Deloitte.
デロイト トーマツ

Deloitte Cyber Trends & Intelligence Report

2023

Dec 2023
デロイト トーマツ サイバー合同会社
Cyber Intelligence Center (CIC)

はじめに

2016年5月に日本にCyber Intelligence Center (CIC)を開設してから7年が経過しました。開設当初に比べるとお客様の数は大幅に増加し、それに伴い監視・分析に従事するメンバーも大幅に増員しています。3年目を迎える本レポートでは新たな執筆陣を迎え、2023年に顕著だった脅威情報を振り返ると共に、技術面を深堀ったコンテンツを用意しました。

「ランサムウェア脅威の動向」では、2019年よりCICが独自に統計を取り続けているリークサイトでのデータ公開件数を引き続き紹介します。2022年と比較して約2倍の公開件数になっていることから、2023年もランサムウェアの猛威が広がっていることを示しています。
「ランサムウェアとサプライチェーンリスク」では、供給網やクラウド事業者が提供するサービスがランサムウェアによって停止した事案を取り上げ、クラウド事業者選定基準についての考え方を紹介します。

「セキュリティログ監視における機械学習（教師なし学習）の活用」では、一般的になりつつある機械学習の中で、セキュリティ監視に取り入れやすい「教師データなし」の機械学習について、CICでの取り組みを紹介します。

「続・SOAR運用の舞台裏 ～運用する『人』と仕組み～」では、2022年のレポートでも取り上げたCICでのSOAR（Security Orchestration, Automation and Response）運用について、運用を担当する「人」について掘り下げた内容を取り上げます。自社でSOAR運用に取り組んでいる担当者向けと間口が狭いテーマですが、製品メーカーからはなかなか情報が出てこない内容であり、CICの運用ノウハウをお伝えするという観点から本レポートで取り上げることとしました。

「EDR製品による検知の限界と攻撃痕跡の調査」の背景には、2023年3月に活動を再開したEmotetの存在があります[1]。活動を休止していた理由は諸説ありますが、CICでの監視を通じ「検知回避」のテクニックが新たに実装されていることを確認しています。一般的にマルウェア・ランサムウェアに対しEDRは有効な手段と考えられていますが、検知回避策の実装により検知が困難になっていることを踏まえ、本章ではMITRE ATT&CK®を用い、5つのEDR製品での検知実績より攻撃手口（Tactics）ごとに得手・不得手があることを示しています。

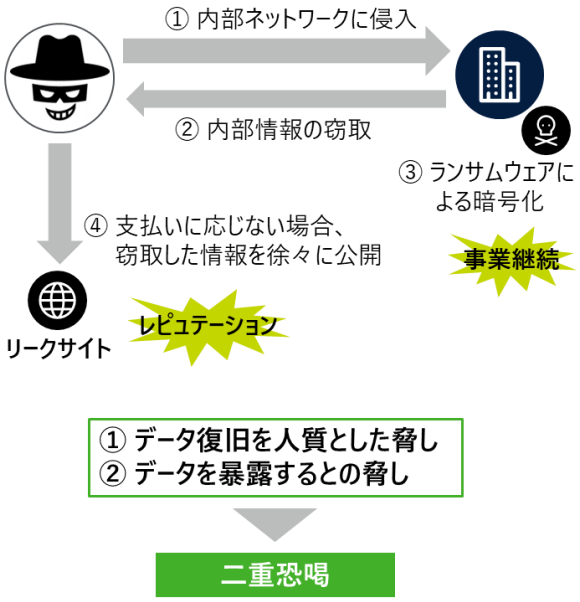
本レポートは広くセキュリティ業務に関与されている方々を対象としていますが、その中でも事業会社や同じセキュリティ業界でセキュリティ監視・分析業務やCSIRT業務に従事されている皆様の日々の業務に何らかのお役に立てば幸いです。

*1：情報処理推進機構,「Emotetの攻撃活動再開について（2023年3月9日）」, https://govoritmoskva.ru/news/351796/

ランサムウェア脅威の動向

ランサムウェア被害は2023年も引き続き世界中で発生しており、脅威が収束する兆しは見えません。
ランサムウェア攻撃の手口としては、システムの暗号化だけでなく被害組織からデータを盗み出し、金銭支払いに応じなければデータを公開すると脅す「二重恐喝」がますます一般的になっています（図表1）。攻撃グループがデータ公開のために運営しているリークサイトの数は、2023年にデータ公開が行われたものだけで約60に及びます。

図表1　二重恐喝ランサムウェアの手口

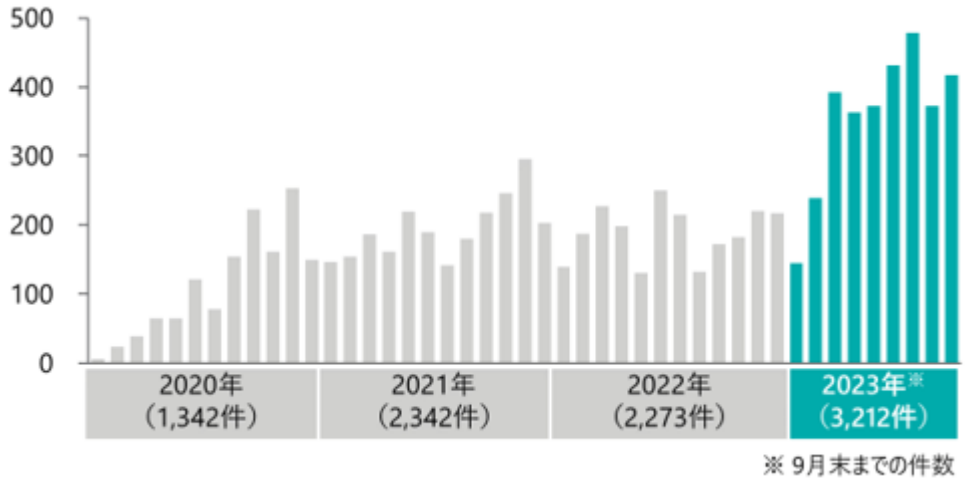


※ 二重恐喝はデータ公開という形で被害が可視化されることから、リークサイトにおけるデータ公開件数を見ることはランサムウェアの脅威を把握するうえで有効です。CICは、二重恐喝が使われ始めた2019年後半からリークサイトをモニタリングしており、被害組織の業種や国を集計しています。そこで本章では、CICによるリークサイトのモニタリング結果に基づき、データ公開状況からランサムウェア脅威の動向を解説します。ただし、リークサイトでのデータ公開は、攻撃グループが自身のサイトで攻撃に成功したと主張しているものであり、虚偽や誇張が含まれる可能性があります。データが公開されたことと、実際にランサムウェア被害が遭ったかはイコールではない点に留意が必要です。

二重恐喝ランサムウェアによるデータ公開被害の状況

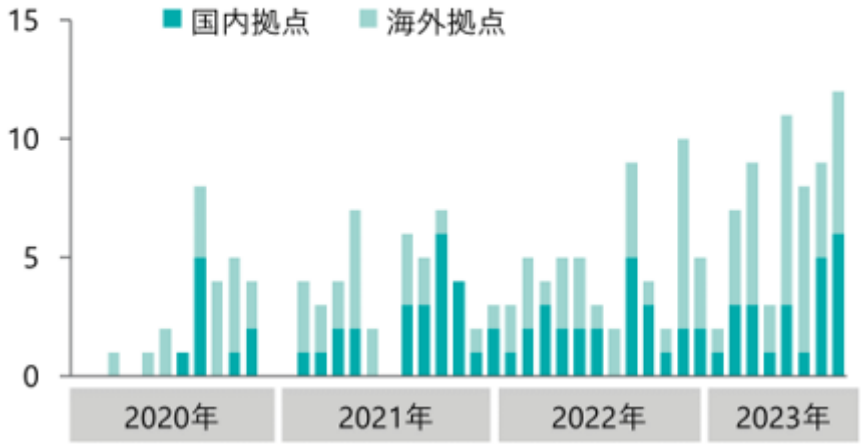
2023年のデータ公開件数は、前年までと比較して顕著に増加しています。
図表2は、リークサイトにおけるデータ公開件数を月ごとにまとめたものです。2022年ごろまでは月間200件前後だったのに対し、2023年、特に3月以降は月間400件近くになっています。
また、累計被害件数を見ると、2023年は9月末時点で前年を超える3,212件に及んでいます。

図表2　リークサイトでデータを公開された企業等の件数の推移



次に、日本企業のデータ公開被害件数を見てみましょう（図表3）。ここでは、国内拠点、海外現地法人の被害を合わせて日本企業の被害としています。世界全体ほど顕著な変化ではないものの、2023年3月以降に被害が増加している傾向が見られます。

図表3　日本企業のデータ公開被害件数の推移



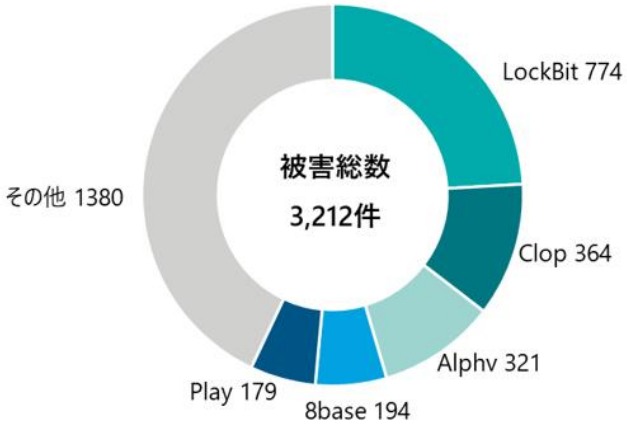
2023年3月からデータ公開件数が増加、すなわちランサムウェア攻撃が活発化している原因は明らかではありません。ただし、この増加はサイバー犯罪を巡るロシア国内の動きが関連している可能性が考えられます。
2023年2月、ロシアの通信社により、同国議会で「ロシア連邦の利益のためにサイバー攻撃を行う者の責任免除」が検討されていることが報じられました[2]。この議会での検討は法制化されたものではないものの、西側諸国などに対するサイバー攻撃が国家のお墨付きを得たと受け止めたランサムウェア攻撃グループが、活動をさらに強めた可能性が考えられます。

*2：Говорит Москва 94.8 FM, 'В Госдуме предложили не наказывать действующих в интересах России хакеров' https://govoritmoskva.ru/news/351796/

ランサムウェア攻撃グループ別の被害件数

ここでは、二重恐喝によるデータ公開被害について、ランサムウェア攻撃グループごとの被害件数を見ていきます。図表4は、2023年1月から2023年9月末までの間のデータ公開被害3,212件について、グループ別の件数を示したものです。

図表4　2023年の被害のうちランサムウェア攻撃グループごとの掲載件数



最も被害が多かったのはLockBitの774件で、全体の約24%を占めています。LockBitは、ファイル転送ソフトウェアGoAnywhere MFTや印刷管理ソフトウェアPaperCutの脆弱性を悪用した攻撃キャンペーンを行ったと見られています。

次に被害が多かったのはClopで、364件です。同グループは、ファイル転送ソフトMOVEitのゼロデイ脆弱性を悪用してデータを窃取し、多数の企業を恐喝しました。

このように、ランサムウェア攻撃グループが特定の脆弱性を悪用して大規模な攻撃キャンペーンを行うことは一般的になっています。こういった脅威に対応するには、脆弱性などの問題点がないよう、自組織の外部公開機器を管理することが重要です。
一方、外部公開機器を全て把握するのは容易ではなく、管理から漏れていたリモート接続機器から内部侵入された事例も複数見られます。

こうした状況を受けて、最近注目されているのがASM（Attack Surface Management）という取り組みです。ASMは自組織の外部公開機器に存在するリスクをインターネット側から評価するもので、外部から見ることで、これまで把握できていなかった機器の発見にもつながります。2023年5月には、経済産業省からも導入ガイダンスが公開されており、実施が推奨されています[3]。

*3：経済産業省,「「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」を取りまとめました」, https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

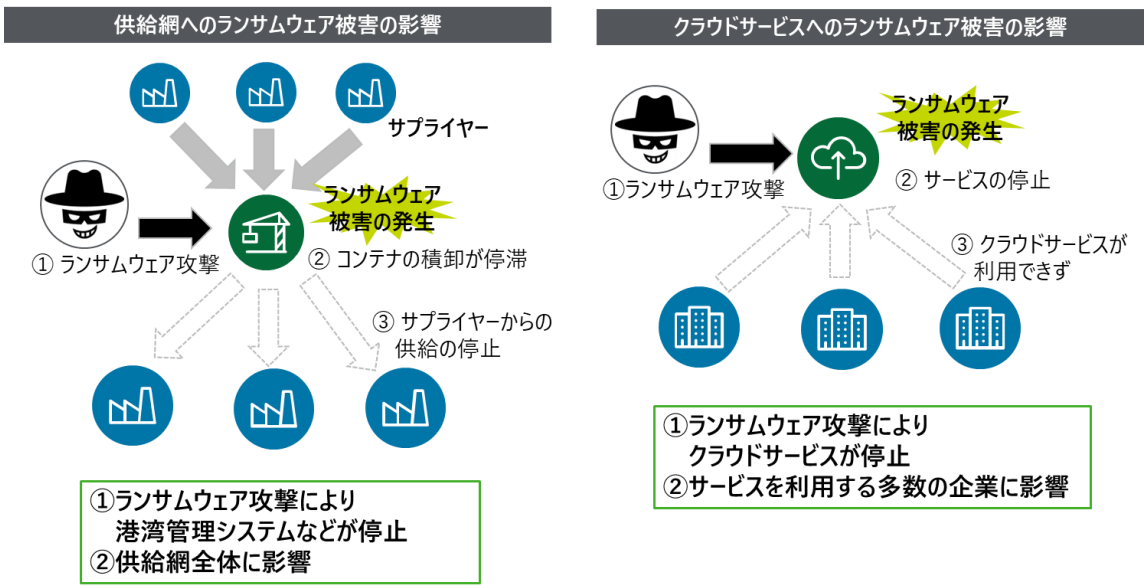
ランサムウェアとサプライチェーンリスク

ランサムウェアの被害に遭った組織では、事業に大きな支障をきたす可能性があります。被害組織が第三者にサービス提供を行っている場合、取引先や利用者にも大きな影響を及ぼします。

ランサムウェアの脅威の増大により、取引先などの被害によって自社の業務に影響が及ぶ「サプライチェーンリスク」が顕在化する可能性も高くなっています。実際に、2023年は国内でランサムウェア被害によりサプライチェーンリスクが顕在化した事例が複数見られました。

ここでは、2023年に国内で見られた事例として、「供給網の一時停止」と「クラウドサービスの停止」を取り上げます。

図表5　サプライチェーンリスクにつながるランサムウェア被害



供給網の一時停止

2023年7月、名古屋港で管理システムがランサムウェア攻撃を受け、2日間にわたってコンテナ作業が停止する事態が発生しました。
本事案を受けて国土交通省に設置された「コンテナターミナルにおける情報セキュリティ対策等検討委員会」の資料[4]によると、この被害の影響は次の通りです。

- 荷役スケジュールに影響が生じた船舶37隻（最大 24 時間程度の遅延が発生）
- 搬入・搬出に影響があったコンテナ約2万本（推計）
- 自動車メーカーにおけるいくつかの工場の稼働停止
- アパレルメーカーにおける衣類の入荷遅延

名古屋港は貨物取扱量で国内1位の港湾であり、コンテナ作業停止の影響の大きさがうかがえます。

ただし、名古屋港における約2日でのシステム復旧は、ランサムウェア被害としては早い部類に入ります。警察庁の資料[5]によると、国内のランサムウェア被害組織において1週間未満で復旧できたのは27%です。また、海外で発生した港湾のランサムウェア被害では、復旧に10日以上かかった事例も見られます[6]。
2日間の作業停止であったものの、それ以上の事態が生じる可能性は十分あります。

今回紹介した港湾のほか、部品メーカー、業務委託先、運送会社などがランサムウェア被害に遭い、供給網の一部が途絶して自社に影響が及ぶというサプライチェーンリスクに対応するには、BCP（事業継続計画）の策定が有効です。

供給網の途絶が自社に与える影響は、その原因がランサムウェア被害であっても自然災害であっても基本的に変わりはありません。このため、すでに供給網の途絶に備えたBCPを策定している場合、新たなものは必要ありません。

ただし、サイバー攻撃はいつ、どの組織で被害が生じるか予測できない点には注意が必要です。
サプライチェーンリスクを考える場合、政治、国際情勢、災害などの観点でリスクが高いシナリオを想定し、これに基づきBCPを策定するのが一般的と考えられます。
一方、サイバー攻撃では被害の生じやすい箇所を特定するのは困難です。このため、既存のBCPがあるとしても、想定している脅威シナリオ、具体的には供給網が途絶する箇所に考慮漏れがないかは点検する必要があります。

*4：国土交通省,「名古屋港のコンテナターミナルにおけるシステム障害を踏まえ 緊急に実施すべき対応策について（案）」, https://www.mlit.go.jp/kowan/content/001633384.pdf
*5：警察庁,「令和 5 年上半期におけるサイバー空間をめぐる脅威の情勢等について」, https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf
*6： IAPH 国際港湾委員会, 'IAPH Cybersecurity Guidelines for Ports and Port Facilities Version 1.0', https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf

クラウドサービスの停止

2023年6月には、国内の3つのクラウドサービス事業者で立て続けにランサムウェア被害が発生し、サービス提供への支障が生じました。各社の提供するサービスとランサムウェア被害の影響は図表6の通りです。

図表6　国内のクラウドサービス事業者におけるランサムウェア被害の影響

	提供サービス	影響範囲
A社	社会保険労務士向け クラウドサービス	社会保険労務士 事務所2,700以上
B社	LPガス事業者向けの クラウドサービスなど	LPガス会社 1,100社以上
C社	ファイル転送サービス、 メール暗号化サービスなど	国内1,000社以上

被害企業のうちC社は、ランサムウェア被害の原因としてメンテナンス用VPN機器の脆弱性を悪用された可能性が高いことを明らかにしています。
このように、クラウドサービス事業者であっても脆弱性管理の抜け・漏れなどによってランサムウェア被害に遭うことはあり得ます。利用者側に対応の責任がないとしても、クラウドサービス事業者が被害に遭い、サービス提供を受けられなくなる可能性は考えておく必要があるでしょう。

ランサムウェア被害などによるクラウドサービスの停止に対し、利用者側でできる対策は「安全性の高いサービスの選定」と「クラウドサービスの障害を想定したBCPの策定」です。

クラウドサービスに障害が発生した場合、利用者側でサービス復旧のためにできることはありません。このため、安全性の高いサービスを選定し、サービス停止が発生する可能性を低減することが重要です。
安全性の高いサービスの選定にあたっては、図表7のような認証制度が参考になります。クラウドサービスの選定にあたっては、候補となるサービスの提供事業者がどのような認証を取得しているかも評価項目とすることが有効です。

図表7　クラウドサービス事業者の認証制度など

認証制度など	概要
ISMSクラウド セキュリティ認証	通常のISMS認証（ISO/IEC27001）に加え、ISO/IEC27017に規定されたクラウドサービス固有の管理施策が導入・運用されていることを認証
クラウド情報セキュリティ 監査制度	■ クラウドサービス事業者における情報セキュリティ対策の状況を監査 ■ 安全性が確保されていると認められた事業者は、CSマークの表示を許可される
ASP・SaaS情報開示 認定制度	クラウドサービス事業者が安全・信頼性に関する評価のために必要な情報を開示していることを認定する制度
ISMAP	政府が求めるセキュリティ要求を満たすクラウドサービスを評価・登録する制度

ただし、こうした認証制度は事業者のセキュリティ体制などを評価するものであり、認証を取得しているからといってサイバー攻撃被害に遭わないことを保証するものではありません。
サービスの長期停止につながるランサムウェア攻撃への対策、特にバックアップの態勢などは、可能であれば事業者に確認することが望ましいと言えます。

また、クラウドサービスが停止した場合に備えてBCPを策定しておくことも有効です。自社の業務において重要なクラウドサービスが長期間利用できなくなる事態を想定し、代替手段などを決めておくことで業務への影響を低減することができるようになります。

セキュリティログ監視における機械学習（教師なし学習）の活用

CICは、SIEM（Security Information and Event Management）を利用してセキュリティ脅威を検出し、それらの分析・通知を行う監視サービスを24時間365日体制で行っています。セキュリティ脅威を検出するアプローチの一つとして機械学習の活用が挙げられますが、その学習方法によって「教師なし学習」と「教師あり学習」の二つに分けることができます。本章では、教師なし学習のセキュリティログ監視への活用事例と、活用する際のポイントを解説します。

教師なし学習の活用事例

教師なし学習とは、データの中から共通項や特徴を見つけ出してグループ分けを行う技術であり、異常なデータや外れ値といった特異点を見つけるために有効な技術です。図表8は、教師なし学習を活用したセキュリティ脅威の検知例について、それぞれ想定しているシナリオや検知の要件となる事項をまとめたものです。

図表8　セキュリティ脅威の検知例と検知の要件

セキュリティ脅威の検知例	想定シナリオ	検知の要件
Active Directoryにおける異常な認証試行	端末がマルウェアに感染し、大量の認証試行が試みられる	平時とは異なる大量の認証試行があった場合に検出する
プロキシにおけるデータサイズの大きいファイルのアップロード	端末がマルウェアに感染し、大量のデータの情報漏洩が試みられる	平時とは異なる大量のデータサイズのアップロード試行があった場合に検出する
Webアプリケーションにおける同一情報の異常な登録	Webアプリケーションの不正利用者が、攻撃者の所有する情報に変更し、不正な操作を試みる	平時とは異なる大量の同一登録があった場合に検出する

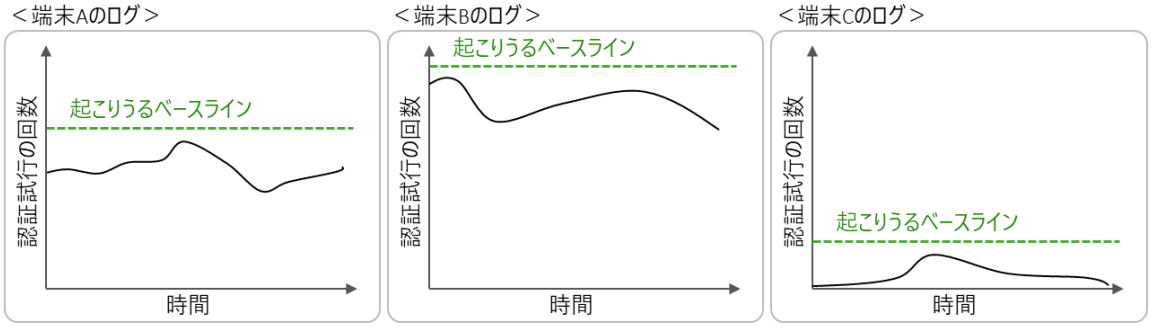
CICでは検知の要件をもとに、教師なし学習をリアルタイムの監視に活用しています。これらの監視を実現するためには、「異常スコアの判定法」と「チェックする時間間隔」を整理することが重要です。次節では、これらの必要性について、Active Directoryのログ分析を一例としてまとめます。

セキュリティ脅威を検出するアプローチ

異常スコアの判定法

図表8の「Active Directoryにおける異常な認証試行」にまとめた通り、「平時とは異なる大量の認証試行があった場合に検出する」ことが、検知の要件となります。この検知は、教師なし学習の機能を用いて、端末ごとの起こり得る認証試行の回数をベースラインとして定め、ベースラインを超えたものを異常な回数として検知することにより実現できます。このように「端末ごと」や「認証試行の回数」といった条件が異常スコアの判定法となります。図表9は、教師なし学習の機能を用いて、端末ごとの認証試行回数におけるベースラインを定めるイメージを示したものです。

図表9　端末ごとのベースライン策定イメージ



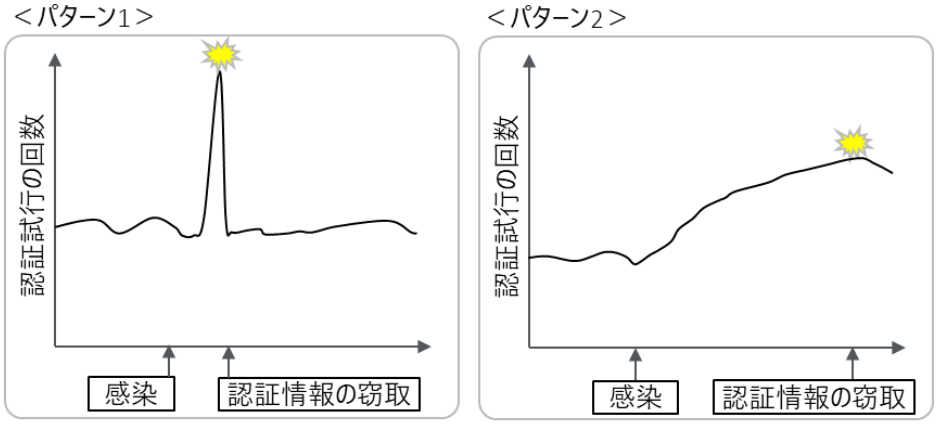
それぞれの端末は、業務内容などにより平時から認証する回数が異なります。そのため、異常と判断するためのベースラインは端末によって異なることから、それぞれベースラインを設ける必要があります。実際の環境では対象となる端末は多数存在することが大半であり、個々のベースラインを静的なしきい値として設定することは現実的ではありません。教師なし学習を利用することで、端末ごとに認証試行回数のベースラインを定めて検知することが可能となります。

このように、検知したいセキュリティ脅威や想定シナリオから異常スコアの判定法を整理してルールに反映することが、教師なし学習を活用するうえで重要となります。

チェックする時間間隔

図表10は、端末がマルウェアに感染し、そのマルウェアが別のアカウントの認証情報を窃取するまでの時間と、認証試行の回数の想定例をまとめたものです。

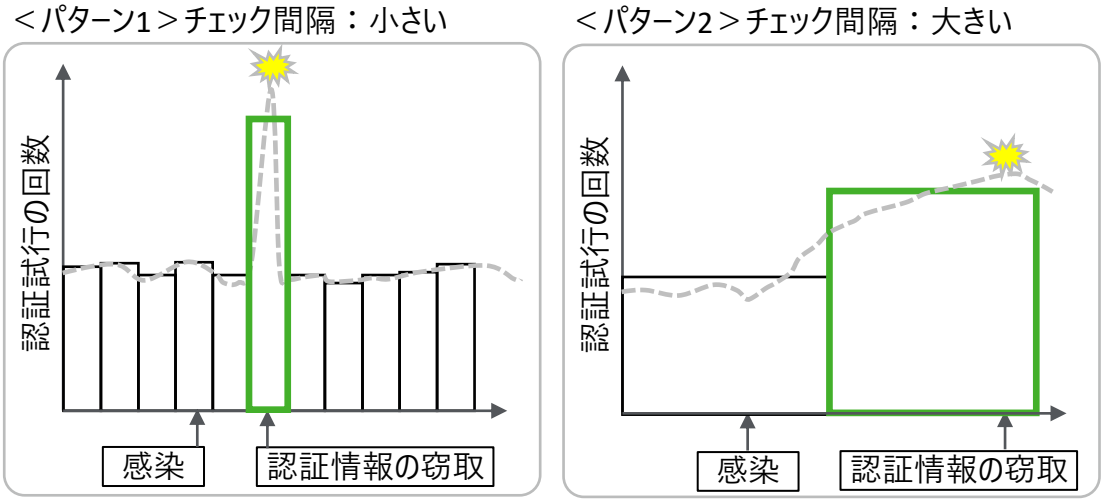
図表10　マルウェアが認証情報を窃取するまでの想定される認証試行回数の例



パターン1では短期間による大量の認証により推測を試みるのに対し、パターン2では比較的長期間で認証情報の推測を試みていることが分かります。双方とも異常な認証試行であることから、教師なし学習の効果が期待できるものの、挙動としては大きく異なることから、捕捉するための条件設定では考慮が必要となります。

図表11は、図表10で示した想定するログに対する教師なし学習の判定イメージを示したものです。

図表11　教師なし学習の判定イメージ



教師なし学習のルールを設計する際のポイントの一つとして、チェック間隔の設定があります。図表11にまとめた通り、チェック間隔の大きさに応じて、その間隔内に含まれる認証試行回数の合計を算出し、合計値がベースラインを超えた場合に異常と判定します。同図表に示すように、チェック間隔を小さく設定すると短期間における異常を検出することができ、逆にチェック間隔を大きく設定すると長期間における異常な傾向を明らかにすることができます。このチェック間隔を適切に設定できないと、誤検知や検知漏れを引き起こす懸念があります。そのため、具体的なチェック間隔は、平時の業務利用による増減の傾向や攻撃時に行われる特徴を踏まえて適切な値を設定する必要があります。

セキュリティ脅威を検出する実現例

前節では、脅威を検出するアプローチについて説明しました。本節では、そのアプローチをふまえて、図表8の「Active Directoryにおける異常な認証試行」を一例に、セキュリティ脅威の検出を行うための具体的な対応内容を紹介します。

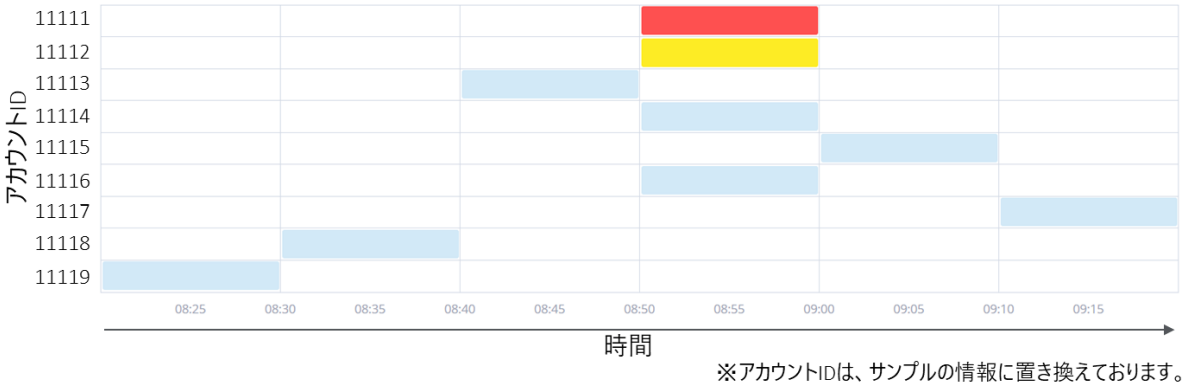
図表12　セキュリティ脅威の検出を行うための対応内容

Step	概要	具体例
1	異常スコアの判定法の整理	Active Directoryのログから、「カウントすべきセキュリティイベントID」や「アカウントIDごと」といった異常スコアの判定条件について整理する
2	学習ルールの実装とモデルの作成	Step1で整理した内容をもとに学習ルールを実装する。SIEMに格納済みのログを最低3か月分※学習させることにより、ベースラインを策定したモデルを作成する
3	チューニングの実施	モデルの結果を確認し、必要に応じてチェック間隔の変更や、学習対象外とする条件などのチューニングを行う。チューニング後にStep2のモデルの再作成を行う
4	ログ監視の実施	SIEMに随時格納されたログに対して、作成したモデルをもとに異常スコアを算出し、異常と判定されたものがあれば検知する
5	検知内容の分析	異常と判定された事象がセキュリティ脅威に直結するとは限らないため、検知内容の分析を行う。具体的には、検知前後のActive Directoryログや他のログを調査し、マルウェア感染などの内部侵害の疑いがないか調査する

※一定のログ量が無いと、モデルが不安定で検知精度に課題が残るため

図表13は、CICで実際にActive Directoryにおける異常な認証試行を検知した例を示したものです。

図表13　異常な認証試行の検知内容



※アカウントIDは、サンプルの情報に置き換えております。

縦軸がアカウントIDの一覧となっており、横軸が時間となります。異常スコアの判定値が高くなるにつれて、「水色」「黄色」「赤色」に分類されます。同図表より、アカウントID「11111」が特定の時間帯で、異常な認証試行があったことが分かります。CICは、図表12のStep1～Step5の内容を全て行い、最終的なセキュリティ脅威の判定を行っています。

まとめ

本章では、教師なし学習のセキュリティログ監視への活用事例と活用する際のポイントについて紹介しました。教師なし学習を監視に活用するためには、「異常スコアの判定法」と「チェックする時間間隔」の双方の整理が必要であることを解説するとともに、CICで実際に行っている実現例について紹介しました。また、これらの要件を適切に整理するためには、製品特性や実際に行われた攻撃事例の特徴把握といったノウハウが必要となります。自社ですでにSIEM運用をしているものの、こういったノウハウを蓄積することが難しい場合は、SOCのアウトソースによって監視の高度化を図ることも選択肢の一つと考えます。

続・SOAR運用の舞台裏 ～運用する「人」と仕組み～

2022年に発行した「Deloitte Cyber Trends & Intelligence Report 2022」では「SOAR運用の舞台裏 ～自動化するということ～」という題で、SOARの概要から導入における注意事項、具体的なプレイブックの実装について取り上げました。本章ではSOARを運用するにあたって必要な役割や、CICでの具体的な運用方法について紹介します。

必要なロールと人員を明確にする　～SOARの運用を支える人々～

SOARを導入した直後や、SOARの導入を検討する中で「どこから手をつければよいのか」や「どのような準備が必要か」について迷う方は多いのではないのでしょうか。CICでもSOAR導入初期には「誰が」「何を」「どうするのか」という点が曖昧なケースがあり、SOARを活用する段階でオペレーションが混乱するという事象が見られました。

本節では、安定した運用を実現するためにCICで実践しているタスクや役割を紹介します。CICではSOAR運用にあたって管理者、開発者、プレイブック作成者の3種類のロールを定義しています。それぞれのロールに求められる知識や実際に行うタスクを図表14に整理しました。

図表14　SOARを運用するロールと求められる知識／スキル

青字：必須のスキル
黒字：あると望ましいスキル

	ロール概要	タスク	求められる知識 / スキル
管理者	SOARを導入しているハードウェアやソフトウェア・ユーザーの管理を行う	• アップデート対応 • ユーザー管理 • 障害対応	• OSの基本的理解 • アプリケーション/OSのエラーハンドリング • リソース冗長化等の構成の知識
開発者	未実装の機能の開発を行う	• 新機能の設計/実装 • プレイブック作成者と連携した実装作業 • 開発成果物のドキュメント作成	• オブジェクト指向やデザインパターンに対する基本的な知識 • コード管理システムの理解
プレイブック作成者	SOAR上でプレイブックを作成する ※プレイブックとは、業務フローをSOAR上で実行可能な処理に実装したもの	• プレイブック実装対応 • プレイブック完成後のリリース周知対応	• ログ分析業務の知識 • 簡易なスクリプト言語の理解

管理者や開発者については、他のソリューションを運用する場合と同様のスキルセットが求められますが、プレイブック作成者は、SOARを用いて自動化を行う業務フローの運用者が担当している点に注意が必要です。

プレイブック作成者と開発者をロールとして分けた理由

プレイブック作成者と開発者を明確にロールとして分離していることについては理由がいくつか存在します。CICも導入当初は2つの役割を分離していませんでしたが、運用していく中で次のような問題が発生しました。

- SOARの開発をメインで行う担当者は、普段SOAR化対象となる業務に直接携わっていないため、最新の業務フローの把握に時間を要していた
- プレイブックを実装するには運用が標準化されている必要があるが、業務担当者と開発担当者の間で行う情報整理の負荷が高かった
- 業務フローへの理解が十分でないために、プレイブックを実装した後に実際の運用に即していない部分が判明し、手戻りが発生していた

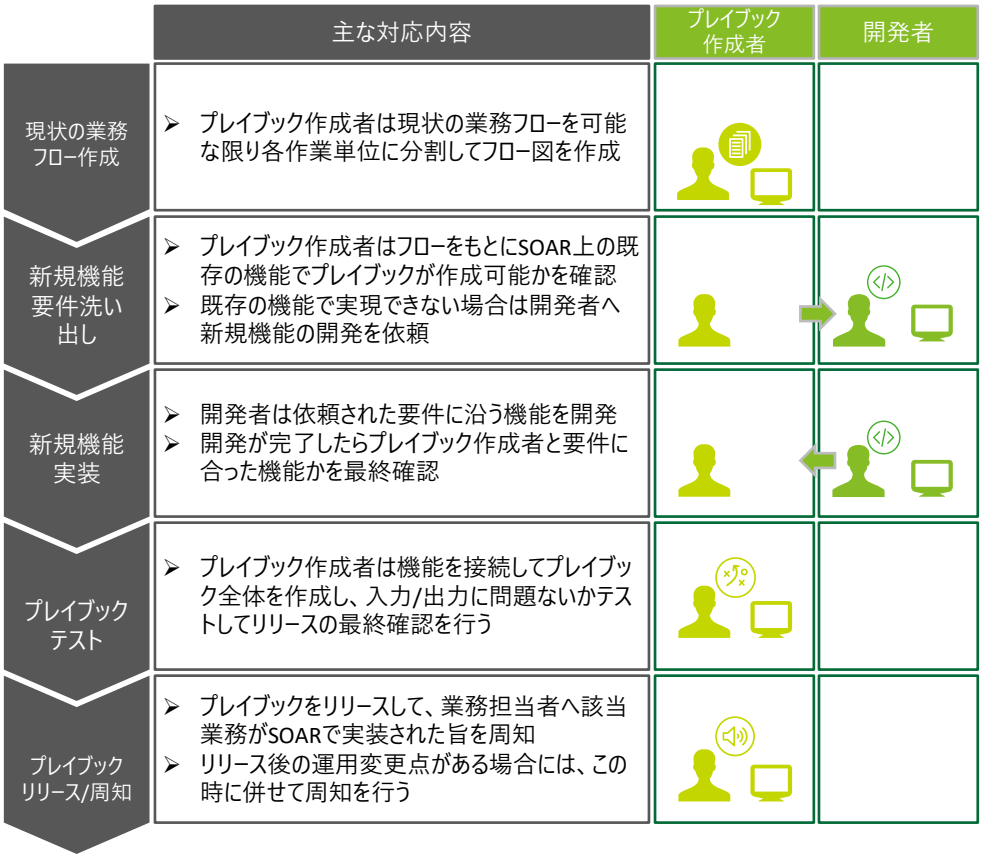
上記から、プレイブック作成者は実際にログ分析を担当しているメンバーが適切であると判断しました。

業務プロセスを明確にする　～運用のイメージはできているか～

前節ではSOARを運用するにあたって必要な人員やタスクについて紹介しました。本節ではSOAR特有の運用部分であるプレイブックの作成を、CICではどのように行っているのかを紹介します。

CICでは、プレイブック作成者はログ分析業務の知識をもとにプレイブックを作成し、新規機能を実装する必要がある際には開発者が機能開発を行います。イメージをしやすいように、現状のプレイブックリリースまでの流れを図表15に示します。

図表15　プレイブックリリースまでの業務プロセス



同図表の流れのように、運用の実態を知るプレイブック作成者と開発者を分離して互いが運用メインと開発メインのそれぞれのタスクにリソースを注力できる体制としました。これにより、プレイブック作成者と開発者を分離する前よりも開発の手戻りを抑え、プレイブックを作成する時間を短縮することができました。

加えて、プレイブック作成者は該当機能の仕様を把握しておけば、基礎的なプログラミング言語の知識のみでプレイブックが作成可能であり、開発者とプレイブック作成者に求められる能力も上手く分離できていたのも特筆すべき一つの特徴です。

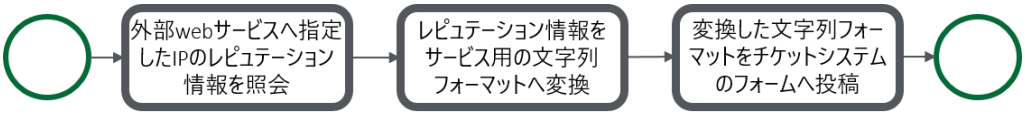
具体例を交えてロールの各動きを説明

日々セキュリティアラートの分析をしているアナリストは、検知されたIPのレピュテーション情報を外部サービスで確認を行い、自社のチケットシステム上に入力するタスクを手動で行っていました。今回はそのタスクの自動化を例に、プレイブックの作成法を紹介します。

業務のフロー化／必要な機能の洗い出し

まずはプレイブックを作成するにあたり、プレイブック作成者にあたるアナリストが一連の手順をフローチャートに落とし込みます。

図表16　一連の手順のフローチャート



フローチャートの作成が完了したところで、各業務プロセスに必要な機能の洗い出しを行います。
この時、既に実装されている機能と新規に開発が必要な機能を洗い出しておきましょう。

図表17　必要機能の洗い出し結果

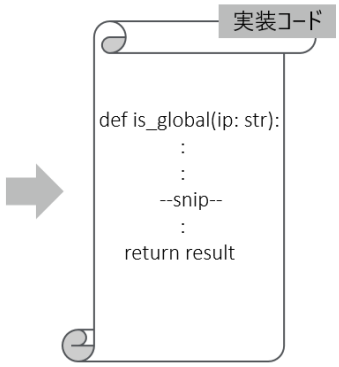
業務プロセス	機能洗い出し結果
外部webサービスへ指定したIPのレピュテーション情報を照会	新規機能 IPアドレスをグローバルIPかプライベートIPか判別する機能 HTTPリクエストを送出し、レスポンスを取得する機能
レピュテーション情報をサービス用の文字列フォーマットへ変換	定型文字列を任意の文字列へ加工を行う機能
変換した文字列フォーマットをチケットシステムのフォームへ投稿	チケットシステムのフォームの値を更新する機能

新規機能の開発依頼

新規に開発が必要な機能については開発者へ開発依頼を行い、開発者は要件に沿うコードの開発を行います（CICのSOARではPythonでの実装をサポートしているため、Pythonで開発を行います）。

図表18　必要機能の洗い出し結果

開発項目	内容
目的	IPアドレスを入力値としてグローバルIPかどうかを判定させる機能
入出力内容	入力値: IPアドレス 出力値: True/False
例外処理	入力値がIPアドレスフォーマットではない/IPアドレスで定義される範囲外の値である場合には処理停止を行う

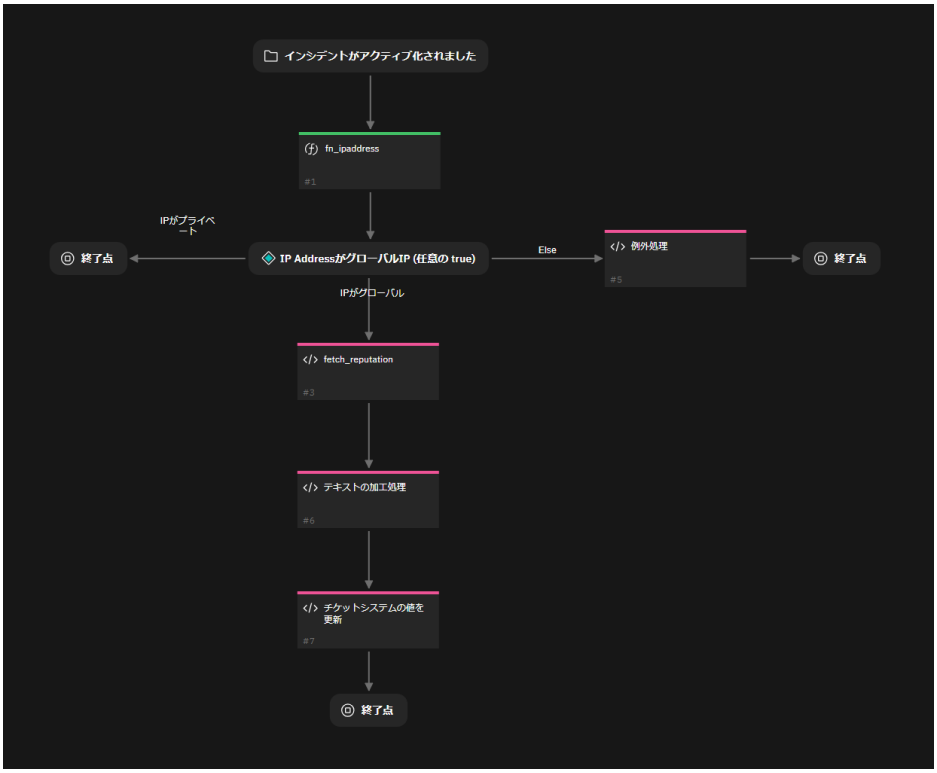


開発者はコードの実装が完了した後にプレイブック作成者に連絡を行います。

プレイブックの作成

必要な機能の実装が一通り完了したら、プレイブック作成者は各機能を接続してプレイブックを完成させます。

図表19　作成完了したプレイブック



リリース周知

正常系や異常系のテストで意図した結果を得られた後は、プレイブック作成者がSOARでの運用開始リリースを行います。この時、特定業務が自動化されることへの注意点や、SOARの処理が例外終了した際の手順も併せて周知します。

以上、SOARでプレイブックを作成する際の動きについて具体例を交えて説明しました。本章で実際にプレイブックを作成する際のイメージをつかめていただけたら幸いです。

まずはスモールスタートから　～運用してみないと分からないことも～

さて、ここまでSOARに関わる人員や、彼らがどのような関係性でプレイブック作成をしているのかを説明しました。後は実際に始めるだけですが、まずは分析手順がシンプルなものや、過去の対応から手順がある程度定型化ができているアラートに対するプレイブックから作ることをお勧めします。

2022年のレポートでも記載していますが、「手順が複雑」「高度な判断が伴う」「取得するイベントが時間経過で若干変わる」といったものは、プレイブックの作成は困難を極めます。

製品仕様を理解するといった意味でも、作成難易度が低い業務フローからプレイブック化を行い、徐々に高度な業務フローのプレイブック化を検討することがSOARの安定した運用への近道であると考えます。

また、新規の業務フローが追加される際に、運用開始前にSOARで実装を行ったところ実際には該当業務の発生頻度が少なく、SOARからの恩恵をあまり受けられないといった失敗もありました。

こういった失敗を防ぐためにも、すでにある運用の中から作業者の負荷が高い、または発生頻度の高いオペレーションからSOARでの自動化を検討していくことをお勧めします。

最後に

今回はSOARを活用する上でCICがどのような人員を各タスクに振り分けて運用をしているかを紹介しました。CICではSOARを運用してから1年が経過しており、紆余曲折を経ながらも安定した運用を実現しています。本稿が、これからSOARを運用する、またはすでにSOARを運用している方々にとっての参考となれば幸いです。

EDR製品による検知の限界と攻撃痕跡の調査

昨今、多くの組織でEDR（Endpoint Detection and Response）製品の導入が進んでいます。一方で、攻撃者側はEDR製品に対し、さまざまな検知回避策[7]を日々編み出しています。本章ではEDR製品による検知の限界と、同製品では検知が難しい攻撃に関する痕跡の調査方法を紹介します。

EDR製品は「万能」か？～EDR製品による検知の限界～

MITRE Engenuity ATT&CK®Evaluationsでは、現実の攻撃を再現して各社EDR製品における検知能力を評価しています。CICは、このセキュリティソリューションを評価するテストをもとに攻撃手口ごとの検知精度、および検知対象ログソースごとの検知イベント数を調査しました。

まず攻撃手口ごとの検知精度に関しては、図表20に示すように「実行」「権限昇格」「影響」の項目については概ね検知精度が高いことが分かります。一方で「コマンド&コントロール」「認証情報アクセス」「探索」など一部の項目については、製品によっては検知精度が低い場合があります。

図表20　攻撃手口ごとの検知精度

攻撃手口(Tactics)	検知精度				
	A社	B社	C社	D社	E社
収集	中	中	中	中	中
コマンド&コントロール	高	低	高	高	低
認証情報アクセス	高	低	高	高	低
防衛回避	高	中	高	高	低
探索	中	低	低	高	低
実行	高	高	高	高	中
持ち出し	高	中	高	高	中
影響	高	高	高	高	中
ラテラルムーブメント	高	中	高	高	中
永続化	高	中	高	高	中
権限昇格	高	高	高	高	中

参照：MITRE Engenuity ATT&CK®Evaluations[8]

*7：一例として次が挙げられる。Cybersecurity and Infrastructure Security Agency “People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection”, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

*8： MITRE “Wizard Spider + Sandworm ”, https://attackevals.mitre-engenuity.org/enterprise/wizard-spider-sandworm

また、ログソースごとの検知イベント数を見てみると、図表21に示すように「プロセス」「ファイル」「ネットワーク通信」の項目で多く検知しています。他方、Windowsの「ログオン・セッション」「Active Directory」「ネットワーク共有」といったWindowsイベントログに痕跡が残る項目では、攻撃試行の検知が少ない傾向にあります。

図表21　ログソースごとの検知イベント数（一部抜粋）

検知対象ログソース	検知イベント数				
	A社	B社	C社	D社	E社
プロセス	多	多	多	多	多
ファイル	多	多	多	多	多
ネットワーク通信	多	多	多	多	多
ログオン・セッション	少	少	少	少	少
Active Directory	少	少	少	少	少
ネットワーク共有	無	少	少	無	無

参照：MITRE Engenuity ATT&CK®Evaluations

以上の調査結果より、EDR製品には不得意な分野もあり、攻撃試行の中にはEDR製品では検知が難しいものがあることがうかがえます。

EDR製品の検知が難しい理由とは？～検知回避のメカニズムと攻撃痕跡の調査～

EDR製品での検知が難しい理由は、どこにあるのでしょうか。ここでは、4つの攻撃例をもとに検知回避のメカニズムを説明します。また、EDR製品で検知が難しい攻撃の痕跡を調査する方法も併せて紹介します。

OS正規ツールの悪用

攻撃手法、検知回避のメカニズム

OS正規ツールが悪用される事例としては、Windowsの管理ツール「WMI（Windows Management Instrumentation）」を利用する手法が挙げられます。攻撃者はWMIを侵害環境での探索行為やC2サーバーとの通信等に利用することがあり、その際、EDR製品ではWMIの利用がユーザーの意図したものであるか判別することができず検知されない可能性があります。

攻撃痕跡の調査方法

OS正規ツールの悪用痕跡を調査する際は、通常と異なるツールの利用状況を確認することが重要なポイントとなります。IcedID[9]など一部のマルウェアでは、侵害した端末上で動作するアンチウィルス製品を判別するためにWMIを利用することが知られています。そのため、通常そのような目的でWMIを利用しない環境において、製品の探索や情報収集に関する挙動が確認された場合は、マルウェアによるものである可能性があります。

不審なプロセスによる機微情報へのアクセスが可能なDLLファイルの読み込み

攻撃手法、検知回避のメカニズム

機微情報へのアクセスが可能なDLLファイルの例としては、Microsoft Entra ID （旧 Azure Active Directory）のPRT（Primary Refresh Token）[10]取得に利用されるDLLファイル[11]「MicrosoftAccountTokenProvider.dll」が挙げられます。当該DLLファイルは通常ブラウザソフト等によって読み込まれますが、Azure環境へのアクセスに必要な認証情報の窃取を目的として、マルウェアが当該DLLファイルを読み込んで悪用するとのリスクが指摘されています[12]。この場合も、EDR製品ではDLLファイルの読み込みが正常な挙動であるか識別できないことから検知されない可能性があります。

*9：Cybereason “【脅威分析レポート】すべての道はCobalt Strikeに通じる – IcedID、Emotet、QBot”, https://www.cybereason.co.jp/blog/malware/7797/
*10：シングルサインオン用トークン。Microsoft “プライマリ更新トークンとは”, https://learn.microsoft.com/ja-jp/entra/identity/devices/concept-primary-refresh-token
*11：Windowsにおいて複数のプログラムでコード、データを共有するライブラリファイル
*12：GMOサイバーセキュリティ byイエラエ,「Azure AD参加端末におけるPRT (Primary Refresh Token)悪用のリスクと対策について」, https://gmo-cybersecurity.com/blog/azuread-prt/

攻撃痕跡の調査方法

不審なプロセスによる機微情報へのアクセスが可能なDLLファイルの読み込みを調査する際は、利用の用途が不明なプロセスによるDLLファイルの読み込みを確認することが重要なポイントとなります。例えば、通常、実行ファイルが格納されることのないフォルダ上で実行されているプロセスによる「MicrosoftAccountTokenProvider.dll」の読み込みが確認された場合、マルウェアが不正に認証情報を取得しようとしている可能性があります。

プロセスハロウイング

攻撃手法、検知回避のメカニズム

プロセスハロウイング（Process Hollowing）は、正規プロセスを不正コードに改ざん、実行することでセキュリティ製品の検知を回避する手法です。例えば攻撃ツールCobalt Strikeは、プロセスハロウイングにより実行ファイルrundll32.exeをCobalt Strike本体に改ざんする場合があります[13]。

攻撃痕跡の調査方法

プロセスハロウイングでは、プロセスの中身が不正コードに変わるため、コマンド実行時に当該コマンドでは未実装のコマンドライン引数を使用する痕跡が残る場合があります。上記のCobalt Strikeの場合、rundll32.exeは通常実行する際は次の1のように引数として実行ファイル名、関数名を入力します。しかし、改ざん後は引数が不要となるため2のように引数を指定せず実行します。

① 正常なコマンドライン

- rundll32.exe printui.dll,PrintUIEntry
  （printui.dll：実行ファイル名、PrintUIEntry：関数名）

② Cobalt Strikeによる改ざん後のコマンドライン

- rundll32.exe
  （引数が存在しない）

このように、実行時に必要な引数を指定していなかったり、本来の仕様では存在しない引数を指定していたりするコマンドの実行はマルウェアによる挙動である可能性があります。

Windows認証の悪用

攻撃手法、検知回避のメカニズム

Windows認証を悪用する攻撃の事例としてPass the Hash攻撃があります。これは、窃取した別ユーザーのNTLMハッシュ（認証情報）を用いてそのユーザーになりすます攻撃です。Pass the Hash攻撃は、特定の攻撃ツールを使用した際にWindowsイベントログに攻撃痕跡が残ることを確認しています。しかし、図表21で示したように、EDR製品ではWindowsイベントログに痕跡が残る攻撃試行の検知が難しい可能性があります[14]。

攻撃痕跡の調査方法

通常、Windowsのログオンイベント（イベントID: 4624）では、ログオンプロセスには「Kerberos」「Advapi」などが出力されますが、攻撃ツールMimikatz（バージョン: 2.2.0）を使用してPass the Hashを実行した場合は「seclogo」が出力されることを確認しています（図表22）。そのため、このようなログオンイベントが確認された場合はPass the Hashを試行した際の痕跡である可能性があります。ただし、runasコマンドを実行した際にもログオンプロセスとして「seclogo」が出力されるため合わせて当該コマンドの実行の有無や、それが意図した挙動であるかの調査が必要です。

図表22　Mimikatz実行時のWindowsのログオンイベント（イベントID:4624）

*13：Fortra “Beacon Command Behavior and OPSEC Considerations”, https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide/content/topics/appendix-a_beacon-opsec-considerations.htm

*14： 通常、EDR製品は、攻撃ツールのファイルや実行コマンドよりPass the Hash攻撃を検知しているが、難読化などにより、これらの検知は無効化される可能性がある

安心・安全のためにできること～EDR製品で検知が難しい攻撃の定期的な調査～

これまで説明してきたように、EDR製品では検知が難しい攻撃があり、EDR製品の検知は万能ではありません。そのため、EDR製品の不得意分野を補完する調査を日々のセキュリティチェックに組み込むことは有用です。このような調査は、一見すると通常イベントと変わらない挙動から、特定環境での利用状況、およびプロセスや認証における仕様の視点から異常動作を見つける作業となります。

またEDR製品によってはWeb APIを使用した調査も可能であるため、手動だけでなくスクリプトによる自動化も可能です。

CICは、EDR製品で検知が難しい攻撃試行の痕跡調査手法を日々検証し、新たな脅威に対応しています。皆様の環境においても本節の事例をご参考にしていただければ幸いです。

おわりに

今回のレポートでは「脅威インテリジェンス」「セキュリティ監視・分析」「運用」の三つの観点から最新の動向を紹介しました。いずれもCICを構成する重要な領域となりますが、当然それぞれ独立して存在しているのではなく、相互に補完し合ってサービスの質を高めています。「EDR製品による検知の限界と攻撃痕跡の調査」で紹介したように、特定の製品でカバーできる範囲には限界があります。複数のログを組み合わせたり異常値を抽出したりすることで、各製品の不得意分野を補うことが必要となってきます。また、これらの分析に関わる一連の作業を整理し、プログラムできる状態に落とし込んでSOARのようなツールで自動化することも不可欠です。

こういった取り組みは、昨今提唱されている「複数の領域からデータを収集して分析するXDR（Extended Detection and Response）」の考え方と整合します。現在、セキュリティベンダー各社からXDR製品が販売されていますが、CICはXDRをセキュリティ対策の「概念」と捉えています。その構成要素の全てが新しい技術ということではなく、運用の現場によってはバラバラにチェックしていたツールを統合して、その関連性やコンテキストを見ていくセキュリティ対策の手法がXDRのアプローチです。
CICでも従来から展開している統合監視・分析サービスをさらに進めていきますが、読者の皆様においてもセキュリティ戦略を練るうえで重要な考え方となりますので、この領域を検討される際にはぜひご相談いただければと思います。

今後もセキュリティ対策や情報収集の参考にしていただくべく、CICの監視およびインテリジェンスサービスで得られた知見や分析結果を発信していきます。

本レポート執筆者

佐藤 功陛	パートナー
鳥谷部 彰則	マネージングディレクター
畑中 健作	
清水 真人	
大内 和樹	
水越 尚平	

Deloitte.
デロイト トーマツ

デロイト トーマツ サイバー合同会社
Cyber Intelligence Center (CIC)
Mail　ra_info@tohmatsu.co.jp
URL　www.deloitte.com/jp/dtcy
【国内ネットワーク】　東京・名古屋・福岡