5-2　Co-Nexus A: 各種観測基盤による共同解析と解析者コミュニティ形成

5-2　Co-Nexus A: Accumulation & Analysis

安田 真悟　佐藤 隆行　毛利 公一
YASUDA Shingo, SATO Takayuki, and MOURI Koichi

サイバーセキュリティネクサスは我が国のサイバーセキュリティ対処能力の絶え間ない向上に貢献し、社会全体でセキュリティ人材を持続的に育成していくため、サイバーセキュリティに関する情報分析・人材育成などの産学官連携の中核的拠点として令和 3 年度に発足した。令和 5 年 10 月からはアライアンス体制へ移行し、Co-Nexus A / S / E / C の 4 つのサブプロジェクトを擁し、それぞれの担当領域で活動を行っている。CYNEX Co-Nexus A では STARDUST や WarpDrive といったサイバーセキュリティ研究室の研究開発成果である各種観測基盤を活用して、サイバーセキュリティ情報を大規模に収集・蓄積するとともに、Co-Nexus A に参画する組織の解析者のコミュニティを醸成し、共同分析の実現を目指している。本稿では、Co-Nexus A の STARDUST 独自解析の結果を中心に現在の活動状況と今後の課題について詳述する。

Cybersecurity Nexus was established in 2021 as a nexus for industry-academia-government collaboration in cybersecurity information analysis and human resource development, in order to contribute to the continuous improvement of Japan's cybersecurity response capability and to continuously develop security personnel throughout society. In October 2023, CYNEX Co-Nexus A shifted to an alliance structure, with four sub-projects (Co-Nexus A, S, E and C), each of which is active in its respective area of responsibility. It aims to collect and accumulate cybersecurity information on a large scale using various observation boards that are the results of the Cybersecurity Laboratory, as well as to foster a community of analysts from the organizations participating in Co-Nexus A and realize joint analysis. This paper details the activities of Co-Nexus A from its inception to date and future challenges.

1　まえがき

サイバーセキュリティネクサスは我が国のサイバーセキュリティ対処能力の絶え間ない向上に貢献し、社会全体でセキュリティ人材を持続的に育成していくため、サイバーセキュリティに関する情報分析･人材育成などの産学官連携の中核的拠点として令和 3 年度に発足した。令和 5 年 10 月からはアライアンス体制へ移行し、Co-Nexus A / S / E / C の 4 つのサブプロジェクトを擁し、それぞれの担当領域で活動を行っている。その 1 つである Co-Nexus A ではサイバーセキュリティ研究室の研究開発成果である NICTER、STARDUST [1]–[3] と WarpDrive の各種情報収集基盤を活用し、サイバー攻撃に関する情報を大規模に収集・蓄積している。また、STARDUST、WarpDrive 及び LETTICE の 3 つの解析者コミュニティを形成し各情報収集基盤などで得られた情報の共有と議論を行っている。本稿では解析者コミュニティで共有している STARDUST での NICT 独自の解析結果を中心に Co-Nexus A の全体活動状況を報告する。

2　STARDUST NxtGen の貸与と誘引実験

2.1　STARDUST NxtGen の貸与

STARDUST はサイバーセキュリティ研究室で研究開発している主に標的型攻撃を対象としたサイバー攻撃に関して、攻撃者の挙動を長期分析するための攻撃誘引基盤である。攻撃者を外部から誘引するために、企業サイズの精巧な模擬環境“並行ネットワーク”を自動構築し、標的型攻撃に用いられるマルウェアを解析者が模擬環境内で実行することでステルス性の高いリアルタイム観測・分析が可能である。2023 年 10 月の

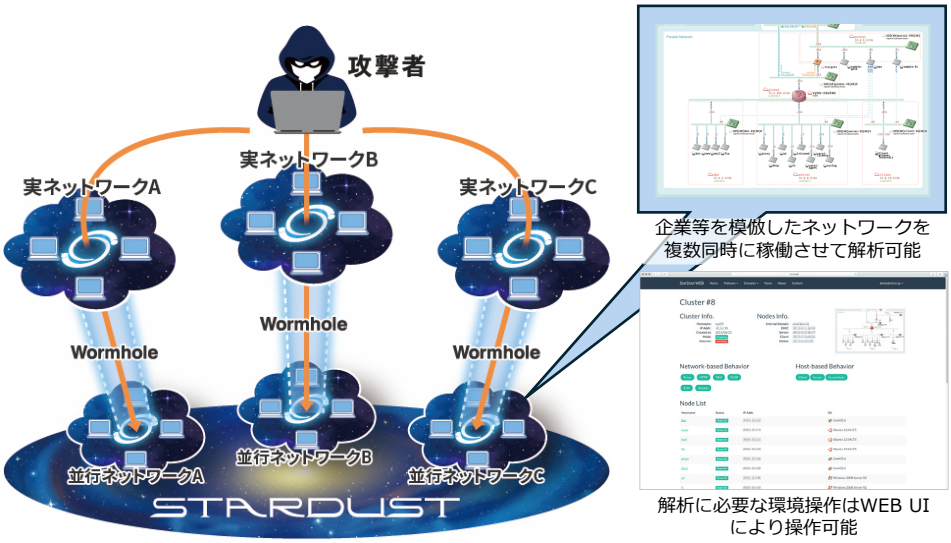

図 1　サイバー攻撃誘引基盤 STARDUST NxtGen

CYNEX アライアンス発足に併せて貸与を開始した次世代版STARDUSTであるSTARDUST NxtGen（図1）では模擬環境の設計・VM/NW 配備・稼働テストなど含む構築・運用を自動化するマネジメントシステムを開発し、従来比約 10 倍の高速化を達成した。さらにライブフォレンジック機能や後述する CURE との連携機能も追加するなど、セキュリティ観測・実験・評価基盤となっている。Co-Nexus A では 2024 年 6 月現在 26 参画組織に STARDUST NxtGen を貸与し、各組織で入手したマルウェア検体の解析を支援している。また、CYNEX アライアンスの発足に伴って、これまでの共同研究契約から利用契約へ移行したことに伴い、利用している組織の一部では教育プログラムでの利用事例も見られ、実解析にとどまらない利用方法も実現している。

2.2　STARDUST での誘引実験

Co-Nexus A では STARDUST NxtGen の貸与による参画組織による解析と並行して、年間 300 回を超える NICT 独自の解析も行っている。昨今のサイバー攻撃では、サイバーキルチェーンと呼ばれる攻撃の各段階での分業と技術の標準化が進んでおり、初期検体の解析だけでは攻撃者グループや目的の推定までの全容の解明が困難になっている。そこで独自解析では標的型攻撃等による不正活動について、その実態及び被害の発見・検知につながる脅威の特徴を明らかにするため、実在する会社と連携し標的型攻撃のアタック・ベクタとして利用されることの多いファイル（PDF 形式、XLS 形式、DOC 形式、EXE 形式、ZIP 形式等）が添付されたメールを収集し、その中からマルウェアと疑われるファイルを抽出。これらのファイルがSTARDUSTを用いて組織を模擬したネットワークで実行される

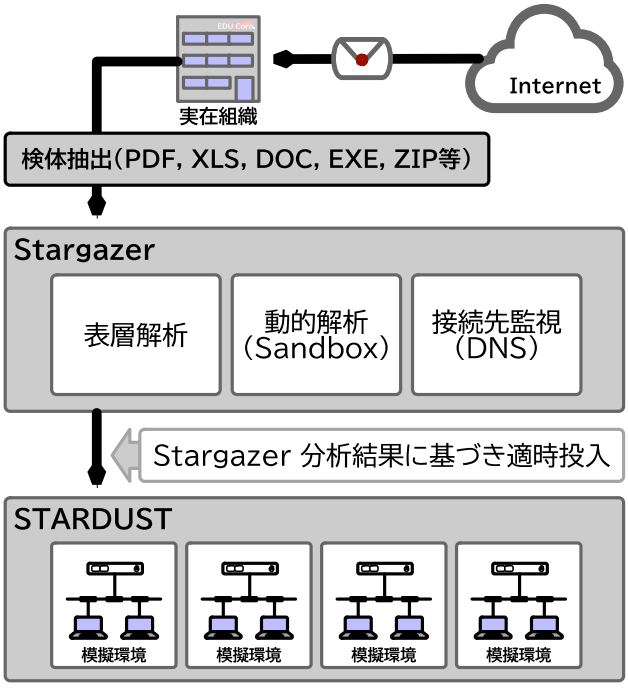

図 2　独自解析におけるシステム構成と解析の流れ

（感染する）ことで、サイバー攻撃の攻撃者の誘引を伴う攻撃観測を実施している。

2.3　独自解析の構成

独自解析における解析のフローを図 2 に示す。攻撃観測においては感染後の C&C サーバとの通信の可否が初期誘引の成功の分岐点となる。これは検体の鮮度、攻撃者が攻撃の隠密性や分析回避の為に攻撃対象や C&C サーバの稼働時間を攻撃者の活動期間だけに絞り込む意図、Malware As A Service（MaaS）、Ransomware As A Service（RaaS）などの攻撃者側の基盤の挙動などが要因である。検体を起動しても

表 1　検体収集と解析数

収集・解析実施期間	令和 5 年 9 月 1 日～ 令和 6 年 2 月 16 日
悪性と判断されたメール件数	90,379 通
マルウェアファミリー名が推定された件数	12,468 検体
解析対象検体抽出数	364 検体
中期観測基盤解析 Stargazer 解析件数	272 件
STARDUST 解析件数	49 件

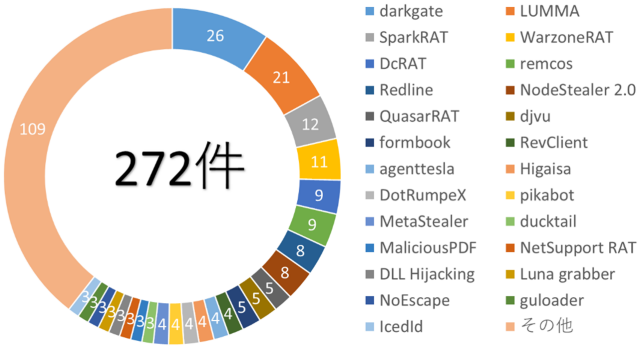

図 3　Stargazer 解析における検体検知名の分布

表 2　STARDUST を用いた代表的な解析結果・観測事象 (2023 年度)

#	検体名	観測事象
1	Purplefox	外部への感染拡大(SMB ブルートフォース攻撃)活動
2	Dtrack	攻撃者による手動の操作、既知の IoC 情報に無い新しい検体使用
3	remcos	三次検体(AgentTesla)による情報窃取
4	Luna Grabber	Discord への通信
5	NoEscape	ファイルの暗号化と脅迫文の表示

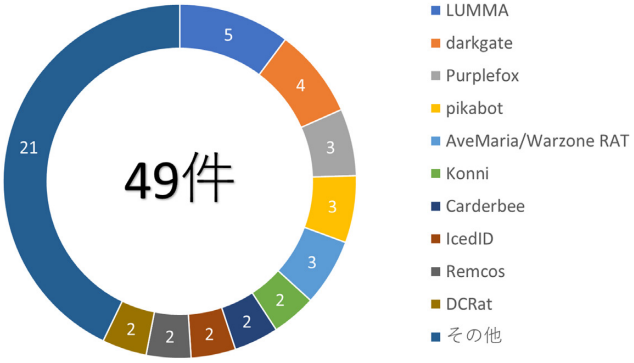

図 4　STARDUST 解析における検体検知名の分布

C&C サーバに接続できない場合は、攻撃者の誘引に失敗するため、解析を止めて模擬環境を初期化したり、C&C サーバに接続が可能になるまで模擬環境を維持するか選択と作業が必要となる。これは人的運用コストや STARDUST の解析効率低下を招くため、選定、解析開始タイミングの決定は動的解析の効率向上において重要なポイントである。そこで、独自解析においては STARDUST 解析の前段階として収集した検体を中期観測基盤 Stargazer [4] に投入し、表層解析、サンドボックス解析に加えて C&C サーバの DNS による名前解決の可否を調査することで、検体解析の適時性を高めて解析効率の向上を実現している。この Stargazer システムも今後参画組織が利用するための改修を実施した後希望する STARDUST 利用組織にオプション貸与をする予定である。

2.4　独自解析結果

2023 年度における解析数を表 1 に記載する。約 7 か月の期間において悪性と判定されたファイルが添付されたメールが 90,379 通あり、その VirusTotal 等でマルウェアファミリー名が推定できたファイルが 12,468 件であった。また、これに加えて OSINT や通報などによる収集も含めて最終的に 364 検体を解析対象として選定し、そのうち 272 検体を中期観測基盤 Stargazer で解析を実施した。

Stargazer にて解析した検体の検知名の分布を図 3 に示す。darkgate や LUMMA、SparkRAT など特定の目的をもって動的活動観測までを行った検体ファミリーが多い状況となった。この中から解析の結果攻撃者の誘引の可能性が高いと判断し、49 件を STARDUST で解析を実施した。STARDUST で解析した検体の検知名の分布を図 4 に示す。

昨年度解析したこの 49 件の解析において代表的な解析結果・観測事象を表 2 に示す。

#1 の Purplefox [5] では外部セキュリティベンダの情報 [5] により SMB パスワードブルートフォース攻撃を利用して外部への感染拡大を試みるとの情報から、対策設定を施した模擬環境で解析を行った結果、外部セキュリティベンダの情報を裏付ける活動が観測された。Powershell 起動後に意図的に一定時間動作を止める Sandbox 回避機能を有する検体が使われていた。

#2 の Dtrack の解析では攻撃者の誘引並びに OSINT 等の事前情報調査では判明していなかったペンテストツール「Sliver」をベースにした RAT と推定される三次検体の使用が確認された。

#3 の remcos では端末の認証情報や GeoIP 等の情報窃取、#2 と同じく事前情報調査では判明していなかった三次検体(AgentTesla)の使用が確認された。GeoIP 取得後に攻撃が継続されなかったことから、端末の所属国で攻撃対象を選別している可能性がある。

#4、#5 は解析のし易さから選定したインフォスティーラーとランサムウェアで、#4 は感染した端末のシステム情報を特定の Discord に送信する機能を有していたものの、解析次点で送信先の Discord アカウントの Webhook がすでに無効になっていた。また、#5 のランサムウェアの検体は動作するものの、表示されたコンタクトサイトには既にアクセスできなかった。一方でリークサイト等の脅威アクターのインフラが停止している状況であっても端末上のファイルの暗号化が実行されることが確認され、破壊的な意図を達成する検体としては依然脅威であることが確認された。

様々な媒体で公開されている脅威情報の確認、信頼できる詳細情報の蓄積には独自の解析が必要であるが、そのためにはサンドボックス解析を用いられることが一般的である。しかし、#1 のようにサンドボックス解析を回避する挙動を示す検体もあり、STARDUST のような模擬環境を用いた攻撃誘引を伴う攻撃観測は、攻撃者の意図や三次検体などのより攻撃が進行した段階での手法を明らかにする為に有効であることがわかる。また、脅威アクターのインフラ停止後の検体挙動の把握は、インフラ停止後の解析が必要となりリスクの継続的な再評価において重要な要素になるものの、攻撃解析の前線においては見落とされ易い視点であり、サイバー攻撃に関する情報を大規模に収集・蓄積、解析者コミュニティにより国内のサイバー攻撃に対する対応力を強化することを目的としたCYNEX の活動として、継続的に取り組む活動であると考えている。

このように、STARDUST はサーバ攻撃の実体解明に必要な詳細な情報取得能力を有しているが、取得したログなどの分析は各解析者の技量が求められるため、解析手法の一般化と汎化可能な作業の自動化など解析者の負担を軽減する補助システムの開発を引き続き検討する。

3　WarpDrive プロジェクト

Co-Nexus A では Web 媒介型攻撃の実体解明と対策技術の研究開発を目的として、Web 媒介型攻撃のユーザー参加型大規模観測基盤 WarpDrive（Web-based Attack Response with Practical and Deployable Research InitiatiVE）の開発と運用を行っている [6]。このプロジェクトは平成 28 年度に開始した委託研究「Web 媒介型攻撃対策技術の実用化に向けた研究開発」の成果応用として、令和 3 年度 4 月より NICT 自ら研究として CYNEX Co-Nexus A へ移管して継続しているプロジェクトである（図5）。

IP アドレスが有限の空間でその総数が決まっているのに対して、URL は無限かつ短時間に新規の URL を作成することが可能である。その結果、悪性の Web サイトを閲覧するだけでマルウェアに感染する Web 媒介型サイバー攻撃の実態把握のためには攻撃に使われる URL を継続して把握する必要がある。そのためにはフィッシングメールや広告リンクなど実際の攻撃の端点を受信しているユーザー端末での観測、情報収集が欠かせない。しかし、一般ユーザーにとって端末がアクセスしている URL の情報の提供は個人情報に隣接する問題であり、ユーザーが協力する動機が生まれにくいことが課題になる。情報収集の研究においては謝金の支払いによってデータ収集する手法もあり、WarpDrive の委託研究の初期には同様のアプローチで被験者に謝金を支払い、データ収集実験を実施した実績もある。しかし、この手法は費用面でのスケールと継続性において課題があるため、現在の WarpDrive では Android スマートフォンと Google Chrome 拡張機能向けのアプリケーションである「タチコマ・セキュリティ・エージェント」（タチコマ SA）を開発に際して

図 5　WarpDrive Project 概要図

表３　タチコマ SA が提供しているセキュリティ機能の一部

機能	備考
疑わしいサイトへのアクセス検出警告機能	PC/Mobile 版共通機能
疑わしいサイトへのアクセス予測警告機能	
疑わしいサイト・コンテンツの報告機能	
外部からのネットワークスキャン機能	
アンケート機能	
ローカルネットワークスキャン機能	Mobile 版のみ

アニメ攻殻機動隊シリーズ [7] の意匠を活用とセキュリティアプリとしての一般的な機能の提供を通じたユーザーメリットの提供によりユーザーの協力を持続的に得ることを目標としている。具体的には壁紙などのコンテンツ提供に加えて、タチコマ SA はユーザーが所有する PC もしくはスマートフォンの Web ブラウザの中で Web 媒介型攻撃の観測・分析を行い、攻撃検知時には悪性 Web サイトの閲覧をブロックしたり、ユーザーに警告やアドバイスを行ったり、セキュリティアプリとしての基本機能を有している（表3）。

また 2023 年 10 月の大型アップデートではユーザーの能動的な利用動機の多様化と持続的な利用促進として、セキュリティの知識を習得できるゲーム機能をリリースした [8]。このゲーム機能のリリースにより新規ユーザーの獲得とアプリケーションの起動時間が延びたことにより収集するデータ量ではゲーミフィケーション機能リリース前が 100 万 URL/ 日であったのに対して、リリース後は 700 万 URL/ 日と 7 倍になるなどの効果が得られた。さらに、2024 年度 2 月にはモバイル版にローカルネットワークスキャン機能を追加した。この機能はモバイル端末が WiFi 接続している家庭内ネットワーク内にポートスキャンをユーザーが実行し、IoT デバイスの探索とポート開放状況を確認できる機能であり、これによりユーザーが意図しない IoT デバイスの残存や家庭内に潜む感染拡大リスクを確認と対応を支援することが可能となった。また、これまで NOTICE [9] で実施している国内グローバル IP アドレスへの大規模スキャンでは、家庭内のブロードバンドルーターの内側のネットワークにおける IoT デバイスの普及などの実態把握は困難であったが、この機能により一般の家庭内にどの程度の IoT デバイスが普及しどのようなサービスポートが開放されているかの実態把握を可能になった。

WarpDrive プロジェクトではこうした研究開発と運用により得られたデータを参画組織へ提供して Web 媒介型攻撃の実態把握や検知技術の研究開発に寄与している。

4　解析者コミュニティと LETTICE プロジェクト

Co-Nexus A では STARDUST 利用組織を中心とした解析者コミュニティ、WarpDrive コミュニティと LETTICE の 3 つのコミュニティを形成している。この章では各コミュニティ活動を紹介する。

4.1　解析者コミュニティ

STARDUST 利用組織を中心とした解析者コミュニティは Co-Nexus A 全般の情報を集約して議論する中心的なコミュニティとして、解析者が動的活動観測や OSINT 等で得られた解析結果やサイバー攻撃の特徴情報を共有している。

コミュニティ活動では CYNEX アライアンス参画組織が利用する Slack 基盤を通じて解析者同士の定常的なコミュニケーションチャネルを確保するとともに、NICT による STARDUST での独自解析の逐次報告、OSINT 情報などが共有されている。また、このオンラインコミュニケーションのほかに定期会合方式の Co-Nexus A 会合も年に 4 回実施しており、各会合の参加者は R5 年度第 4 回会合現在で 70 名を超える規模になっている。通常の会合は招待発表者を除いて参画組織の指名者のみが参加できるクローズド会合を採用しているが、毎年度 12 月に開催している第 3 回会合はコミュニティ活動の広報活動を兼ねて、クリスマスセキュリティワークショップ（CSWS）と位置づけて、参画組織の参加メンバーが招待した参画組織外の解析者も参加できるセミオープン会合となっている。

4.2　WarpDrive コミュニティ

WarpDrive プロジェクトで収集しているデータの分析共同研究を促進するため、令和 5 年度に新たに発足したコミュニティである。WarpDrive Workshop を年 1 回程度の頻度で開催し、WarpDrive プロジェクトに参画している組織間での研究開発成果の共有をしている。また、NICT では参画組織の知見として得られた解析の為の標準的な手法・ツールを NICT で標準ツールとして WarpDrive 分析基盤に整備を進めるなど、参画組織の研究開発を支援している。

4.3　LETTICE プロジェクト

令和 6 年度に発足した一番新しいコミュニティ活動である。これまでの Co-Nexus A での活動では、解析作業を各参画組織が各々実施して成果と知見を持ち

寄って共有する方法のみであったが、LETTICE プロジェクトでは参画組織から希望者を募って脅威情報分析チーム LETTICE として活動することでの共同分析を目指している。現在初期メンバーによって活動方針の整理、活動に必要なツール・分析基盤の整備を行っている。

5　おわりに

本稿では、Co-Nexus A における大規模データ収集及び解析者コミュニティの形成に関する活動を紹介した。

サイバーセキュリティ研究室の研究開発成果である STARDUST、Co-Nexus A で開発している WarpDrive などの各種情報収集基盤は、情報収集・解析活動ならびに Co-Nexus A のコミュニティのフィードバックを活用し、継続して研究開発を進めている。変化の激しいサイバー攻撃の分析においては、このような利活用に基づいたフィードバックは必要不可欠である。

今後も研究開発成果の利活用を通じて参画組織での解析と情報共有を進め、国内のサイバーセキュリティ結節点として、日本のサイバー攻撃対応能力の向上に寄与していく。

【参考文献】

1　国立研究開発法人情報通信研究機構：プレスリリース — サイバー攻撃誘引基盤 “STARDUST”（スター ダスト）を開発 — NICT- 情報通信研究機構, https://www.nict.go.jp/press/2017/05/31-1.html
2　井上大介：サイバー攻撃誘引基盤 STARDUST 事後対応からリアルタイム対応, https://digitalforensic.jp/wp-content/uploads/2018/03/community2017-05-3inoue.pdf
3　津田 侑、“STARDUST による攻撃活動観測と次世代のセキュリティ技術, ” https://www2.nict.go.jp/csri/plan/H30-symposium/pdf/tsuda.pdf
4　Shota Fujii, Takayuki Sato, Sho Aoki, Yu Tsuda, Nobutaka Kawaguchi, Tomohiro Shigemoto, Masato Terada: “Stargazer: Long-Term and Multiregional Measurement of Timing/ Geolocation-Based Cloaking,” IEEE Access, vol.11, pp.52750–52762, 2023.
5　Akamai Blog, “Purple Fox Rootkit Now Propagates as a Worm,” https://www.akamai.com/blog/security/purple-fox-rootkit-now-propagates-as-a-worm
6　WarpDrive Project, https://warpdrive-project.jp
7　© 士郎 正宗・Production I.G/ 講談社・攻殻機動隊 2045 製作委員会
8　国立研究開発法人情報通信研究機構, “Web 媒介型サイバー攻撃対策プロジェクト「WarpDrive」を大型アップデート！,” https://www.nict.go.jp/press/2023/10/16-1.html
9　国立研究開発法人情報通信研究機構, “NOTICE,” https://notice.go.jp

安田 真悟（やすだ しんご）
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
CYNEX 研究開発運用室
室長
博士（情報科学）
アプリケーション検証環境、サイバー攻撃検証環境、サイバーセキュリティ人材育成
【受賞歴】
2022 年　2022 年度 JNSA 賞「特別賞」（Hardening Project）
2022 年　Good Design Award 2022（Hardening Project）
2017 年　MWS 2017 ベストプラクティカル研究賞

佐藤 隆行（さとう たかゆき）
株式会社日立製作所
セキュリティサービス本部
セキュリティプロフェッショナルセンタ
シニアセキュリティスペシャリスト／
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
協力研究員
サイバーセキュリティ
【受賞歴】
2023 年　2023 年度 CSEC 優秀研究賞
2022 年　FIT2022 FIT 船井ベストペーパー賞
2022 年　2022 年度 CSEC 優秀研究賞

毛利 公一（もうり こういち）
学校法人立命館
立命館大学情報理工学部
教授
博士（工学）
オペレーティングシステム、仮想化技術、コンピュータセキュリティ、組込みシステム
【受賞歴】
2021 年　CSEC 優秀研究賞
2016 年　辻井重男セキュリティ論文賞 特別賞
2014 年　MWS2014 優秀論文賞