

ゼロトラスト時代の SOC構築と運用ガイドライン

1. はじめに.....	4
2. ゼロトラストとは.....	5
2.1. ゼロトラストの共通的な特徴.....	5
2.2. ポリシーを適用したアクセス制御.....	5
2.3. ユーザやエンティティの検証.....	6
2.4. アクセス制御の4つのフェーズ.....	6
2.5. 全てのアクセスの仲介とその記録.....	7
3. アクセス制御を行う場所を検討する.....	8
3.1. ネットワーク境界におけるアクセス制御.....	8
3.2. エンドポイントにおけるアクセス制御.....	9
3.3. その他のアクセス制御.....	10
3.4. ゼロトラストを意識したアクセス制御の選択.....	10
4. リスクベースのアクセス制御の実践.....	11
4.1. ゼロトラストにおけるリスクの検証.....	11
4.2. ユーザリスクの検証.....	11
4.3. デバイスリスクの検証.....	11
4.4. その他のリスク検証.....	12
4.5. リスクベースのアクセス制御.....	12
5. EDR を活用した動的ポリシー制御の拡充.....	13
5.1. EDR (ENDPOINT DETECTION AND RESPONSE) とは.....	13
5.2. EDR における検出機能.....	13
5.3. シグナルの共有と脅威インテリジェンスの活用.....	14
5.4. EDR における対応機能.....	15
5.5. ゼロトラストと EDR の関係.....	15
6. エンドポイントセキュリティの要件.....	16
6.1. ゼロトラストにおけるモダン OS の利用.....	16
6.2. EDR の利用.....	16
6.3. EDR の要件.....	18
7. ID 管理システムの要件.....	22
7.1. ゼロトラストにおける ID 管理.....	22
7.2. ID 管理システムのセキュリティ要件.....	22
8. クラウドセキュリティの要件.....	23
8.1. ゼロトラストとクラウドの利用.....	23
8.2. クラウドの要件.....	23

9. ネットワークセキュリティの要件.....	26
9.1. ゼロトラストにおけるネットワークセキュリティ	26
9.2. ネットワークセキュリティの要件	26
10. オンプレミスの要件.....	28
10.1. ゼロトラストにおけるオンプレミスのセキュリティ	28
10.2. オンプレミスの要件	28
11. SOC の構築.....	29
11.1. SOC の役割.....	29
11.2. CSIRT の役割	30
11.3. SOC の機能と要件	30
11.4. SOC の設計・構築	32
12. SOC の運用	36
12.1. SOC 運用における注意点	36
12.2. SOC のテストと評価	37
13. MODERN SOC.....	38
13.1. 衛生管理 / 脆弱性管理	38
13.2. 脅威インテリジェンス	38
13.3. 攻撃面管理.....	38
13.4. エンリッチメント	39
13.5. 脅威ハンティング	39
13.6. UEBA (USER AND ENTITY BEHAVIOR ANALYTICS)	39
13.7. XDR (eXTENDED DETECTION AND RESPONSE)	40
13.8. SOAR (SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE)	40
14. 用語.....	41
14.1. 用語の解説.....	41
15. 参考資料.....	44
15.1. 本書を実現するためのラックのソリューション	44

1. はじめに

2010 年くらいから話題になっていたゼロトラストネットワークという考え方が、ゼロトラストとしてユーザを除く全ての資産やリソース、サービスなどエンティティ全般に適用されるようになり、エンドポイントセキュリティの重要性がさらに高まってきました。

エンドポイントセキュリティに注目が集まるにしたがってセキュリティコントロールを実施するポイントも変化し、ネットワークセキュリティを前提として構築されたセキュリティ運用センター（SOC : Security Operation Center）も見直しが必要になってきました。

本ガイドラインでは、ゼロトラストによって変化した IT 基盤をベースにした情報収集や分析をどのように実施することが望ましいかについて解説し、SOC 構築と運用のベストプラクティスとして活用いただける内容としています。

2. ゼロトラストとは

2.1. ゼロトラストの共通的な特徴

ゼロトラストについて記載された文書はさまざまあり、それがゼロトラストネットワークのことを記載していたり、ゼロトラストのことを記載していたり、具体的な実装について明確になっていないものもあります。

とはいえ、多くのゼロトラストに関する文書に共通する記載は以下の2点であり、これを冗長に記載したり、詳細に記載したりしているものがほとんどです。

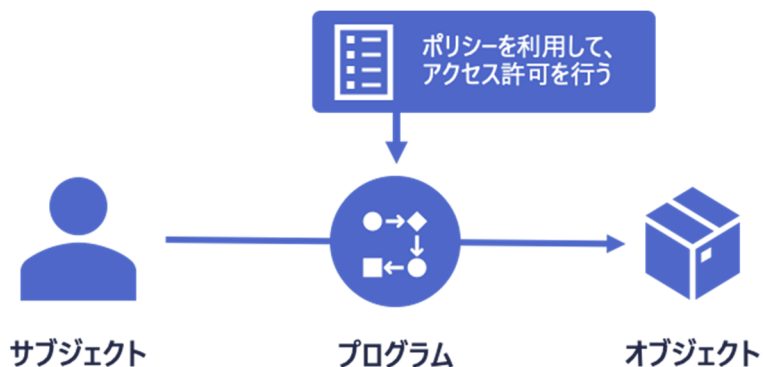
1. リスクに応じた動的なアクセスポリシー制御

2. ユーザやエンティティの動的な検証

つまり、ゼロトラストとは、セキュリティ対策の実装に必要なアクセス制御を、現代のニーズに合わせて提案するアクセス制御の概念だと考えることができます。

2.2. ポリシーを適用したアクセス制御

アクセス制御の基本的なモデルには、任意アクセス制御と強制アクセス制御があります。これらのうち、強制的にポリシーを適用することができるのは強制アクセス制御です。強制アクセス制御は、以下の図の通り、全てのアクセスについて仲介する機能があり、そこでポリシーを適用し、アクセスの可否を決定します。



図： 強制アクセス制御

適用されるポリシーについては、さまざまな種類があります。

誰がどの資産にアクセスできるかなどを示したものをアクセスコントロールリストと呼びます。さらにそれを詳細に資産に対してどのような行動が許可されているかを示したものをキャパビリティリストと呼び、たとえばあるデータに対して参照のみできるのか、編集や削除などができるのかなどを記載することが可能になります。ここで記載される行動の許可のことをアクセス制御では「認可」と呼びます。

ゼロトラストにおいては、この認可を動的に設定することで、あらかじめ決めておいたルールではなく、状況に合わせたアクセス制御を可能にします。

2.3. ユーザやエンティティの検証

一般的にエンティティと言った場合にはユーザも含まれていますが、セキュリティソリューションではこれを分けて記載することが多いため、本書でもユーザとエンティティとします。具体的には、ユーザを除く全ての資産やリソース、サービスなどをエンティティとします。

ユーザやエンティティを検証するためには、それぞれを個別のものとして扱う必要があります。これらのそれぞれを判別するための要素を識別子と言います。識別子にはさまざまなものがありますが、一般的にはIDを付与して、それぞれを個別に管理します。ここでいうIDは、ユーザIDのことだけを指しているわけではありません。全てのユーザやエンティティを個別のものとして区別するためのIDとなります。

ID、つまり識別子を付与することを「識別」と言います。ユーザ登録や資産などを管理台帳に登録する際に何らかのIDをつけることから、識別と登録は同じであると考えても良いでしょう。

ゼロトラストにおいては、識別子を持ったユーザや資産を動的に検証することになっています。これは単にユーザや資産の識別子だけで判断するのではなく、ユーザや資産の状態を反映した検証を行う必要があるということです。

ユーザの検証のことをアクセス制御では「認証」と呼びますので、動的な認証としている文書もあります。

2.4. アクセス制御の4つのフェーズ

アクセス制御には4つのフェーズがあります。これまでに説明した「識別」「認証」「認可」、そしてこれらが適切に実施されたことを説明するための要素となる「説明責任」です。

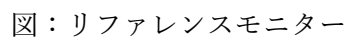


図：アクセス制御の4つのフェーズ

説明責任は、説明する責任だと勘違いされることがありますが、実際には説明の裏付けとなる要素のことです。説明する責任は説明義務と呼ぶのが一般的です。説明責任は英語ではAccountability（アカウンタビリティ）と記載し、支払いの根拠のことを示します。買い物や食事をした時のレシートや明細書などもその一つであるとすればわかりやすいかもしれません。

つまり、説明責任のフェーズでは、識別、認証、認可のそれぞれについて行動の記録を取ることとなります。

ゼロトラストにおいては、リスクに応じたポリシーを適用したアクセス制御を実施し、それらをすべて記録しておくことになります。強制アクセス制御の実施に加えて、全てのやりとりの記録を行うため、以下のような構成となります。

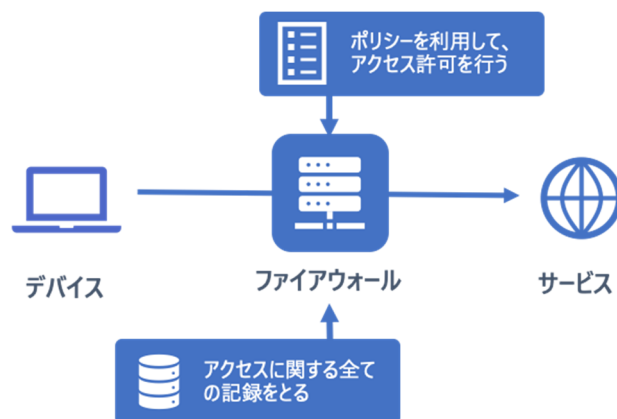


7

3. アクセス制御を行う場所を検討する

3.1. ネットワーク境界におけるアクセス制御

インターネットが活用されるようになって、インターネットと LAN の間にファイアウォールが配置されるようになりました。このファイアウォールもアクセス制御のためのリファレンスモニターとなっています。



図：ネットワークではファイアウォールがリファレンスモニターになる

基本的な機能を有したファイアウォールは、IP アドレスやポート番号を利用して、LAN に接続されたデバイスがインターネット上に配置されたサーバに接続することを許可したり、データを受け取れることを許可したりします。

ファイアウォールが利用するポリシーは、IP アドレスとポート番号を識別子としたアクセスコントロールリストであり、アクセスの許可について都度検証を行なっています。

ここまでの説明を考慮すれば、ファイアウォールもゼロトラストのためのアクセス制御システム、つまりリファレンスモニターとして役に立っているように思われます。しかし、TCP/IP の環境ではそれがうまくいかないことになります。

課題は、ポリシー適用の際に識別子となっている IP アドレスの信頼性についてです。TCP/IP は認証機能を持たないプロトコルであるため、IP アドレスそのものを信頼することができません。国別、地域別に利用しても良い IP アドレスは決まっているものの、セグメントごとに許可された IP アドレスであれば、他人が使っていない限り自由に利用することが可能です。IP アドレスは自分自身で付与することができるオレオレ識別子となり、IP アドレスを信頼したモデルは成り立たないということになります。

ゼロトラストネットワークが提唱された時に境界型防御の限界であると言われたのは、ファイアウォールが利用できるポリシーとなるアクセスコントロールリストの限界だったということです。ちなみに、ファイアウォールで保護された LAN のことを信頼されたネットワーク（トラストネットワーク）と呼んでいたため、それが無くなったということで、ゼロトラストネットワークという言葉ができました。現在では、ネットワークだけではなくさまざまなものの信頼を確保するこ

とが難しくなったので、ネットワークというキーワードを削除してゼロトラストと呼ばれることになりました。

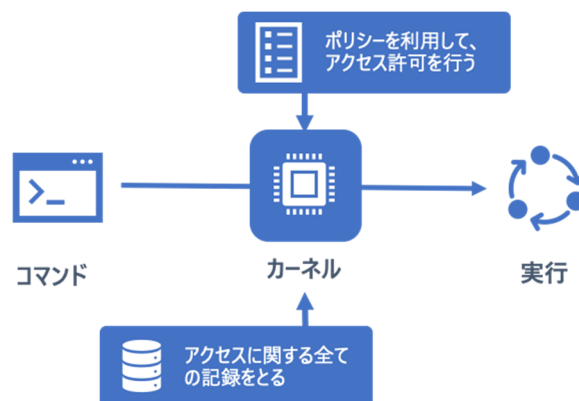
ネットワーク境界（ペリメタ）を利用したゼロトラストネットワークのモデルの一例として SDP（Software Defined Perimeter）があります。

ゼロトラスト環境での SDP の活用では、パケット単位でユーザ検証を行うとした提案がされているものがありますが、膨大なデータのやりとりにおいてはその検証を行うことが難しい場合があります。それよりも重要なことは、ポリシー適用時の識別子と、それが適切な認証局などを利用して付与されたものであるかを検討することです。もしも識別子が信頼できないものであれば、ゼロトラストは実現することができないことになります。

3.2. エンドポイントにおけるアクセス制御

エンドポイントでのアクセス制御は主に OS によって行われます。

最近の OS はそのコア機能となるカーネルにリファレンスモニターが採用されており、セキュアカーネルとして全ての処理を仲介します。これは正式なアプリケーションの実行においても、マルウェアの実行においても必ずセキュアカーネルを通じて処理されることになります。カーネルが改ざんされていない限り、ここでアクセス制御を行うことができます。



図：OS でのコマンド実行はカーネルがリファレンスモニターとなる

コマンドが実行される際、システムユーザやアプリケーションなどがどのようなコマンドを実行するのかを判別し、その実行の可否を決定します。コンピュータ上で実行される全ての処理はイベントログとして記録されます。

コンピュータフォレンジックではこのイベントログを活用して、コンピュータの動作を時間軸に並べ、システムやユーザのアクティビティを調査します。

また、EDR（Endpoint Detection and Response）ソリューションでも、このイベントログの中から怪しい動作をしたものを抽出し、シグナルを形成し、組織内のセキュリティインサイトや、ベンダーが提供するセキュリティインテリジェンスの構築に役立てます。

もちろんこれらの機能は OS が改ざんされていないことを前提としていますので、OS に改ざん検知の仕組みが搭載されていることが前提となります。

制御システムや IoT などの組み込み OS でログを取得することができなかつたり、改ざん検知の仕組みが搭載されていなかったりする場合は、エンドポイントでのアクセス制御を十分に活用することはできません。

3.3. その他のアクセス制御

最近ではクラウドサービスとして提供される API (Application Programming Interface) を利用してシステムを構築する場合があります。API は OS を伴わないものもあり、API そのものでアクセス制御が実施されますが、この場合にもアクセスポリシーを参照しています。

最近の OS は API によって構成されていることもあり、カーネルだけではなく、個々の機能の実行においてもアクセスポリシーを参照して制御されています。

たとえば、OS 上のある機能の脆弱性が発見された場合、セキュリティパッチをあてることなくポリシーの変更によって、脆弱性を利用したコマンドの実行をさせないという制御を行うことも不可能ではありません。

Java などのオブジェクト指向プログラミングでは、CORBA (Common Object Request Broker Architecture) を活用して、ネットワークを介して分散されたオブジェクト通信を仲介し、強制的にアクセスポリシーを反映させることができるようになっています。

3.4. ゼロトラストを意識したアクセス制御の選択

これまでに説明したように、アクセス制御はさまざまな場所で行うことができます。

ゼロトラスト環境を構築する際に、どこでアクセス制御を行うのが適切かということであれば、それはどこでも構わないというのが結論です。

しかしながら、TCP/IP を利用した環境ではネットワーク上のアクセス制御において十分な識別子を提供することができません。つまり、信頼できるアクセス制御ポリシーを作成することが難しいと言えます。

ネットワーク上でアクセス制御を行いたい場合には、適切な認証を実施した SDN 上での運用が前提となるでしょう。

もちろん、エンドポイントでの制御ができない端末やシステムも存在することは否めません。その場合には、できる限り管理対象を細かくセグメント化されたネットワーク上に配置し、ネットワークのアクセス制御を詳細に実施できるように工夫する必要があります。これをマイクロセグメンテーションと呼んでいます。

4. リスクベースのアクセス制御の実践

4.1. ゼロトラストにおけるリスクの検証

リスクとは将来発生するかもしれない不確実な事象を指します。想定外の損失の場合もあれば、逆に想定外の利益の場合もあります。つまり、なにが起きるかわからないことがリスクです。

リスクマネジメントとは、何らかのリスク対策を実施することによって、将来起きるさまざまな不確実性を低減していくことです。

ゼロトラスト環境を構築するには、ユーザ、エンティティのリスクを動的に検証し、即座に対応するための仕組みを用意する必要があります。ユーザ、エンティティのリスクとは何かを理解しながら、それぞれの具体的な仕組みについて検討します。

4.2. ユーザリスクの検証

ユーザリスクの大半はなりすましです。攻撃者が正規のユーザのふりをして情報にアクセスしたり、改ざんしたりすることがないように、ユーザの確認をおこないます。

ユーザは必要十分な認証情報とともに登録（識別）の際に何らかの識別子を付与されています。その認証情報を使って識別子を持ったものが正規ユーザであることを確認するプロセスを認証と言います。

たとえば、ユーザ登録時にパスワードを登録した場合、認証はパスワードを利用して実施します。電話番号やスマートフォンなどのデバイスを登録していないので、それらは認証に使うことができません。もしもこれらを認証の要素として利用したい場合は、あらかじめ適切な方法で登録しておく必要があります。

このような多要素認証の手間を削減するための考え方として、リスクベース認証があります。すでにアクセスしたことのあるデバイスからのアクセスにおいては ID とパスワードだけで認証しますが、新規のデバイスの場合のみ多要素認証によって再確認をするというものです。リスクベース認証においては、ユーザにデバイスを紐づけておく必要があります、これを厳密に行うためにはディレクトリサービスを活用することが推奨されます。

4.3. デバイスリスクの検証

主たるデバイスリスクは、脆弱性を残したままの環境です。OS やアプリケーションのアップデートができていない環境は攻撃が成功する可能性が高く、もしかするとすでにマルウェアによって侵害を受けている可能性もあります。

デバイスリスクの検証では、組織が推奨するデバイスの環境、必須のアプリケーションがインストールされ、適切な設定となっていること、そして OS やアプリケーションが適切にアップデートされていることなどが求められます。

組織はいわゆる標準デバイス環境を設定しておき、それに準拠しているかを検証します。

BYOD（私有デバイスのビジネス利用）を許可する場合には、デバイスリスクの検証を行うことが有効な手段だと考えることもできます。PCに限らず、スマートフォンなどの標準デバイスの基準を策定し、検証することでリスクの低減が可能です。

また、単に検証するだけでなく、必須アプリのインストールやアップデートを促すような仕組みも用意することが望ましいと言えるでしょう。

4.4. その他のリスク検証

その他のリスクもさまざま検証する必要があるかもしれません。

たとえば、ネットワーク犯罪などが多い国からの接続においては、アクセス可能なリソースを制限するなど、アクセス環境におけるリスクマネジメントを実施する必要がある場合、それらの状況（属性）を検証します。

そのほかにも、1時間前は大阪からアクセスしたにもかかわらず、現在は東京からアクセスしているとか、以前に不正利用された可能性があるデバイスからアクセスしているなどもその他のリスクとして検証することが可能です。

4.5. リスクベースのアクセス制御

このようにさまざまなリスク検証を行い、その場に応じたアクセス制御を行うことを、属性ベースのアクセス制御（Attribution Based Access Control: ABAC）といいます。マイクロソフトはこれを条件付きアクセス（Conditional Access）としてソリューションを提供しています。

ユーザリスク、デバイスリスク、その他のリスクを判断し、適切なアクセスポリシーを作成して、その場に応じたアクセス制御を行うことで、生産性を維持しながらセキュリティの確保を行うことが可能です。

ゼロトラストにおける動的なポリシー制御も ABAC であると考えられます。

5. EDR を活用した動的ポリシー制御の拡充

5.1. EDR (Endpoint Detection and Response) とは

アンチマルウェアソリューションが既知の攻撃に対しては有効であるが、未知の攻撃については有効でないということから、次世代アンチマルウェアソリューションが提供されることになりました。これらは NGAV (Next Generation Anti-Virus) や EPP (Endpoint Protection Platform) と呼ばれ、統計や AI 活用によるセキュリティインテリジェンスをベースに攻撃を検出します。これらが、攻撃だけではなく、デバイスにインストールされた OS やアプリケーション、そしてデータなどの資産の状態を把握しながら、異常検知を行うタイプのソリューションとして進化し、Endpoint Detection and Response (EDR) と呼ばれるようになりました。EDR の明確な定義はなく、NGAV/EPP を EDR としたり、資産管理のためのエージェント機能を EDR としたりするものもあり、EDR として足りない機能を SOC で補うなどしながら、ソリューションとして提供しているのが現状です。

これらが注目されたのは、APT (Advanced Persistent Threat) 攻撃が全盛となり、ゼロトラストネットワークが提唱されたことで、エンドポイントセキュリティの必要性が問われるようになったためです。多くの組織がアンチマルウェアソリューションの次の対策として EDR を導入しました。

5.2. EDR における検出機能

EDR の一つの機能は攻撃や異常の検出です。

エンドポイントセキュリティにおいては、OS 上のセキュアカーネルが記録したイベントログの中から、怪しい挙動 (Suspicious Event) を抽出します。この怪しい挙動のことをシグナルと呼びます。

これらのシグナルを集約することで攻撃であるかを判断し、攻撃であるとした場合にはアラートとしてセキュリティ管理者に知らせます。ただし、アラートが出ている段階では攻撃が成功しているとは限りません。攻撃が成功し、何らかの被害が出ている時には、インシデントとして取り扱うことになります。

同様に、攻撃の形跡が見られない場合、もしくは攻撃が検知できない場合でも、知らない間にデータやアプリケーションへの不正なアクセスや改ざんが行われている場合もあります。このような高度な攻撃に対しても資産の不適切な変更を検出するのも EDR の仕事です。これらも同様にシグナルとして検出して集約します。

EDR を選択する際には、攻撃の検出、資産の異常検知など、組織が必要とするシグナルを検討する必要があります。また、これらの機能を別のソリューションで用意した場合は、シグナルを集約するために SIEM (Security Information and Event Management) を導入し、シグナル集約のためのキーとなる情報が双方のソリューションに含まれていなければなりません。相性問題などを

考慮した場合、攻撃の検出、資産の異常検知など、同一エンドポイントの情報は一元的に検出できるようなソリューションを選択することが、迅速な対応の要素となります。

5.3. シグナルの共有と脅威インテリジェンスの活用

エンドポイントからのシグナルを集約することで、単体のエンドポイントではわからなかった様々な情報を得ることができます。

組織の中のシグナルを活用して、組織内で活用できる情報としてまとめたものを脅威インサイトと言います。組織における攻撃の傾向や、脆弱性の残存状況を把握できるようになります。

また、シグナルは組織外で共有することも可能です。同じ EDR が検出したシグナルは同一のフォーマットになっているため、組織内の機微な情報を削除した形で共有することで、さらに詳細な情報を得ることができます。

ある組織に対する標的型攻撃だと思っていたものが、実は他の企業も受けていた一般的な攻撃だったり、すでに対策が講じられているにもかかわらず、自らの組織だけがその対策を行っていないということもわかるようになります。

このように組織を超えてシグナルを共有することで構成される脅威情報を、脅威インテリジェンスと呼びます。脅威インテリジェンスを活用することで他組織がすでに受けた攻撃を未然に防ぐことが可能になります。

脅威インテリジェンスの内容は提供するベンダーによってさまざまですが、以下の情報が含まれていることが望ましいといえます。

- ・ 脅威に関する概要
- ・ 攻撃の手法（MITRE の ATT&CK などの業界標準の情報と照らし合わせることができるようなもの）
- ・ 脅威が対象としている脆弱性（CVE 番号などを含む）
- ・ 対象となる脆弱性をスキャンするためのツールもしくは方法
- ・ 脆弱性を低減するためのツールもしくは方法

脅威に対する概要だけを提供してインテリジェンスとする場合もありますが、それだけでは実際の対応を行うことができません。

現在、攻撃をされているかどうかを把握するために、まずは攻撃の手法を理解し、攻撃を受けた形跡があるかどうかを判断します。イベントログもしくはシグナルと攻撃手法を照らし合わせることで、攻撃が行われたかどうかを判断することが可能です。

攻撃がどのレイヤーまでたどり着いていたかを知りたい担当者にとっては、MITRE の ATT&CK などの記載に従った情報であることも重要かもしれません。

攻撃を受けていた場合は封じ込めとして、攻撃を受けていない場合は予防として、対象となる脆弱性を低減する必要があります。そのために、脆弱性をスキャンするためのツールやスクリプトなどがあると良いでしょう。さらに、低減するためのツールなども必要です。

脅威インテリジェンスを活用することで、迅速なインシデントレスポンス（封じ込め）を行うことができ、被害を最小限にすることが可能です。これによってサイバーレジリエンスの確保を行うことができます。

また、脆弱性のない状態を維持するための衛生管理も重要です。

5.4. EDR における対応機能

EDR は異常検出のほかに対応の機能も備わっています。

実際には、EDR ソリューションとして販売しながらも対応機能を持たないものもあるので、どのような対応を行うのかを把握しておくとい良いでしょう。

前項に記載したとおり、EDR で集約したシグナルは脅威インテリジェンスとして自動対応のためのツールやスクリプトと連動します。

しかし、脆弱性によってはアプリケーションにパッチをあてなくてはならないものもあります。その際には自動でパッチを当てるのか、それともアラートだけに留めるのかなどを組織の方針として決めておく必要があります。また、それを EDR の設定として行なっておく必要があります。また、場合によってはパッチが間に合っていないような脆弱性もあるかもしれません。その際には、動的ポリシー制御によって、OS や API のポリシーに脆弱性を誘引するような機能にアクセスできないようにしておく必要があります。

例えば、Windows 10 では Microsoft Intune を利用することで、ポリシー制御を行うことができます。多くの EDR がこの機能を利用してパッチで制御できない粒度の脆弱性を封じ込めています。最近の脆弱性では、Remote Code Execution (RCE) と呼ばれる、外部からコードが実行できるものが悪用されがちです。これを外部からは使えないようにしたり、特定のシステムユーザからしか使えないようにしたりすることも、アクセスポリシーの変更で対応可能です。

EDR によるパッチ適用やエージェントでのアクセス制御だけではなく、OS や API のポリシー変更ができるかを確認しておくことも重要です。EDR ベンダーが独自に提供するエージェントによる制御は OS のポリシー制御に比べて管理の粒度が荒い場合があり、関係のない機能まで制限してしまうことがあるためです。

5.5. ゼロトラストと EDR の関係

ここまでで説明したように、ゼロトラストで求められている動的ポリシー制御のために EDR ソリューションは大きな役割を果たしています。SOC の適切な運用を行うためにも、CSIRT が適切な対応をするためにも、それらの人的コストを抑制するためにも EDR と脅威インテリジェンスの正しい利用が求められています。

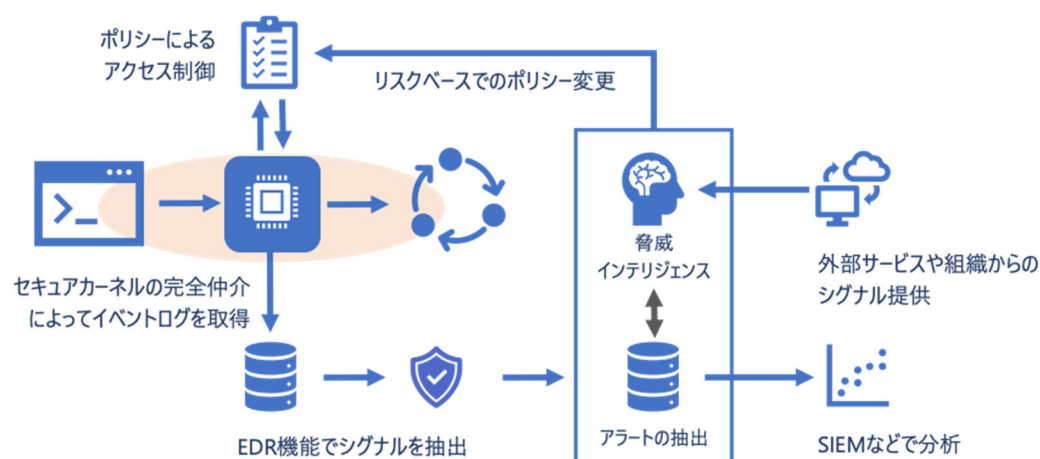
6. エンドポイントセキュリティの要件

6.1. ゼロトラストにおけるモダン OS の利用

ゼロトラストアーキテクチャでは、ポリシーを強制するための仕組みとして、強制アクセス制御やリファレンスモニターを活用しています。Windows 10 をはじめとする最近の OS はモダン OS と言われ、セキュリティカーネルを持ち、さまざまな機能は API として提供されています。このセキュリティカーネルや API がまさにリファレンスモニターとして全てのやりとりを仲介することになっています。

これによって、EDR などのエンドポイントセキュリティの仕組みでは、特別なエージェントを利用しなくても、エンドポイントのデバイス上で実行された様々なイベントがログとして記録されることになります。これらのログのことをイベントと言います。

ゼロトラスト環境を構築する際にモダン OS を活用することで、シンプルな環境を構築することが可能になります。



図：モダン OS におけるログ取得とポリシー適用の関係

6.2. EDR の利用

境界セキュリティでは、ファイアウォールなどのネットワークでの制御と監視が主に行われていました。ゼロトラストでは、ユーザに最も近いエンドポイントでの制御と監視が必要です。なぜならば、リソースにアクセスするエンティティ（ユーザ、アプリケーション、デバイス）に対して、制御を行うポリシー実施ポイントの大半は、エンドポイントになるからです。ここでは、エンドポイントの重要な2つの機能について、詳しく解説します。

➤ EPP (Endpoint Protection Platform)

マルウェアなどの脅威からエンドポイントを保護し、被害の拡大を防止するソリューション。高度な攻撃手法に対応するために、従来のアンチウイルスに加えて複数の保護機能を備えている。

➤ EDR (Endpoint Detection and Response)

エンドポイントの挙動を記録して解析することで、脅威を検知して隔離などのレスポンスを可能にするソリューション。挙動の記録には複数の方法があり、必要な記録が行われることが極めて重要となる。

EPP および EDR はエンドポイントで動作するため、同じ機能を持つ複数のソリューションの導入は避けた方がいいでしょう。特に EPP のリアルタイムスキャンは同時に動かない可能性があるため、EPP/EDR が統合されたソリューションを推奨します。

また、ゼロトラストを実現するためには、エンドポイントから収集されるシグナルを元に、エンティティの信頼性を算出します。この信頼性に基づいて、エンドポイントなどでポリシーでのアクセス制御を行います。EPP/EDR は信頼性を算出するためのシグナルの重要なデータソースであり、ポリシーによるアクセス制御の機能を持つものもあります。EPP/EDR が導入されていない場合と、統合された EPP/EDR ソリューションがある場合との比較を、以下の表にまとめます。このように、ゼロトラストでは統合的な EPP/EDR ソリューションが適しているため、これより以降ではこれらの機能をまとめて EDR と呼びます。

役割	EPP/EDR が無い場合	EPP/EDR がある場合
防御	既知の脅威、高度な攻撃を防御できない。	マルウェアや高度な攻撃を防御する。
検知	マルウェアや高度な攻撃は検知しない。	マルウェアや高度な攻撃で発生する不審な挙動を検知する。
封じ込め	エンドポイントを手動で特定した上で、場合によってはオンサイトで物理的に隔離する。	エンドポイントを自動的に特定し、リモートから論理的に隔離する。
調査	ネットワークのログ調査、エンドポイントのフォレンジック調査を実施する。	エンドポイントから収集済みのログで調査を実施する。
復旧	エンドポイントを初期化して再利用する。	悪性ファイルなどを削除し、変更されたものを修正したうえで利用する。
制御	他のソリューションを使用して信頼性を算出して、ネットワークで通信を遮断する。	シグナルから信頼性を算出して、エンドポイントで動的にアクセス制御を行う。

6.3. EDR の要件

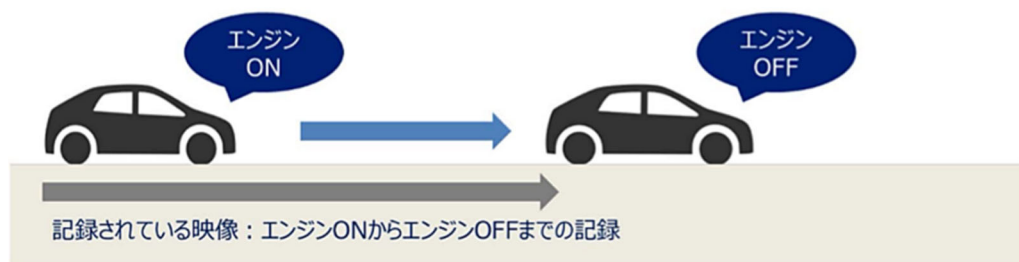
ゼロトラストにおいて EDR ソリューションが果たす役割を説明しました。残念ながら EDR が最も効力を発揮するのは、インシデントが発生したときです。しかし、ソリューションを評価する際にインシデントを想定した観点で評価するのは、なかなか難しいのが実情です。そのため、実際にインシデントレスポンスを行う上で、必要となる EDR の 5 つの要件について詳しく説明します。

6.3.1. ログがハイブリッド記録方式であること

EDR はエンドポイントで発生するシステムやユーザによるアクティビティを記録して、防御・検知・調査などで使用します。しかし、エンドポイントで発生するアクティビティは膨大な量のため、各ソリューションで様々な工夫を行っており、その工夫が記録方式となって現れます。たとえば、EDR のログの記録方式は、自動車のドライブレコーダーの記録方式と似ています。

➤ 常時記録タイプ

エンジンが動いている間のアクティビティを常に記録する。EDR の場合、エンドポイントが起動している間のアクティビティを常に記録する。



図：常時記録タイプの場合

➤ イベント記録タイプ

車に衝撃が加わった際の前後のアクティビティだけ記録する。衝撃が弱い場合は、これを検知せず記録されないケースもある。EDR の場合、不審な挙動を検知した場合にアラートを発報するとともに、関連する挙動を記録する。



図：イベント記録タイプの場合

➤ ハイブリッド記録タイプ

常時記録方式とイベント記録方式の両方を兼ね備え、常にアクティビティを記録しつつ、衝撃を検知した際にも記録する。EDR では、常にアクティビティを記録しつつ、不審な挙動を検知した場合にアラートを発報するとともに、関連する挙動を別途記録する。

ハイブリッド記録方式の場合、常にアクティビティを記録しているため、EPP/EDR 以外のソリューションで異常を検知した場合でも、EDR のログから対象のエンドポイントの調査が可能です。全てのインシデントがエンドポイントで発生・検知するわけではないため、どんな場合でもエンドポイントのアクティビティを調査できるようにすることが必要です。

6.3.2. 分析が AT 車タイプであること

EDR は、エンドポイントで実行されたプログラムの親子関係や通信先などの情報を分析し、不審な挙動を検知します。この分析のロジックや設定について、大きく分けると 2つの方式があります。

➤ AT 車タイプ

AT 車がアクセルを踏むだけで進むように、分析ロジックや設定が不要なタイプ。新たな攻撃手法などへの対応は EDR ベンダーが実施し、ユーザの設定は基本的に不要。

➤ マニュアル車タイプ

マニュアル車がクラッチとギアの操作が必要なように、導入直後は分析ロジックや設定が何も無い状態になっており、ユーザが自組織の運用方針に合わせて組み込む必要があるタイプ。新たな攻撃手法などへの対応は EDR ベンダーが提供するが、ユーザが設定する。

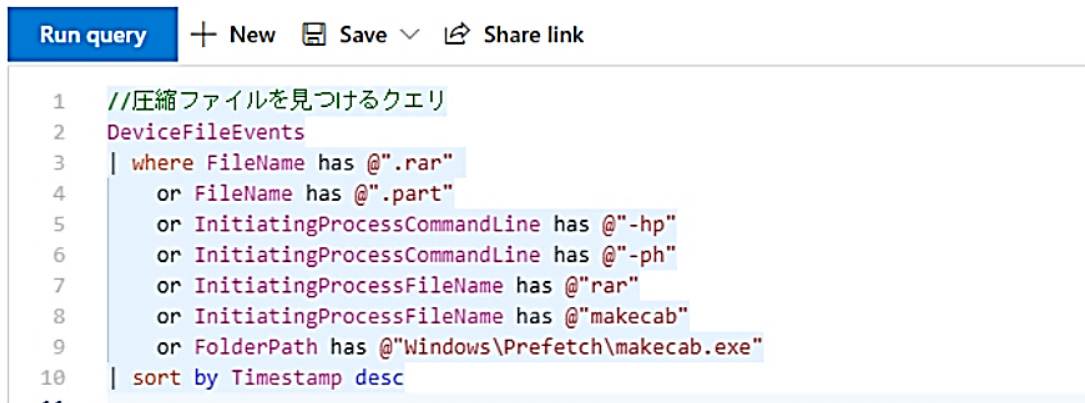
マニュアル車タイプの EDR は、コミュニティなどの情報から迅速に分析ロジックを追加でき、チューニングの柔軟性も高いのですが、分析ロジックの維持にコストがかかるというデメリットがあります。AT 車タイプの EDR は、最新の脅威に対応しつつ、インシデントの調査や対処などの本質的な対応に多くの時間を割けるというメリットがあります。

6.3.3. クエリ言語を用いた任意の検索機能を有すること

インシデントの際には、EDR が記録したログの中からインシデントに関係するログを調査します。ログを時間帯で絞り、ホスト名・ファイル名などで単純検索する機能は、ほとんどの EDR 製品に実装されています。

常時記録タイプおよびハイブリッド記録タイプの EDR では、非常に多くのログが記録されます。アラートが発生した際に、膨大なログから効率よく調査するために、プログラム実行・ネッ

トワーク通信などのイベントタイプでフィルタするなど、ノイズとなるログを除外して調査する必要があります。そのためにはクエリ言語を用いて、複雑な条件を用いた任意の検索（下図参照）を行う必要があります。



```
Run query + New Save Share link
1 //圧縮ファイルを見つけるクエリ
2 DeviceFileEvents
3 | where FileName has @".rar"
4    or FileName has @".part"
5    or InitiatingProcessCommandLine has @"-hp"
6    or InitiatingProcessCommandLine has @"-ph"
7    or InitiatingProcessFileName has @".rar"
8    or InitiatingProcessFileName has @"makecab"
9    or FolderPath has @"Windows\Prefetch\makecab.exe"
10 | sort by Timestamp desc
..
```

図：クエリ言語の例

6.3.4. 対処機能を有すること

インシデントが発生した際、被害拡大を防止するため、迅速に封じ込めや復旧を行う必要があります。特にエンドポイントが離れた場所にある場合は、管理コンソールなどを通じて、リモートから対象のエンドポイントに対して以下の操作を実施する必要があります。

- ネットワーク隔離
エンドポイントを必要最小限の通信を許可したまま、ネットワークから論理的に隔離する。
- ファイル取得
エンドポイントに存在するファイルを指定して取得する。
- ファイル削除
エンドポイントに存在するファイルを指定して削除する。
- プロセス停止
エンドポイントで動作している特定のプロセスを停止させる。
- リモート操作
コマンド入力によるファイル一覧、プロセス一覧、メモリダンプ取得などのリモート操作を行う。

6.3.5. API で全ての操作が可能であること

EDR で収集したデータは、エンティティの信頼性を計算するためのデータソースとなります。また、信頼できない場合には、エンドポイントに対してリソースへのアクセスを停止させる必要があるかもしれません。これらの状態は動的に変化し、一連の操作は他のソリューションと連携して実施する場合があります。そのため、API (Application Programming Interface) ¹で全ての操作が可能である必要があります。

¹ API (Application Programming Interface) は、プロダクトやソリューションを連携するためにプログラムから利用可能なインタフェース（「14.1 用語の解説」参照）。

7. ID 管理システムの要件

7.1. ゼロトラストにおける ID 管理

ゼロトラストにおいて、ID とはリソースへのアクセスをリクエストしているエンティティを特定する極めて重要な情報です。ID 管理システムは、一般的にはユーザ ID を管理するとともに、ID に紐づいたユーザを認証し、ID にひもづけられた権限を付与（認可）します。また、認証に成功した ID に関する情報を収集して記録する機能を持つものもあります。

このように重要な基盤となる ID 管理システムは、オンプレミスとクラウド上に存在し、複数のシステムに分かれていることがあります。また、それぞれのシステムが連携・同期している場合と、連携・同期していない場合があります。また、それぞれの ID 管理システムを連携するための、別のサブシステムが存在する場合があります（例：HR と呼ばれる人事情報を管理するシステム）。

SOC は、組織内に存在する全ての ID 管理システムおよび関連するサブシステムを正確に把握する必要があります。また、それぞれのシステムで適切なログを取得して監視します。次項では、各システムにおいてどのようなログを取得すべきかを説明します。

7.2. ID 管理システムのセキュリティ要件

ID 管理システムが保護している ID は、セキュリティ侵害があったときに、最も狙われやすいデータです。攻撃者は ID 管理システムの中でも、最も高い権限を持つ ID を狙って活動するため、その過程で ID 管理システムには様々な痕跡が残ります。これらの痕跡から攻撃の進行をいち早く検知して、被害が発生する前に食い止めることが必要です。これを実現するためには、複数の ID 管理システムおよびサブシステムの構成を把握して、それぞれのシステムで必要なログを取得します。

➤ 認証・認可ログ

ID を使った認証（誰が）と認可（どのような権限を付与されたのか）の成功と失敗が記録されるログ。失敗したログに攻撃の痕跡が残りがちで、無効になっている場合があるので必ず有効にする。

➤ 監査ログ

ID の作成や権限の付与、ポリシーの変更などのデータやシステムに対する操作の記録。無効になっている場合があるので必ず有効にする。

➤ セキュリティログ

上記以外に、セキュリティに関連する重要なイベントの記録。異常なサインインなどが記録されることがある。

8. クラウドセキュリティの要件

8.1. ゼロトラストとクラウドの利用

ゼロトラストでは、「場所」を暗黙の信頼としないことが求められます。そのため、アクセス元やアクセス先の信頼性を動的に評価して、十分な信頼性があるものだけ、最小限のアクセスを許可します。このためには、アクセス先であるリソースだけでなく、アクセス元であるエンティティが、どこにあってもサービスを適切に提供できることが必要となります。そのため、ゼロトラストにおいては、クラウドサービスを利用することが多くなります。

しかし、クラウドサービスはオンプレミスとは違い、インターネットからアクセス可能であるため、攻撃者にとって格好の標的となります。そのため、オンプレミス以上に注意して必要なログを取得して、適切なセキュリティ運用・監視を行う必要があります。幸いなことに、クラウドサービスは API を提供することで、オンプレミスでは実現できなかった自動化された高度な運用が可能になります。

SOC は、組織が利用するクラウドサービスを正確に把握する必要があります。また、それぞれのクラウドサービスで適切なログを取得して監視します。

8.2. クラウドの要件

クラウドサービスで取得するログを理解する前に、クラウドにおける共同責任について理解しておく必要があります。クラウドにおける共同責任モデルとは、クラウドにおける一部の責任についてはクラウド事業者が委譲されますが、ユーザと責任を共有するものと、ユーザの責任となるものが存在することを表します。この責任の範囲は、サービス提供形態（一般的には SaaS²、PaaS³、IaaS⁴がある）によって異なります。これを正しく理解したうえで、利用しているサービスに応じてユーザの責任範囲となっているログの管理を間違えないことが重要になります。

² SaaS (Software as a Service) は、アプリケーションソフトウェアをサービスとして提供する形態（「14.1 用語の解説」参照）。

³ PaaS (Platform as a Service) は、アプリケーションソフトウェアが稼働するためのデータベースやプログラム実行環境など、プラットフォームをサービスとして提供する形態（「14.1 用語の解説」参照）。

⁴ IaaS (Infrastructure as a Service) は、システムが稼働するためのサーバやネットワークなど、インフラストラクチャをサービスとして提供する形態（「14.1 用語の解説」参照）。

■ 責任共有モデル

責任	SaaS	PaaS	IaaS	On-prem	
情報とデータ	■	■	■	■	常にユーザに責任がある
デバイス（モバイルとPC）	■	■	■	■	
IDとアクセス管理	■	■	■	■	
ID・ディレクトリ基盤	■	■	■	■	サービスによって責任範囲が異なる
アプリケーション	■	■	■	■	
ネットワーク制御	■	■	■	■	
OS	■	■	■	■	
物理ホスト	■	■	■	■	常にクラウド事業者 to 責任がある
物理ネットワーク	■	■	■	■	
物理データセンター	■	■	■	■	

クラウド事業者
 ユーザー

図：クラウドにおける共同責任モデル

- 認証・認可ログ（IaaS、PaaS、SaaS）
クラウドサービスへの認証（誰が）と認可（どのような権限を付与されたのか）の成功と失敗が記録されるログ。失敗したログに攻撃の痕跡が残しやすいが、無効になっている場合があるので必ず有効にする。
- 監査ログ（IaaS、PaaS、SaaS）
クラウドサービスの設定変更など、データやシステムに対する操作の記録。無効になっている場合があるので必ず有効にする。
- CSPM で発生したアラート（IaaS、PaaS、SaaS）
CSPM（Cloud Security Posture Management）/SSPM（SaaS Security Posture Management）はクラウドのセキュリティの状態を可視化して、誤って不適切な設定を行った時や、データの露出などが確認された時などに、アラートで通知することができる。
- CWPP で発生したアラート（IaaS、PaaS）
CWPP（Cloud Workload Protection Platform）はクラウドのワークロード（例：仮想マシン、サーバレス）を保護する複数のセキュリティ機能を提供し、異常があった場合にアラートで通知することができる。

➤ CASB で発生したアラート (SaaS)

CASB (Cloud Access Security Broker) はクラウドサービスへのアクセス制御を行い、不審な利用や情報漏えいの痕跡が確認された場合などに、アラートで通知することができる。

➤ アクティビティログ (SaaS)

クラウドサービスにおいて、ユーザのアクティビティを記録し、大量のファイル削除などの異常を検知する。

9. ネットワークセキュリティの要件

9.1. ゼロトラストにおけるネットワークセキュリティ

ゼロトラストでネットワークセキュリティが不要になるわけではありません。境界セキュリティの主要な機能であるファイアウォールや WAF (Web Application Firewall) ⁵、URL/DNS フィルタリングについては、よりユーザに近いエンドポイントでも提供されることがあります。一方で、各ソリューションがサポートしていないエンドポイントや IoT・ネットワーク機器もあるため、依然としてネットワークでのセキュリティ機能提供も必要です。

また、エンドポイントやシステムへの侵害を許してしまった場合に、横展開などを検知・防御して、被害の発生を防ぐためには、IDS/IPS (Intrusion Detection System/Intrusion Prevention System) ⁶を用いたネットワーク監視も引き続き有効です。

SOC は、組織のネットワークを正確に把握する必要があります。また、ネットワークの適切なログを取得して監視します。次項では、ネットワークにおいて、どのようなログを取得すべきか説明します。

9.2. ネットワークセキュリティの要件

ネットワークで必要となるログは、オンプレミスだけでなく、クラウドサービスでも共通であることを理解しておく必要があります。オンプレミスで稼働していたシステムがクラウドに移行した場合に、クラウドの中にネットワークが構築されることとなりますが、クラウドの中でもネットワークセキュリティの必要性は変わりません。ただし、オンプレミスで使用していたソリューションが使えない場合もあり、その場合にはクラウドサービスに対応したソリューションや、クラウド事業者が提供するサービスを使用します。

➤ トラフィックログおよびアラート

ネットワークに発生する通信のログと、過剰なトラフィックなどの異常を検知して発生するアラート。

➤ WAF や IDS/IPS のログおよびアラート

WAF や IDS/IPS で記録されるログと、異常が発生したときに発生するアラート。

⁵ WAF (Web Application Firewall) は、Web システムの脆弱性を突いた攻撃や調査活動などの通信を識別して、防御や検知を行うソリューション (「14.1 用語の解説」参照)。

⁶ IDS/IPS (Intrusion Detection System/Intrusion Prevention System) は、ネットワークトラフィックから、システムの脆弱性を突いた攻撃や調査活動などの通信を識別して、防御や検知を行うソリューション (「14.1 用語の解説」参照)。

➤ URL/DNS フィルタリングのログ

URL（Web）や DNS 通信については、攻撃者やマルウェアが外部のサーバと通信するコマンド&コントロールやマルウェアのダウンロードに悪用されやすいので、可能な限り全てのアクティビティを記録する。また、不審なアクセスを検知した場合のアラートも必要。

➤ ネットワーク機器のセキュリティログ

ネットワーク機器が侵害を受けて、横展開のきっかけとなることがあるため、ネットワーク機器自体のアクセスやログインなどのセキュリティログ。特にインターネットにさらされているものは必須とする。

10. オンプレミスの要件

10.1. ゼロトラストにおけるオンプレミスのセキュリティ

ここまでで、ゼロトラストにおける必要なログの要件を定義しましたが、組織によってはオンプレミスにもシステムが存在するはずです。特に組織のゼロトラスト化が進むと、ゼロトラストに対応できない古いシステムが取り残される可能性があります。このような弱点があると、攻撃者に弱点を突かれてしまう可能性があります。

SOC は、組織のシステムを把握して、弱点となりうるシステムの監視ができていない、ということが無いように注意を払う必要があります。次項では、オンプレミスにおいて、盲点となりやすいシステムやログの存在について説明します。

10.2. オンプレミスの要件

ここでは、実際のインシデント事例から、盲点となりやすいシステムやログの存在について説明します。環境によっては、オンプレミスではなく、クラウドなどに存在する可能性があるため、自組織の中で該当するものが無いか確認してください。

➤ 重要なサーバ

サーバについてもエンドポイントと同じソリューションを導入するのが望ましいが、ライセンスやプラットフォームの関係で対応していない場合がある。重要なシステムについては、監査ログやセキュリティログなどを取得する。

➤ ソリューションの管理サーバ

管理サーバが侵害を受けて、管理サーバ経由でエンドポイントにマルウェアが配布されるといった事例がある。重要なシステムと同様に、監査ログやセキュリティログなどを取得する。

➤ サービスのゲートウェイ

自組織とネットワーク接続して、マネージドサービスや子会社からサービスの提供を受けている場合がある。サービスで提供されるゲートウェイを組織内に設置していた場合に、マネージドサービスや子会社経由で侵害を受ける可能性がある。これらの第三者が提供するシステムやゲートウェイについては、監査ログやセキュリティログ、アクセスログなどを取得する。

➤ 保守事業者が持ち込む機器

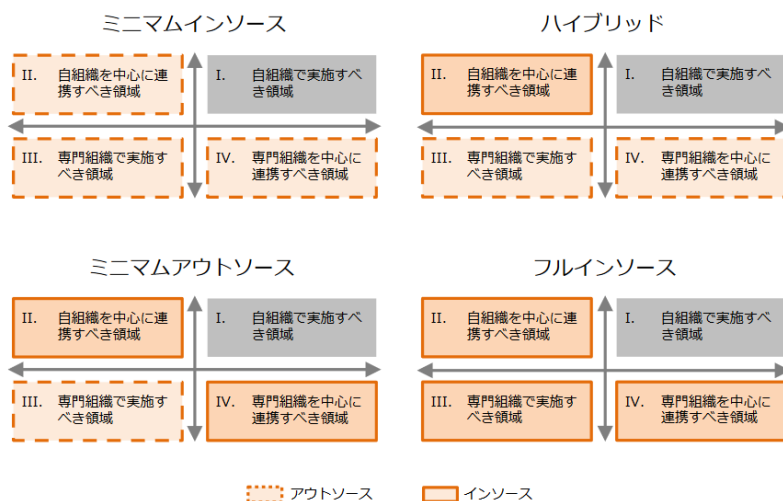
保守事業者が持ち込むエンドポイントなどの機器が侵害されており、組織内のネットワークに接続した際に被害を受ける可能性がある。保守事業者が接続できるネットワークを限定して、監査ログやセキュリティログ、アクセスログなどを取得する。

11.SOC の構築

11.1. SOC の役割

SOC はインシデントを防止し、セキュリティ上の脅威を監視するとともに、インシデントが発生してしまった場合には迅速に対応して、被害の拡大を防ぐ役割があります。近年は、防止や監視はソリューションが提供する機能に任せて、SOC は脅威の検知と、SOC の改善に注力するように移りつつあります。なぜならば、防止や監視といった機能は、ソリューションが提供する機能に依存し、SOC が関与すべきことが少なくなっているからです。一方で、ソリューションで対応できない脅威を検知し、適切な運用が行われていないものを見つけて改善することが、組織のセキュリティ強化に貢献するからです。

ここまでで説明してきたように SOC のカバーすべき範囲は広く、自組織だけでは対応が難しいため、MSSP (Managed Security Service Provider) ⁷の利用も検討します。ただし、MSSP は「イベント・脅威の検知」や「インシデントの対応」かつ、対応しているソリューションも限定されているのが一般的です。そのため、SOC の運用を全て MSSP に任せるのは現実的ではありません。反対に、無理に SOC の全ての運用を MSSP に任せても、柔軟な対応ができず運用が硬直化する恐れがあります。したがって、MSSP を利用する場合には、自組織で対応すべきものと、MSSP で対応すべきものを見極めて、適切に役割を分担する必要があります。日本セキュリティオペレーション事業者協議会では、①取り扱う情報の性質と②セキュリティ専門スキルの必要性により、インソース（自組織での対応）とアウトソース（MSSP などの利用）を使い分ける考え方について、以下のように分類しています。



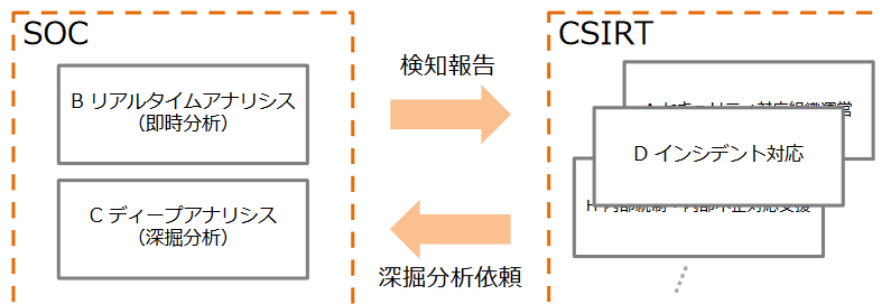
図：「セキュリティ対応組織の教科書」より引用⁸

⁷ MSSP (Managed Security Service Provider) は、セキュリティの運用・監視サービスを提供する事業者のこと（「14.1 用語の解説」参照）。

⁸ 日本セキュリティオペレーション事業者協議会 (ISOG-J) の「[セキュリティ対応組織の教科書](#)」の P.24 より。

11.2. CSIRT の役割

インシデントが発生した場合には、一般的には CSIRT（Computer Security Incident Response Team）⁹が影響範囲や原因の調査、ステークホルダーに対する説明や対応を行います。CSIRT が主体となることでインシデント対応をコントロールしつつ、SOC と協力して調査や対応を行います。日本セキュリティオペレーション事業者協議会では、セキュリティ対応組織として SOC と CSIRT を位置づけており、一般的な区分として以下のように分類しています。



図：「セキュリティ対応組織の教科書」より引用¹⁰

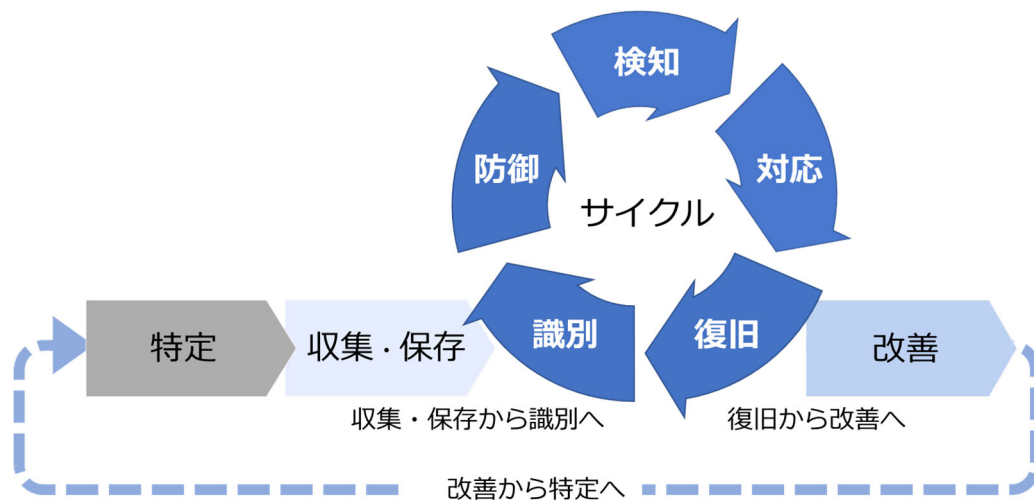
11.3. SOC の機能と要件

SOC と CSIRT の役割を説明しましたが、特に CSIRT に関しては組織によって対応範囲が異なります。組織によっては CSIRT が SOC の役割を持つこともあるでしょう。そのため、ここでは一般的な SOC に必要な機能と要件を定義します。

まず、SOC の機能を大きく 8 つに分類します。このうち、「識別」から「復旧」までの 5 つの機能は、継続して実施することが求められるコアな機能です。残りの 3 つの機能については、SOC の立上げなどの初期などに実施するだけでなく、随時や定期的にも実施するのがよいでしょう。

⁹ CSIRT（Computer Security Incident Response Team）は、セキュリティインシデントが発生した際に、原因や影響の調査、対処を行う組織（「14.1 用語の解説」参照）。

¹⁰ 日本セキュリティオペレーション事業者協議会（ISOG-J）の「[セキュリティ対応組織の教科書](#)」の P.21 より。



図：SOC の 8 つの機能とサイクル

それぞれの機能において、実施すべきオペレーションの概要と、要件を以下の通り定義します。

➤ 特定

オンプレミスやクラウドに渡り、組織のシステムを把握して、これらを適切に保護するために必要なログや資産を特定する。資産は機器やデータなどであり、資産を特定することで保護する対象を明確にし、リスクの識別などに使用する。必要なログや資産は変動的であり、常に最新の状態を把握するためには、自組織の IT 運用チームの協力が不可欠である。

➤ 収集・保存

ログや資産を特定した上で、必要なものを収集して保存する。このとき、重要度に応じて収集頻度や保存期間、保存する場所（オンプレミスやクラウド）を決めて、適合する SIEM（Security Information and Event Management）¹¹ソリューションなどを使用する。

➤ 識別

システムに存在する脆弱性などを把握して、存在するリスクを識別し、必要な対処を行う。このとき、必要に応じて資産管理や脆弱性管理ソリューションを使用する。脆弱性については、脆弱性のスコアだけの判断では重大なリスクを見逃すため、「資産」「脅威」などの観点も加えて定量的に判断するリスクベースの脆弱性管理を実施するのが望ましい。

¹¹ SIEM（Security Information and Event Management）は、セキュリティに関するログやイベントを収集・保存して、リアルタイムで分析を行いアラートなどで通知するソリューション（「14.1 用語の解説」参照）。

➤ 防御

組織が晒されているあらゆる脅威からの防御を行う。一般的にはソリューションの機能を利用し、SOC ではソリューションが対応していないものを中心に、対応を検討する。ソリューションが対応していない機能が多いほど、SOC でカバーする範囲が大きくなるため、適切なソリューションの選定が重要になる。

➤ 検知

各ソリューションで検知したセキュリティイベントや、SOC で定義した脅威について、誤検知の判断と重要度などの決定を行う。誤検知などが多い場合には、適切にチューニングを行い、SOC が対応しなければならないイベントを削減する。また、SOC のアナリストの負荷を減らし、アナリストが対応すべき調査に時間をかけられるようにするため、SOAR (Security Orchestration, Automation and Response) ¹²を導入することも検討する。

➤ 対応

イベントや脅威について何らかの対処が必要なものは、インシデントと定義する。インシデントは、決定した重要度に応じて必要な対応を行う。被害を封じ込めるために一次対応を行い、根本的な対応は次の復旧で行う。

➤ 復旧

インシデント発生前と同様の状態まで復旧する。インシデントの原因や影響を特定した上で、根本的な復旧や対策を実施する必要がある。これらが不十分だと、二次被害や、再度インシデントが発生する可能性があるため、原因や影響の特定などの調査は十分に行う必要がある。

➤ 改善

新しいシステムや資産の増加や、構成変更など、セキュリティ態勢が変化する可能性がある。また、適切にソリューションが機能していない、適用されていないということが発覚することもある。そのため、随時 SOC 運用の改善を行い、必要に応じて収集するログや資産も変更する。

11.4. SOC の設計・構築

SOC の設計は、基盤となるシステムの設計だけでなく、SOC の運用に関する設計も必要です。ただし、運用については最初から全ての手順を確立できないため、SOC と連携する組織やステークホルダーとの役割分担とコミュニケーション方法の定義のみで十分です。ここでは、SOC のシ

¹² SOAR (Security Orchestration, Automation and Response) は、各種のセキュリティ情報を統合することで、運用を自動化や効率化するためのソリューション（「13.8 SOAR」参照）。

システム設計で検討しなければならない要件と、連携すべき組織やステークホルダーの例を説明します。

11.4.1. システムの設計

SOC のシステムは、「11.3. SOC の機能と要件」で定義した要件に基づいて、必要なソリューションやシステムを選定する必要があります。これを始めるために、まず対象の組織と、そのシステムを把握する必要があります。SOC が把握していない場合には、IT 運用チームや、各システムの担当にヒアリングをする必要があるでしょう。

➤ ログや資産の特定

「11.3. SOC の機能と要件」と同じ。

➤ MSSP 利用の検討

「11.1. SOC の役割」を踏まえたうえで、「11.3. SOC の機能と要件」の機能のうち、どこまでを MSSP に任せるか検討する。なお、対象とするソリューションによっては、MSSP が対応していない可能性があるので、自組織と MSSP でのハイブリッドでの運用が必要になる場合がある。MSSP を利用する場合には、MSSP が提供するシステムを使える場合があるが、要件が合わない場合には別途 SIEM ソリューションを検討する必要がある。

➤ SIEM ソリューションの検討・設計

SIEM ソリューションを検討する場合には、対象のログや資産などに対応できるかを調査したうえで、必要に応じて評価を行う。評価を行う際には、評価項目をあらかじめ用意してから実施すべきだが、要件が多く全ての評価が難しい場合には、重要な要件に絞って評価する。ログの量や保存期間などにより、システム構成や価格が大きく変化するため、SIEM の仕様を正しく理解したうえで必要な見積もりを行う。近年では、SaaS 形式で提供する SIEM も存在し、設計や導入だけでなく運用の手間も削減できるため、まず SaaS 形式の SIEM を検討するのがよい。

➤ その他ソリューションの検討・設計

「11.3. SOC の機能と要件」の機能のうち、SIEM ソリューション以外の資産管理や脆弱性管理、SOAR などのソリューションを利用するかを検討する。SOC に合わせて新規で導入する場合には、必要に応じて評価を行う。ソリューションによっては、SIEM や MSSP との連携が可能であり、効率化・自動化などに役に立つため、技術的に可能であれば連携を検討する。

➤ ログや資産の取得・保存の設計

特定したログや資産を SIEM や MSSP に取り込む際には、データソースからデータの取得・送信方法などを、SIEM や MSSP に合わせる必要がある。データソースのシステム管理者や

組織が異なる場合は、データソース側の設計に加えて、手順などを用意して作業を依頼する必要がある。また、SIEM や MSSP にデータを送信するために、必要な通信の許可や経路など、ネットワークの設計も必要となる。

➤ SIEM やその他ソリューションの導入

SIEM やその他ソリューションを設計に基づいて導入して、ソリューション同士の連携を行う。これらのソリューションは SaaS 形式の場合にはハードウェアやソフトウェアの準備がほとんど必要なくなるため、導入の期間も短くて済む。

➤ ログや資産の取得

データソースの設計や手順に基づいて、データの転送を開始する。データソースが複数ある場合には、一度に全ての転送を行うのではなく、段階的に転送を行って SIEM や MSSP にログの欠落や過負荷などの障害が発生しないか確認しながら行う。

➤ イベントのチューニング

ログの転送を開始するとイベントの検知が始まるが、誤検知などが大量に発生する場合には、イベントのチューニングを行う。

11.4.2. 別組織やステークホルダー

SOC の運用では、SOC と連携する組織やステークホルダーとの役割分担を定義して、それらの組織やステークホルダーとのコミュニケーション方法を定義します。特に、インシデントはいつ発生するか分かりませんので、夜間や休日であっても連絡が取れる手段は明確にしておく必要があります。また、インシデントの重要度もしくは優先度を 4 段階程度で定義して、組織の特性に合わせた指標で具体的に定義しておく¹³と、複数の組織が関わった場合でも分かりやすいでしょう。

ここでは、SOC と連携する組織やステークホルダーの例を説明します。

➤ CSIRT

セキュリティインシデントが発生したときに主体的に対応を行う。ステークホルダーとの連絡は CSIRT が担当することで、インシデントをコントロールする。

➤ MSSP

¹³ 例えば米国の国土安全保障省傘下の CISA（重要インフラストラクチャの保護を目的とする）は、インシデントの優先度を 6 段階で定義している（<https://us-cert.cisa.gov/CISA-National-Cyber-Incident-Scoring-System>）。

SOC の一部の役割を担当するセキュリティ運用サービスの提供ベンダー。自組織に合わせてカスタマイズしたサービスを提供するのは一般的には難しいため、自組織と MSSP で役割を分担するのが望ましい。

➤ インシデントレスポンスサービス

インシデントが発生した際に、インシデント対応の支援や、フォレンジック調査などのサービスを提供するベンダー。これらの作業は専門的な知識が必要となるため、重大なインシデントの際にはサービスを利用することがある。

➤ NOC (Network Operation Center)

ネットワークやネットワーク機器の運用や保守を行う組織、もしくはサービスを提供するベンダー。インシデント対応の一環でネットワーク機器の設定変更などを行う場合は、夜間や休日でも緊急時に対応が必要となるため、一部の作業は SOC が担当することも検討する。

➤ IT 運用

システムやサーバなどの運用や保守を行う組織、もしくはサービスを提供するベンダー。IT システム全般を担当するが、モバイルやエンドポイント等、担当が分かれていることがある。

➤ システム担当

特定のシステムの運用や保守を行う組織、もしくはサービスを提供するベンダー。重要なシステムには専門の担当やベンダーが存在する場合がある。

➤ ソリューション担当

SOC が使用するソリューションの運用や保守を行う組織、もしくはサービスを提供するベンダー。ソリューションによってサポート内容やレベルが異なる。

➤ サプライチェーン

SOC が対象とするシステムや資産に影響を受ける、もしくは影響を与える組織や事業者。

➤ 関係省庁や外部 CSIRT

重大インシデントが発生した場合には、監督省庁に報告が必要な場合がある。また、外部の CSIRT などに IOC などを提供することで、他組織への攻撃や脅威が発生していた場合の助けになることがあるため、情報の提供だけでなく入手も検討する。

12.SOC の運用

12.1. SOC 運用における注意点

ここまでで、ゼロトラスト時代の SOC について、SOC の対象とするログの要件から SOC 自体の要件を説明しました。そのうえで、SOC の設計と構築について、具体的なポイントを解説しました。ここでは、SOC の運用が始まった際に、陥りやすい問題について説明します。

12.1.1. 多層防御について

多数のセキュリティソリューションが導入されており、多層防御という目的で同じようなソリューションが稼働していることがあります。多層防御とは、最初の層をすり抜けてきた脅威が、次の層で検知して防御することを期待するものです。ところが、実際には同じようなソリューションを重ねているだけで、多層防御ではなく多重防御となっている場合があります。同じような機能を持ったソリューションを重ねるだけでは、期待するほどの効果は得られません。

本来の多層防御とは、ソリューションの足りていない機能や弱点を理解して、それを効率よく補うソリューションを次の層としなければ意味がありません。そのためには、各ソリューションを正しく理解する必要がありますが、ソリューションの選定や評価をベンダーや子会社などに任せたり、単純な比較表で判断したりしている組織ほど、このような失敗に陥りがちです。自組織の弱点とソリューションのアーキテクチャや特徴を理解して、正しく評価できる人材の育成が必要です。

12.1.2. SOC の権限について

組織のセキュリティ運用を担当するため、SOC のアナリストやオペレータは、各システムやサービスに対して高い権限を持っていることがあります。そのため、万が一 SOC が使用するエンドポイントやアカウントが侵害を受けてしまうと、広い範囲に影響が発生する可能性があります。SOC が使用するエンドポイントやアカウントは、通常よりもセキュリティ対策や監視を強化します。

また、NOC や MSSP などのサービスベンダーを利用している場合には、サービスベンダーを踏み台として侵害を受ける可能性もあります。サービスベンダー側のセキュリティ対策や監視については、手出しすることはできないため、サービスベンダーと接続しているネットワークや機器において、必要最小限のアクセス制限や権限の設定を行います。また、使用しているネットワークや機器に対する監査ログを取得し、監視の強化を行います。

12.1.3. ベンダーへの依存について

NOC や MSSP などのサービスベンダーや、システムやソリューションの運用ベンダーに運用を任せている場合、自組織にはセキュリティ運用の知識やノウハウが蓄積されにくくなります。そのため、インシデントが発生して該当システムの調査が必要になったとき、自組織ではシステム構成を把握しておらず、調査の方法や結果が理解できないといったことが起こります。これでは、インシデントが発生した際に、円滑な調査や対応を行うことが出来ずに、被害を拡大させてしまうかもしれません。

これを防ぐためには、日ごろから情報の理解を心がけ、不明な点や理解できない点については、ベンダーへの確認や実物の確認など、自組織での対応を怠らないことが必要です。また、自組織の SOC の中心となるセキュリティリーダーの育成を、日ごろから行う必要があります。

12.1.4. SOC の可視化について

SOC の活動は、普段はあまり見えることがなく、インシデントが発生してはじめて効果が見えるということがあります。しかし、本来インシデントは減多に発生することは無いため、見えない稼働が SOC の稼働の大半を占めることになります。普段の活動のボリューム（件数や、1 件当たりにかかる時間、など）が可視化されていないと、SOC 運用のボトルネックが分かりません。ボトルネックが存在することに気が付かないうえに、定量的に判断して改善を試みることもできなくなります。

そのため、SOC の普段の活動については、定量的に表すことができる数値を記録しておき、定期的に分析してボトルネックを明らかにします。ボトルネックが明らかになれば、SOAR の導入などにより効果的に改善を行うことができます。

12.2. SOC のテストと評価

SOC が機能しているかの評価は、「12.1.4. SOC の可視化について」で説明した可視化だけでは判断できません。脅威を防御してインシデントを検知できるか、インシデント対応を円滑に実施できるかも、評価すべきでしょう。

しかし、SOC のテストと評価のために、脅威やインシデントが発生するのを待つわけにはいきません。そこで、ペネトレーションテスト¹⁴や BAS（Breach and Attack Simulation）¹⁵を実行する際に、SOC が脅威を防御してインシデントを検知し、円滑にインシデント対応が実行できるかも合わせて評価するとよいでしょう。

¹⁴ ペネトレーションテストは、攻撃者と同じ手法やツールを用いてシステムへの侵入を試みて、組織やシステムの弱点を報告するサービス（「14.1 用語の解説」参照）。

¹⁵ BAS（Breach and Attack Simulation）は、ペネトレーションテストと同様のテストを、自動的に継続して実施するソリューション（「14.1 用語の解説」参照）。

13.Modern SOC

13.1. 衛生管理 / 脆弱性管理

衛生管理とは、平時からシステムの脆弱なソフトウェアや設定を排除し、システムの健康を維持することを言います。適切なソリューションを用いて、システムの健康状態を把握し、必要に応じて脆弱性や設定を確認して、改善や修復を日常的に実施します。

SOC がこの機能を担うことができれば、インシデントの発生を減らすことができます。また、万が一インシデントが発生した場合でも、被害の発生や拡大を最小限に抑えることができます。

13.2. 脅威インテリジェンス

脅威インテリジェンスとは、IOC (Indicator of Compromise)¹⁶などのインシデントの痕跡を表す情報や、漏えいした自組織に関する情報など、脅威を把握して適切な対策を打つための情報です。このような脅威インテリジェンスを提供するサービスを、スレットインテリジェンスサービスと言います。

例えば、スレットインテリジェンスサービスから提供される IOC を SIEM などに適用して、該当する通信を防御・検知することで、インシデントの発生をいち早く検知することができます。

また、スレットインテリジェンスサービスで自組織の情報漏えいを監視することで、自組織でのインシデントの発生に気が付くことができ、被害の拡大を防ぐことが出来る場合があります。

SOC がスレットインテリジェンスサービスを活用することができると、SOC の運用を効率化し、これまで検知できなかった脅威が検知できるようになります。

13.3. 攻撃面管理

IT 基盤がオンプレミス中心からクラウド中心になり、どこからでもサービスが提供されるようになるにつれ、組織が把握していない攻撃面 (Attack Surface) が増加しています。攻撃面とは、主にインターネットなどのパブリックなネットワークからアクセス可能なソフトウェアやハードウェア、クラウドの資産などを表します。Web サーバや VPN など、意図して公開しているものは、前出の衛生管理や脆弱性管理によって、リスクを可能な限り減らすことができます。しかし、意図しない攻撃面の露出は、リスクを飛躍的に高めてしまいます。露出している攻撃面を把握して、意図していない露出をいち早く検知して修復することを攻撃面管理と呼びます。

攻撃面管理は、どこにあるかわからない自組織の攻撃面が意図せず露出したときに検知するという技術的に困難な課題があります。しかし、狙われやすい資産を持った組織ほど、露出した攻

¹⁶ IOC (Indicator of Compromise) は、システムが侵害された可能性を示す痕跡 (アーティファクト) のこと (「14.1 用語の解説」参照)。

撃面が悪用される可能性は高いため、これらを考慮して SOC での対応を検討する必要があります。

13.4. エンリッチメント

イベントを検知した際に、関連するドメイン名の Whois¹⁷情報などを参照することがあります。このように、ある情報に対して、関連する別の情報を追加・補足することを、エンリッチメントと言います。SOC は一つのイベントに対して、関連する複数の情報を元に判断するため、エンリッチメントをイベント発生時に自動的に行うことができれば、判断やインシデント対応を迅速に行うことができます。

エンリッチメントを自動的に行うためには、分析の基盤である SIEM と、脅威インテリジェンスサービスなどを API で連携させるのが一般的です。エンリッチメントの機能は、この後説明する XDR や SOAR にも組み込まれています。

13.5. 脅威ハンティング

脅威ハンティングとは、脅威インテリジェンスを利用して、SIEM などのソリューションで検知していない脅威を、過去にさかのぼって広範囲で調査することを言います。脅威ハンティングサービスは、EDR のオプションサービスで提供、MSSP などのサービスの提供、もしくは SOC 自身で実施する場合があります。脅威ハンティングを実施することで、ソリューションでは検知しなかった脅威やインシデントを検知することができます。

13.6. UEBA (User and Entity Behavior Analytics)

UEBA とは、ユーザの実体を表す ID を元にして、ユーザの挙動を機械学習などで分析することで、不審なユーザの挙動を検知するものです。UEBA を使うためには、ID と紐づいたログを取り込んだ UEBA ソリューションが必要です。近年では、SIEM を始めとして、この後説明する XDR や SOAR で実装している場合があります。

ゼロトラスト環境においては、イベントの発生元となった IP アドレスなどは信頼できる情報とは言えません。そのため、ID を元にユーザの挙動を分析する UEBA は、ゼロトラスト環境に適した分析と言えます。UEBA を行うことで、SOC の運用を効率化し、これまで検知できなかった脅威が検知できるようになります。

¹⁷ Whois は、インターネットのドメイン名・IP アドレス・AS 番号の所有者などの情報を検索するためのツールやデータベースのこと。

13.7. XDR (eXtended Detection and Response)

XDR は EDR や NDR といった、エンドポイントやネットワークでの異常検知とインシデント対応の機能を高度に統合して、UEBA のようにユーザの異常検知などにも拡張することを言います。オンプレミスやクラウドに渡る組織の複雑なシステムに対して、SIEM よりも簡単に横断的かつ高度な監視ができます。ただし、一般的には対応しているソリューションは限られるため、対応していないソリューションも監視対象とする場合には、SIEM を利用するか、XDR と SIEM を併用します。XDR の方がデータやユーザインタフェースが高度に統合されているため、最近は SIEM に替わる SOC の基盤として利用されることがあるようです。

XDR を行うことで、SOC の運用を効率化し、これまで検知できなかった脅威が検知できるようになります。

13.8. SOAR (Security Orchestration, Automation and Response)

SOAR はセキュリティ運用の自動化と効率化を可能にするソリューションです。イベントを検知した際に、自動的に関連する情報を集めて（エンリッチメント）、脅威インテリジェンスなどとも連携して、自動的に判断を行うロジックを作ることができます。これにより、イベントの検知だけでなく、インシデント対応の自動化も実現し、SOC アナリストやオペレータの負荷を軽減します。また、アナリストによる同様のイベント・インシデント対応の判断の差異を少なくし、アナリストの育成の時間も短縮することができます。

SOC が SOAR を導入すると、SOC の運用を効率化し、SOC の分析や対応の精度を向上させることができます。

14.用語

14.1. 用語の解説

➤ MSSP (Managed Security Service Provider)

MSSP は、セキュリティの運用・監視サービスを提供する事業者のこと。各事業者によって、対応しているプロダクトやソリューション、サービスの範囲や内容が異なる。そのため、MSSP を使用する目的に応じて、適切な MSSP を選定する必要がある。

➤ CSIRT (Computer Security Incident Response Team)

CSIRT は、セキュリティインシデントが発生した際に、原因や影響の調査、対処を行う組織。CSIRT が対応する範囲や権限は、組織によって大きく異なる。SOC とは密接に連携が必要となる組織である。

➤ SIEM (Security Information and Event Management)

SIEM は、セキュリティに関するログやイベントを収集・保存して、リアルタイムで分析を行いアラートなどで通知するソリューション。SOC の中心となるソリューションであり、機能は多岐にわたる。ソフトウェアやサービスでの提供、オンプレミスやクラウドでの提供など、複数の提供形態がある。

➤ API (Application Programming Interface)

API は、プロダクトやソリューションを連携するためにプログラムから利用可能なインタフェース。ゼロトラスト時代の SOC では、複数のプロダクトやソリューションが連携するために必須の機能である。

➤ SaaS (Software as a Service)

SaaS は、アプリケーションソフトウェアをサービスとして提供する形態。機密情報がファイルなどの形式で存在しており、情報漏えいが発生したときに直接のリスクに繋がる。広く利用されているが、SOC の対象から見落とされることが多いため、SSPM などを活用する。

➤ PaaS (Platform as a Service)

PaaS は、アプリケーションソフトウェアが稼働するためのデータベースやプログラム実行環境など、プラットフォームをサービスとして提供する形態。データベースなどが侵害された時に、膨大なデータが漏えいするリスクがある。広く利用されているが、設定ミスによるインシデントが多発しているため、CSPM などを活用する。

➤ IaaS (Infrastructure as a Service)

IaaS は、システムが稼働するためのサーバやネットワークなど、インフラストラクチャをサービスとして提供する形態。侵害を受けた場合は、情報漏えいだけでなく、コンピューティングリソースの消費（過大な課金）、踏み台としての悪用など、多数のリスクがある。広く利用されているが、設定ミスによるインシデントが多発しているため、CSPM などを活用する。

➤ CSPM (Cloud Security Posture Management) /SSPM (SaaS Security Posture Management)

CSPM/SSPM はクラウドのセキュリティの状態を可視化して、不適切な設定やデータの露出などが確認された時などに検知するためのソリューション。CSPM が主に IaaS、PaaS を対象とするのに対して、SSPM は SaaS を対象とする。複数のクラウドに対応した専用のソリューションもあるが、クラウド事業者が同様の機能を提供している場合があり、それぞれメリットとデメリットを見極めたうえで利用することが推奨される。

➤ WAF (Web Application Firewall)

WAF は、Web システムの脆弱性を突いた攻撃や調査活動などの通信を識別して、防御や検知を行うソリューション。ソフトウェアやサービスでの提供、オンプレミスやクラウドでの提供など、複数の提供形態がある。また、Web アプリケーションだけでなく、ミドルウェアの脆弱性も保護対象としているソリューションが推奨される。

➤ IDS/IPS (Intrusion Detection System/Intrusion Prevention System)

IDS/IPS は、ネットワークトラフィックから、システムの脆弱性を突いた攻撃や調査活動などの通信を識別して、防御や検知を行うソリューション。ネットワークではなく、ホスト上に実装されるものと区別するために、NIDS/NIPS や HIDS/HIPS と呼ぶこともある。ネットワークの境界に設置されることが多いが、いわゆる横展開を検知するためにはネットワーク内部に設置する必要がある。

➤ ペネトレーションテスト

ペネトレーションテストは、攻撃者と同じ手法やツールを用いてシステムへの侵入を試みて、組織やシステムの弱点を報告するサービス。脆弱性診断と混同されがちだが、脆弱性診断はシステムの脆弱性を網羅的に調査する（広く浅く）のに対して、ペネトレーションテストは現実的なシナリオを用いて実際にどこまで侵入できるかを調査する（狭く深く）ことである。

➤ BAS (Breach and Attack Simulation)

BAS は、ペネトレーションテストと同様のテストを、自動的に継続して実施するソリューション。ペネトレーションテストは1回のテストに時間がかかるが、これを自動的にかつ継続的に実施することで、攻撃に対する組織やシステムの耐性を高め、システムの変化による脆弱性の発生をいち早く見つけて修復ができる。

➤ IOC (Indicator of Compromise)

IOC は、システムが侵害された可能性を示す痕跡（アーティファクト）のこと。主要なものとしてIPアドレスやドメイン名、ファイルのハッシュ値などがある。

15. 参考資料

15.1. 本書を実現するためのラックのソリューション

15.1.1. 監視・運用サービス

IDS/IPS/WAF などの各種ソリューションに対応した MSS、EPP/EDR に対応した MDR があります。

- [JSOC[®] マネージド・セキュリティ・サービス \(MSS\)](#)
- [マネージド・ディテクション・アンド・レスポンス \(MDR\)](#)

15.1.2. インシデントレスポンスサービス

セキュリティインシデントなどの緊急事態に、迅速にお客様をご支援する緊急対応サービスです。

- [緊急対応サービス「サイバー119[®]」](#)

15.1.3. ペネトレーションテストサービス

IT システム全体に対して行うペネトレーションテストサービスと、主に公開されたシステムに対して行う Synack 社のサービスがあります。

- [ペネトレーションテストサービス \(侵入テスト\)](#)
- [ペネトレーションテストサービス Synack](#)

15.1.4. CSPM/CWPP

IaaS/PaaS に対して行う設定診断サービスと、CSPM/CWPP の運用を支援するサービスがあります。

- [クラウドセキュリティ設定診断](#)
- [クラウドセキュリティ統制支援サービス](#)

15.1.5. 脅威インテリジェンス

脅威情報をフィード提供する JLIST と、アナリストが早期警戒情報を提供する Threat Landscape Advisory、ラックの独自ツール FalconNest があります。

- [脅威情報提供サービス「JLIST[®]」](#)
- [早期警戒情報提供サービス「Threat Landscape Advisory サービス」](#)
- [無料調査ツール「FalconNest」](#)



「ゼロトラスト時代の SOC 構築と運用ガイドライン」

<執筆・制作・監修>

株式会社ラック

<協力>

日本マイクロソフト株式会社

発行：2021 年 3 月 17 日