにせず、精査・活用し、自分なりの考えに昇華することが出来る		1	1	1	1	1	○
39	992	K0576	新規	―	01IT・セキュリティ基礎	1ICT	1ICT利活用	L	情報環境に関する知識	GitHub等を使ってコードのリポジトリ管理ができる		2	2	2	2	2	○
41	994		SecBoKにて追加	9003	01IT・セキュリティ基礎	1ICT	2ICTリテラシー	L	ITSSレベル2程度の基礎的なITリテラシー	ITSSレベル2程度の基礎的なITリテラシーがある		1	1	1	1	1	○
45	45	K0234	新規	―	01IT・セキュリティ基礎	2セキュリティ基礎	0総論	M	全範囲にわたるサイバー能力（例：防衛、攻撃、エクスプロイト）に関する知識	サイバーキルチェインとそれぞれのフェーズにおける影響、対策を説明できる		1	1	1	1	1	○
47	47	K0295	新規	―	01IT・セキュリティ基礎	2セキュリティ基礎	1情報	L	機密性、完全性、可用性の原則についての知識	機密性、完全性、可用性を説明できる			1				○
50	50	K0287	新規	―	01IT・セキュリティ基礎	2セキュリティ基礎	1情報	M	組織の情報分類/プログラムと情報漏洩の流れに関する知識	当研究所の「セキュリティ研究開発に係る情報セキュリティ対策」を理解している		2	2	2	2	2	○
53	53	K0059	IBNICEに類似項あり	88	01IT・セキュリティ基礎	2セキュリティ基礎	3トピック	L	新興の情報技術とサイバーセキュリティ技術に関する知識	新たな情報技術、サイバーセキュリティ技術を日々追っている		2	2	2	2	2	○
54	54	K0147	IBNICEと同一	952	01IT・セキュリティ基礎	2セキュリティ基礎	3トピック	L	新たに出現したセキュリティ問題、リスク及び脆弱性に関する知識	脆弱性や脅威に関するトピックを日々追っている		2	2	2	2	2	○
65	1089		SecBoKにて追加	9009	02ITヒューマンスキル	1コミュニケーション力		L	レポーティングスキル（難しい内容を、読み手に合わせて書き砕く能力）	技術的な事象を専門知識を持たない相手に説明することができる		2	2	2	2	2	○

図 4　NICT サイバー攻撃解析人材のスコープ

析課題に取り組み、その成果を発表する。最終成果発表で一定の水準を満たす成果発表を行った受講生には修了証が発行される。

2.2　人材育成モデルと受講者のスキル評価

一口にサイバーセキュリティ人材といっても、分野や専門性、仕事上求められる役割などは非常に多岐にわたる。たとえばアメリカ国立標準技術研究所（NIST）が制定したサイバーセキュリティ人材フレームワーク [1] ではサイバーセキュリティに関する業務が 52 の役割に分類されている。一方で、日本ネットワークセキュリティ協会（JNSA）が策定したセキュリティ知識分野（SecBoK）の人材スキルマップ [2] では 16 の役割が定義されている。これらの役割の中には組織の統制役や組織内外との連絡調整役といった事務系の業務もあれば、セキュアな設計開発といった製品セキュリティに関する業務、インシデントの調査分析等の事案対処に関わる業務など、非常に多岐にわたる。

Co-Nexus S では、図 1 に示したように CYNEX 解析チームのアナリストが日々の業務で必要とする知識やスキルの教育やトレーニングの提供を目指しているが、必要なスキルを定義するためのフレームワークとして JNSA のセキュリティ知識分野（SecBoK）を活用している。前述のとおり SecBoK2021 では 14 の役割が定義されているが、これら 14 の役割に加えて、NICT が独自に定義した解析人材のスコープを追加し、関連する SecBoK のスキル項目（小項目）をピックアップし、各スキルの業務での必要性を 3 段階で評価してスキルマップを作成した（図 4）。

受講者は育成プログラムの受講前後でスキルマップを使った自己評価を行う。これにより、受講者においては自身のスキル保有状況の把握やプログラム終了時の成長を確認することができる。さらに教育プログラムを提供する側の NICT においても効果を客観的に把握することができる。

表 1　オンラインコース受講実績

	参加者数	組織数
第 1 期（2022 年上半期）	6 名	2
第 2 期（2022 年下半期）	8 名	3
第 3 期（2023 年上半期）	6 名	2
第 4 期（2023 年下半期）	16 名	8

2.3　オンラインコース

オンラインコースは 2022 年度に受講生の受け入れを開始して以来、4 月から 9 月末までの半年間を上期、10 月から翌年 3 月末までの半年間を下期として年に 2 回コースを開講している。これまでの受講実績を表 1 に示す。本稿執筆時点の第 5 期は 7 組織から 14 名が受講している。

図 5　オンライン学習プラットフォーム「Infinity Chamber」

2.3.1　オンライン自己学習教材

オンラインコースでは、セキュリティアナリストの育成を目的として開発されたオンライン自己学習プラットフォームである「Infinity Chamber」を使用する（図 5）。

このプラットフォームでは、攻撃手法の理解を深める AXOF と攻撃分析と対処について学ぶ AXDF の 2 つの学習コースが用意されている。

AXOF ではネットワーク上のサーバに対して行われる攻撃手法の基礎を習得する。脆弱性診断士やペネトレーションテスターといった攻撃試行を行うアナリストや、攻撃検知の仕組みを理解することが求められる SOC のアナリストの実務に有用な知識を得ることができる。

AXDF ではインシデント発生時の初動対応からファストフォレンジックの基礎、脅威インテリジェンスを活用した攻撃の分析、インシデントの発生防止を目的とした脅威分析といった防御的なセキュリティオペレーション全般を学ぶ。

いずれのコースも、テキストベースの講義とクイズから成る教材を通じて、知識を習得するだけでなく、Web ブラウザ上で利用できる演習用仮想環境やインターネットの各種公開サイトを利用し、実際に手を動かしてオペレーションを体験する実践的な内容になっており、知識のみならず実践的テクニックの習得やスキル向上が期待できる。

教材はテーマごとにモジュールと呼ぶ単位で分けられており、AXDF, AXOF 合わせて計 30 モジュールで構成される（図 6）。

	攻撃の分析と対処（AXDF）	攻撃手法の理解（AXOF）
1	インシデント初動対応	導入
2	デジタルフォレンジック調査	インターネット上の公開情報による偵察
3	原因分析・修復・予防	ホストとポートの探索
4	初期対応	システム情報探索
5	通信ログ分析	脆弱性スキャン
6	拡大防止・調査準備	認証試行
7	証拠保全 I	Web脆弱性調査1 基礎知識編
8	証拠保全 II	Web脆弱性調査2 能動的攻撃
9	マルウェア検体調査	Web脆弱性調査3 受動的攻撃
10	マルウェア関連情報収集	通信の傍受と改ざん
11	永続化調査（レジストリ）	エクスプロイト
12	実行履歴調査（プリフェッチ）	ポストエクスプロイト（バックドア）ポス
13	イベントログ調査	トエクスプロイト（権限昇格）
14	脅威分析	ポストエクスプロイト（探索・持ち出し）
15		ポストエクスプロイト（横展開）
16		侵入総合演習

図 6　Infinity Chamber のコース内容

2.3.2　取組の実績

受講者には SecBoK を活用したスキル評価のほかにセキュリティ関連業務の経験年数や所属部署などについてアンケートを実施している。受講者の約 6 割は未経験もしくは 1–2 年という経験年数であるが、中には業界経験が 10 年以上のベテランが自身の学び直しや部下への受講検討のために受講するケースもある。所属部署は、情報システム部やセキュリティ関連サービスの営業職のほか、研究所や学生（学部、修士、博士）などで年齢的には 20 代が多く上は 50 代まで幅広い層が受講している。

また、オンラインコースに期待することは何かという設問に対しては、「幅広い知識を身につけたい」「経験的に行っていたことを体系的に学び直したい」等の技術習得に関するコメントをはじめ、「今後の参加者との相談コミュニティの形成」「志同じ仲間とのコニュニケーション」等、人材育成の中で生まれるコミュニティへの期待に関するコメントもあった。

a）オンライン自己学習教材の評価

受講生はコース期間中に図 6 で示した 30 個のモジュールを学ぶ。これらのモジュールの内容は、セキュリティアナリストの育成を目的としているため、コンピュータアーキテクチャや通信プロトコルに関する基礎知識があることを前提とした教材となっている。自身のペースで自己学習するというオンラインコースの性質上、受講生がもつ前提知識や経験によっては必ずしもコース期間中に全てのモジュールを修了できるわけではない。コース期間中にそれぞれの受講生が最大限努力しモジュールを消化する、ベストエフォート型の学習方法となる。教材としては、受講生にとって簡単すぎず、かつ難しすぎない難易度のコンテンツが求められる。

第 4 期までの受講生 36 名について、修了したモジュール数と受講生の人数のヒストグラムを図 7 に示す。

25 個以上のモジュールを修了した受講生が 30 名であり、受講生の 8 割以上が 8 割以上のコンテンツを学習することができた。また、全てのコンテンツを修了した受講生はこの内 4 名であり、いずれもある程度のセキュリティ関連業務の経験がある受講生だった。このことから、幅広い層をターゲットとする本オンラインコースの教材の難易度としては適切であると客観的に評価できる。

b）受講生による最終成果発表

最終成果発表では、各受講生がオンライン自己学習で学んだ知識を活用した調査分析課題にそれぞれ取り組み、その成果を発表する。

調査分析課題のテーマは受講生が自ら提案し、取り組む課題と分析アプローチについて解析チームが助言やデータ提供等を行いサポートする。

これまでの受講生が取り組んだテーマをカテゴリ別に集計した結果を表 2 に示す。

最も多いテーマは、SOC アナリストに必要とされる技術の一つであるログ分析に関わるテーマである。一例として、ある受講生は自ら用意した検証環境に対して擬似攻撃を行い、検証環境で発生するセキュリティ機器のアラートや攻撃対象ホストのログを確認することで、攻撃手法とログの因果関係を分析するといったテーマに取り組んだ。この受講生は業務でセキュリティ監視サービスを扱っており、自社サービスの品質向上や機能拡張につなげたいという動機でテーマを選定した。また、ある学生の受講生は、大学のネットワーク環境に設置したハニーポットとパブリッククラウドに設置したハニーポットをそれぞれ同じ条件で運用し、観測したデータの差異を調査分析した。実際に狙われる脆弱性や攻撃に用いられた認証情報に傾向の違いがあり、興味深い結果が得られた。

調査分析課題は、環境準備を含めて 1 か月半程度で実施し、成果をまとめる。本節で挙げた例に限らず、受講生の多くは短い期間でありながら十分な成果が発表しており、自己学習の成果が窺える。

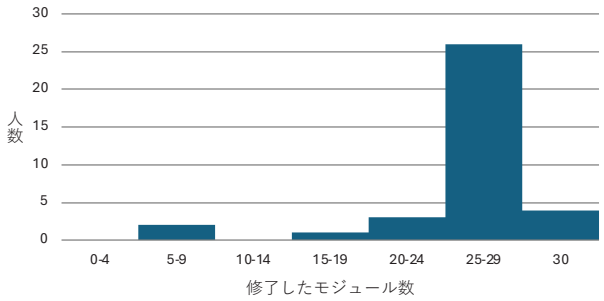


図 7　終了モジュール数と人数のヒストグラム

表 2　成果発表テーマのカテゴリ別集計結果

カテゴリ	人数
ログ分析	10 名
マルウェア解析	9 名
脅威分析	4 名
ツール評価検証	4 名
攻撃技術検証	3 名
攻撃観測データ分析	3 名
その他	1 名

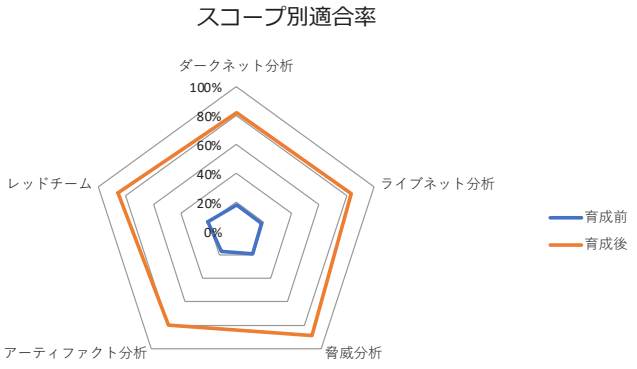


図 8　受講前後のスキル評価結果

c）コース修了後の評価

受講生は本コース受講前と最終成果発表終了後に、2.2 で述べたスキルマップを使った自己評価を実施する。

第 4 期までの全ての修了生において各スコープのスキルの向上が見られた。特に顕著な向上が見られた修了生における受講前後のスキル評価結果を図 8 に示す。

また、修了生には上記スキル評価のほかに受講後のアンケート調査を実施している。

修了生からのコメントとしては、「学習時間を自身でコントロールできる部分が良かった」「成果発表を行うことで学習した内容を深堀りできた」等のコース内容を評価するコメントのほか、「解析チームメンバと受講生のコミュニケーションをもっと取りたい」や「EDR や SIEM の演習を追加して欲しい」等の改善を求めるコメントも頂いた。

2.4　OJT コース

2.4.1　概要

OJT コースではダークネット分析、ライブネット分析、アーティファクト分析の 3 つのコースが用意されている（図 2）。

これら 3 つのコースはそれぞれ CYNEX 解析チームの業務ラインに相当する。受講者は、自身の希望や SecBoK を用いた自己評価の結果を考慮してこれら 3 つのコースの中から 1 つを選択し、コースを提供する業務ラインにアナリストとして配属され、解析・分析業務に従事する。育成期間は 1 年から 2 年を基本とする。半年で修了可能なオンラインコースよりも長期間のコミットメントを要するが、その分オンラインコースでは得られない実務経験を積むことができるプログラムとなっている。

2.4.2　ライブネット分析コース

ライブネット分析コースでは、NICT 内のセキュリティオペレーションに従事する。NICT 内で運用している多種多様なセキュリティアプライアンスで検知した脅威アラートの対応、情報システム部門と連携したインシデント対応にあたる。これらのいわゆる SOC オペレーションはチケットシステムを用い、ライブネット分析チームに所属する複数のアナリストが行っている。

SOC オペレーションと並行して、個別の脅威に関する調査や分析を行う。セキュリティオペレーションにおいては平常時と量的あるいは質的に異なるアラートの検出や、その原因を分析する「ベースライン分析」と呼ばれる調査手法がある。平常時（ベースライン）は組織のサイズや観測対象によって異なるが、OJT では数か月間にわたって実際に NICT で検知されるアラートを日々観測することを通じ、ベースライン分析に必要な知識や経験を得ることができる。またこれと並行して、外部のセキュリティベンダの公開情報や脅威インテリジェンスサービスを活用し、能動的な脅威の調査分析「アクティブスレットハンティング」も行っている。

たとえば、セキュリティオペレーション業務では様々な脅威が検知されるが、断続的に検知される大量のネットワークスキャンのイベントが発生した場合、その発生原因や送信元について、検知対象となった通信のペイロードをフルパケットキャプチャ装置を使って調査したり、発生の頻度をログ分析ツールを使って可視化したり、あるいは送信元 IP アドレスについて外部のインテリジェンスサービス等を使って分析を行ったりする等の作業が発生する。このような事象の調査を行うことで、攻撃者が送信元のインフラとして商用の VPN サービスを利用していることや、スキャンパケットの生成や送信に既存の脆弱性スキャナである Nessus が使われていることや、OAST ツールとして Interactsh が使用されているなど、脅威の検出や分析に関するノウハウを身につけることができる。

2.4.3　取組の実績

OJT コースではこれまで 2 名の受講生を受け入れ、いずれの受講者もライブネット分析コースを修了した。

- 第一期生（2022 年 6 月 1 日～ 2023 年 9 月末）
- 第二期生（2023 年 7 月 1 日～ 2024 年 3 月末）

受講者は前述した SOC オペレーションや調査分析業務に従事する中で、セキュリティオペレーションを効率化、高度化すべき課題を見つけ、その課題を解決する仕組みの提案や実装を最終課題として実施した。

ある受講生は、セキュリティアプライアンスでは検知が難しい通信をフルパケットキャプチャツールである「Arkime」を使って定期的に自動探索し、その結果を通知する取組や、マルウェアをダウンロードさせる悪性通信に含まれる URL を調査し、悪用される脆弱性とマルウェアを紐付けて攻撃キャンペーンを特定する一連の調査を自動化するツールの開発に取り組み、

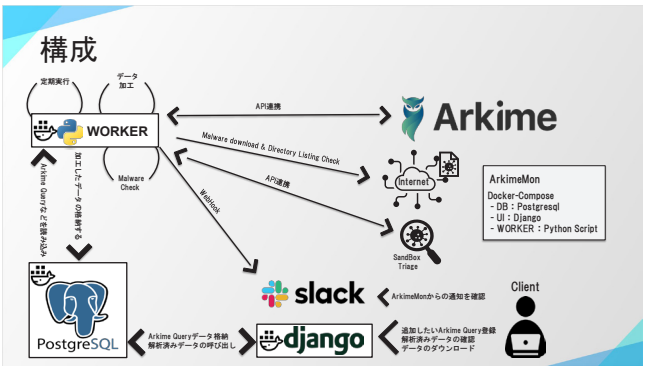


図 9　受講生が開発した脅威検出システムの構成

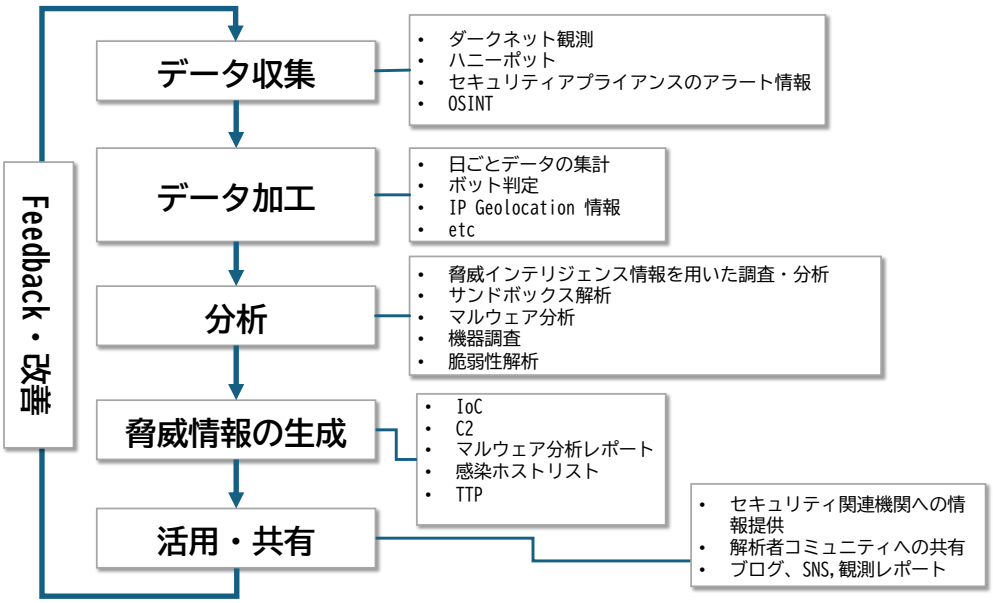


図 10　CYNEX 解析チームにおける脅威情報の生成

その成果を最終成果として発表した（図 9）。

コース修了後のアンケート調査では、OJT による人材育成について「有識者と同じ環境で業務できること」「学びたいこと実践したいことが可能な環境があること」「適切な導きにより良い気づきが得られること」等、本取り組みを評価するコメントを頂いている。

3　国産脅威情報の生成と共有

3.1　脅威情報とその生成

サイバーセキュリティの脅威とは何か。サイバー脅威情報の共有に関するガイドライン NIST 800-150 [3] は次のように定義している。

> 不正アクセス、破壊、情報の流出または改ざん及びサービス妨害攻撃（DoS）といった手段により、情報システムを通じて、組織の業務運営（組織の使命や機能、イメージ、評判を含む）、組織の資産、個人、その他の（二次的な影響を受ける）組織、または国家に悪影響を与える可能性のある状況やイベント。

脅威情報とは、組織が脅威から身を守ったり脅威を検知したりすることに役立つ情報を指す。先に紹介した NIST のガイドラインでは、具体例としてインディケータ情報、サイバー攻撃の手法（TTP）、セキュリティアラート、脅威インテリジェンスレポート、ツールの設定情報などが代表的な脅威情報として挙げられている。これらのほかにも、脆弱性情報や攻撃者の動向なども脅威情報として活用されている。

3.2　CYNEX 解析チームにおける定常解析

CYNEX 解析チームでは図 1 に示されている複数の分析基盤を用いて、アナリストが定常的に脅威の調査・分析を行っている。これらの分析基盤は、それぞれ異なる観測対象を取り扱う。たとえば、ライブネット分析基盤では、NICT のネットワークに到達する通信や NICT 職員宛に送られる電子メールなどのデータを観測・分析対象とする。一方、ダークネット分析基盤では、NICTER ダークネット宛に到達するパケットデータが対象となる。このように、異なる観測データに基づくオペレーションは図 10 に示される流れで行われる。以降の節では、CYNEX 解析チームにおける定常的な脅威分析の概要と代表的な分析事例について説明する。

3.3　ライブネット分析

3.3.1　概要

ライブネットとは、NICT 職員が業務で使用する NICT ネットワークを指し、このネットワークを流れるトラフィックが分析の対象となる。ライブネット分析チームは、日々のセキュリティオペレーションとして、多種多様なセキュリティアプライアンスで検出されたアラートを優先順位付けし、情報システム部門と連携してインシデントに対応する。また、アラートの統計分析や攻撃トラフィックの詳細な解析、SIEM を用いたアラート検出ルールの整備、セキュリティオペレーションの自動化、脅威情報を活用したスレットハンティングといった高度な分析にも取り組んでいる。

3.3.2　Arkime を活用したセキュリティオペレーション

監視対象のログをどこまで保全できるかは、インシ

デント調査において非常に重要な要素となる。特に、トラフィックのフルキャプチャデータは、検出されたサイバー攻撃の詳細調査やその影響範囲を特定する際に不可欠なデータである。CYNEX 解析チームでは、フルパケットキャプチャ及びパケット分析ツールとして、オープンソースの Arkime を利用している。

セキュリティオペレーションで Arkime を使用することには、いくつかのメリットが考えられる。代表的なものとしては以下の点が挙げられる。

- 分析作業をウェブブラウザ上で完結できる
- 豊富なプロトコル分析と検索集計機能を備え、アラートの調査を効率的に行える
- アラートの発生原因となった通信の詳細分析が可能
- アプライアンスが未対応の攻撃を独自クエリで検出できる

最後に挙げた未対応の攻撃検知は、アプライアンスを用いた攻撃検知において避けることのできない課題である。しかし、Arkime を活用して能動的に脅威ハンティングを行うことで、この課題に対処可能である。

例えば、2023 年 10 月 4 日に公開された脆弱性（CVE-2023-22515）は、ベンダによる脆弱性の公表から NICT で攻撃が初めて観測されるまで、以下のようなタイムラインをたどった。

- 10 月 04 日 Atlassian が修正リリース、一部顧客から悪用可能性の報告あり
- 10 月 10 日 Storm-0062 が 9 月 14 日以降悪用していると Microsoft が報告
- 10 月 10 日 Rapid7 が詳細情報を追記（PoC の公開）
- 10 月 22 日 NICT で攻撃を初観測

PoC が公表されてから攻撃が観測されるまでに 2 週間弱のギャップがあるが、アプライアンスが対応していない場合、自組織に攻撃が届いているか否かを確認するためには、通信ログを能動的かつ定期的に検索し、PoC に該当する通信が発生していないかを調査する必要がある。Arkime を使うことで、このような通信を能動的に検出できるだけでなく、Sandbox との API 連携を活用して攻撃成功時の影響を自動的に分析したり、攻撃通信に対するレスポンスの有無を確認するといった影響調査や、検出結果の自動通知など、レスポンスの自動化を図ることができる。

ツールの活用による効率化は、限られた人的リソースの中でセキュリティオペレーションを持続的に維持し、更に高度化させるための不可欠な要素となる。これにより、脅威の迅速な検知と対応が可能になり、組織全体のセキュリティ体制が強化されるだけでなく、脅威情報の生成と共有にも大きく寄与する。

3.4　ダークネット分析

3.4.1　概要

ダークネット分析オペレーションでは、主に次に挙げる 3 つの活動を行う。

1. NICTER 観測の統計値の算出と分析：ポートやプロトコル別の観測パケット数やホスト数の集計など、観測データの統計処理を行うことで、悪性通信の傾向や異常の兆候を把握する。
2. 送信元ホストに関する調査・分析：ボットへの感染が原因と考えられるスキャンパケットの送信元ホストの機器調査を実施し、感染原因を詳細に分析する。必要に応じて、同一の実機を調達して脆弱性の有無や感染経路を調査する。
3. インシデント対応：感染ホストの運用者への連絡、対応方法に関する情報提供、通知後の感染状況の経過観測を行い、感染が止まるまでフォローアップすることで、迅速かつ効果的なインシデント対応を支援する。

以降の節ではこれまでに行った調査分析やインシデント対応の事例を紹介する。

3.4.2　韓国製 DVR の Mirai 感染通信の検知と脆弱性ハンドリング

2022 年以降、日本国内で韓国製 DVR 機器が Mirai に感染する事例が多数観測されている。感染機器の調査を進めた結果、一部の製品には未公表の脆弱性が存在することが判明した。これに対し、日本国内で当該製品を販売するベンダと連絡を取り、脆弱性の詳細や感染状況などの情報共有を行った。また、実機を用いた攻撃観測を実施し、当該機器を狙う攻撃者の長期的な動向を注視している。いくつかのベンダに関する脆弱性は、日本国内の脆弱性ポータルサイトである JVN において公開されている [4][5]。

3.4.3　ASUS 社製ルータに関する脆弱性調査分析

ブロードバンドルータの管理画面は、一般的に LAN からのアクセスのみを許可し、WAN 側からはアクセスできない設定にする。しかし、台湾の ASUS 社のルータの多数がインターネットから管理画面にアクセスできる状態になっていることが判明したため、その原因を特定するために独自の調査を開始した。

調査の過程でルータ管理者の認証情報を詐取可能な中間者攻撃の手法を発見したため、SNS を通じてルータのユーザに注意喚起を行うとともに [6]、同社の PSIRT（脆弱性報告窓口）にこの脆弱性を報告した。ベンダと対応方針について協議し、2023 年 7 月 27 日にはベンダからセキュリティアドバイザリが公開された [7]。

侵害されたルータは APT（Advanced Persistent Threat）攻撃で悪用されているという報告もあり（例：APT31）、また ASUS 社のルータは世界中で使用され

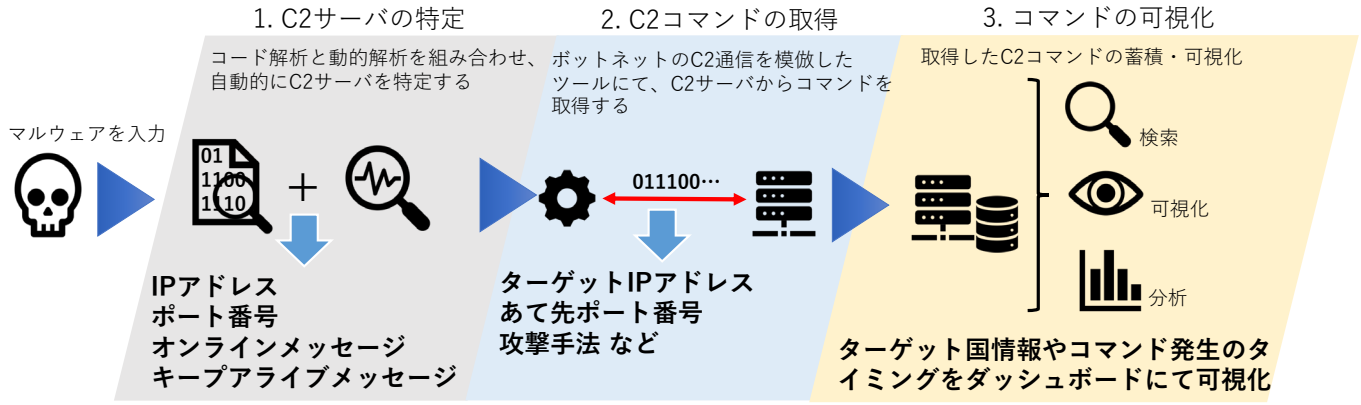


図 11　Mirai C2 コマンド観測システムの概要

ていることから海外のユーザに対する注意喚起も必要であると考え、サイバーセキュリティ分野で最も著名な国際会議の一つである Black Hat Europe において、この発見について発表を行った [8]。

3.5　アーティファクト解析

3.5.1　概要

ライブネット観測では、NICT の職員宛に送付されるメールに添付された悪性ドキュメントが検出される。一方、ダークネット観測では、攻撃者が無差別にばら撒く脆弱性を悪用した攻撃ペイロードにダウンロードされるマルウェアなどの情報が得られる。アーティファクト解析チームは観測オペレーションを行うメンバーと連携し、これらの「アーティファクト」の詳細な分析を実施する。また、外部組織からの解析依頼にも対応する。

マルウェア解析においては、ローカル環境で表層解析や静的解析を行うとともに、オンラインサンドボックスを使用して動的解析を行うこともある。これらの解析結果を基に、解析レポートを作成する。レポートには、マルウェアファミリの特定、C2 サーバや通信先の IP アドレスとポート番号、プロセス生成の詳細、ダウンロードされるファイルの内容、情報窃取系マルウェアの場合は窃取される情報の種類や送信方法、暗号化された文字列の復号結果などをまとめる。

解析結果は観測チームにフィードバックされ、解析の自動化（ツール作成など）の検討が行われる。また、STARDUST [9] を使用して長期的な解析も実施される。

3.5.2　Mirai C2 観測システム

IoT マルウェアの Mirai は脆弱な IoT 機器を主に狙って感染するマルウェアであり、感染すると主に 3 種類の通信を行う。

a）C2 サーバとの通信
b）C2 サーバからコマンドを受信後、DoS 攻撃の実施
c）他のホストへの感染活動

C2 サーバの情報は、マルウェア検体内に難読化されて含まれていることが多いが、特定のコードを解析することで難読化の解除に必要なデータを取得することができるため、C2 サーバの特定が可能である。また、検体の動的解析を行うことで、C2 サーバとの間で行われる通信プロトコルを解析し、Mirai ボットの C2 通信を模倣するツールを開発することができる。

解析チームでは、C2 サーバの特定から C2 コマンドの取得、コマンドの可視化までのオペレーションを自動化する Mirai C2 観測システム（図 11）を開発し、C2 コマンドの長期観測を行い、DDoS 攻撃のターゲットとなっている国や組織、攻撃継続時間等のデータの収集・分析を行っている。

3.6　公開脅威情報の収集分析

3.6.1　概要

サイバー攻撃に関する情報は、インターネット上のニュースサイトやセキュリティアナリストの SNS アカウント、被害を受けた組織からの報告、セキュリティベンダや国のセキュリティ機関が発行するレポートなど、様々な情報源から日々膨大に発信されている。これらの情報は、脅威に関する多様な視点からの分析や評価を可能にし、サイバー攻撃の予兆を捉え、現在発生している攻撃の影響範囲や深刻度を総合的に判断するための重要な手がかりとなる。また、これらの情報は事象に関する詳細な調査分析を行うきっかけとなることもある。

以降の節では CYNEX 解析チームで行っている公開脅威情報の収集分析の取組について述べる。

3.6.2　公開脅威情報の定常的な収集

解析チームでは長年の知見の蓄積に基づき、サイバー攻撃に関する公開情報の収集及び分析を行っている。収集対象の脅威情報は以下の 5 つのカテゴリに分類される。

a）サイバー攻撃関連
　国家支援型サイバー攻撃の主体に関する情報、特に地政学的に日本の脅威となる国に関する情報
b）脆弱性情報
　新規に公開された脅威度の高い脆弱性、特定の脆弱性を TTP として使用する攻撃者グループの活動、脆弱性のエクスプロイトツールへの組み込み、脆弱性の影響範囲及び米 CISA が運営する KEV カタログへの追加情報
c）各国のサイバー関連動向
　各国のサイバーセキュリティ施策に関する情報
d）レポート関連
　シンクタンクやセキュリティベンダが公表したレポートの概要やリンク情報
e）その他
　ライブネット観測、ダークネット観測、アーティファクト分析など、CYNEX 解析チームのアナリストがウォッチしている事象に関する情報
　また、収集された脅威情報を基に、NICT 内の監視対象システムへの影響の有無を調査している。収集された公開情報は解析チーム内で共有されるほか、CYNEX Co-Nexus A の参画メンバーとも共有される。

3.6.3　インシデント情報の収集

サイバー攻撃に関する被害の実態を把握するために、インシデント情報を公開するサイトの更新をウォッチし、日本に関連する情報が新たに追加されているか否かを機械的に判別し、その結果をアナリストに共有している。以下にその一例を示す。

a）ランサムウェア攻撃グループのリークサイト
　各ランサムウェア攻撃グループが公開する侵害組織情報の監視を行い、複数のランサムウェア攻撃グループのリークサイトを監視する。LLM を使って日本に関係があるかどうかを自動判定し、判定結果を付加した侵害組織のリストをアナリストに配信する。
b）DNS 水責め攻撃の対象ドメイン
　DNS 水責め攻撃とは、DNS サーバに対する DDoS 攻撃の一種である。この攻撃では、攻撃対象のドメインのランダムなサブドメインに対する大量の問い合わせを、そのドメインを管理する権威サーバに送りつける。これによりサービス不能の状態を作り出し、当該ドメイン名へのアクセスを妨害する。解析チームでは、DNS 水責め攻撃の対象となったドメイン情報を収集し、JP ドメインに関する新規情報があれば当該情報をアナリストに共有し、NICTER ダークネットや各種ハニーポットの観測データと突合することで、関連する攻撃発生の有無を確認する。

4　おわりに

本稿では、Co-Nexus S における高度 SOC 人材育成及び国産脅威情報の生成と共有について示した。

CYNEX の Co-Nexus S は、1 年間の準備期間を経て、2022 年から本格的に高度 SOC 人材育成を開始した。並行して、CYNEX 解析チームでは、ライブネット分析、ダークネット分析、アーティファクト解析、脅威情報の収集と分析を行い、多様化するサイバー攻撃の脅威に対応するための分析技術を磨いている。これにより、脅威情報の共有を推進し、ノウハウを SOC 人材育成を通じて社会に還元している。

今後も CYNEX 解析チームが中心となって、脅威の観測と分析、対策に必要な脅威情報の共有を CYNEX の枠組みを通じて推進していく。

【参考文献】

1　M.C.S.K.A.W. Rodney Petersen, Danielle Santos, and G. Witte, “Workforce Framework for Cybersecurity (NICE Framework),”. https://doi.org/10.6028/NIST.SP.800-181r1
2　JNSA, “セキュリティ知識分野 (SecBoK) 人材スキルマップ 2021 年版.” https://www.jnsa.org/result/skillmap/
3　D.W.J.S. Chris Johnson, Lee Badger and C. Skorupka, “Guide to Cyber Threat Information Sharing,” https://doi.org/10.6028/NIST.SP.800-150
4　JPCERT/CC, “JVNVU94514762：ユニモテクノロジー製デジタルビデオレコーダにおける複数の脆弱性,” https://jvn.jp/vu/JVNVU94514762/
5　JPCERT/CC, “JVNVU90812349：ケービデバイス製デジタルビデオレコーダにおける複数の脆弱性,” https://jvn.jp/vu/JVNVU90812349/
6　@NICTER 解析チーム, “先日、ルータの管理画面がインターネットに公開されている件についてツイートしましたが、ASUS 製ルータではスマホ向けの設定アプリを使用すると、うっかり WAN 側に対してルータの管理画面を公開してしまう可能性があります。(続く),” https://x.com/nicterjp/status/1646029541004148736
7　ASUS, “07/25/2023 Strengthening DDNS Security for RT-AX1800U, RT-AX3000, RT-AX3000 v2, RT-AX86U, TUF-AX3000 and TUF-AX5400,” https://www.asus.com/content/asus-product-security-advisory/
8　Y.M. Masaki Kubo and K. Okugawa, “One Million ASUS Routers Under Control: Exploiting ASUS DDNS to MITM Admin Credentials,” https://www.blackhat.com/eu-23/briefings/schedule/index.htmlone-million-asus-routers-under-control-exploiting-asus-ddns-to-mitm-admin-credentials-35443
9　津田 侑，遠峰 隆史，金谷 延幸，牧田 大佑，丑丸 逸人，神宮 真人，高野 祐輝，安田 真悟，三浦 良介，太田 悟史，宮地 利幸，神薗 雅紀，衛藤 将史，井上 大介，中尾 康二, “サイバー攻撃誘引基盤 STARDUST,” コンピュータセキュリティシンポジウム 2017 論文集 pp.472–479, 2017.

久保 正樹（くぼ まさき）
サイバーセキュリティ研究所
サイバーセキュリティ研究室／
サイバーセキュリティネクサス
上席研究技術員
脆弱性、サイバー攻撃観測・分析、IoT セキュリティ、セキュアコーディング

神宮 真人（じんぐう まさと）
サイバーセキュリティ研究所
サイバーセキュリティ研究室／
サイバーセキュリティネクサス
主任研究技術員
セキュリティオペレーション、インシデント
レスポンス、ネットワーク設計構築

piyokango（ぴよ かんご）
サイバーセキュリティ研究所
サイバーセキュリティネクサス／
サイバーセキュリティ研究室
上席研究技術員
脅威情報収集分析
【受賞歴】
2024 年　サイバーセキュリティアワード 2023
　　Web・コンテンツ部門 最優秀賞
2022 年　サイバーセキュリティに関する総務
　　大臣奨励賞
2017 年　サイバーセキュリティに関する総務
　　大臣奨励賞