頭を悩ますセキュリティ運用。
検出から対応までに必要な準備とは。

テクマトリックス株式会社
セキュリティ研究所
佐山 享史

目次

1. 本講演でお伝えしたいこと
2. 適切なセキュリティ運用とは
3. 適切なセキュリティ運用を構築するには
4. 事前準備
5. 運用構築
6. 運用・改善
7. TechMatrix Premium Suppportとは
8. 本日のまとめ

1. 本講演でお伝えしたいこと

お伝えしたいこと

適切なセキュリティ運用を実現するために必要なことはシンプル

自社の"リスク"を理解してセキュリティ運用を設計する

- セキュリティは積み上げ式ではなく、削減式
- 自社のリスクは自社でしか分からない
- セキュリティ専門会社へ丸投げすると 無駄な 余計な コストがかかる
- 自社だけでやっても非効率なので、バランスが大事

戦略は？

戦略といえば「孫氏の兵法」

「彼を知り、己を知れば、百戦して危うからず」

「彼を知らずして己を知れば 一勝一負す・
彼を知らず己を知らざれば 戦う毎に必ず殆し」

（敵と味方の実情を熟知していれば、百回戦っても負けることはない。
敵情を知らないで味方のことだけを知っているのでは、勝ったり負けたりして勝負がつかず、敵のことも味方のことも知らなければ必ず負ける。）

2. 適切なセキュリティ運用とは

適切なセキュリティ運用とは

そもそも“適切”なセキュリティ運用とはどういったものだろうか。
セキュリティ運用の目的は、安全な状況であることを担保（監視）し、
インシデントの発生があった場合には迅速に対応して被害を最小にすることである。

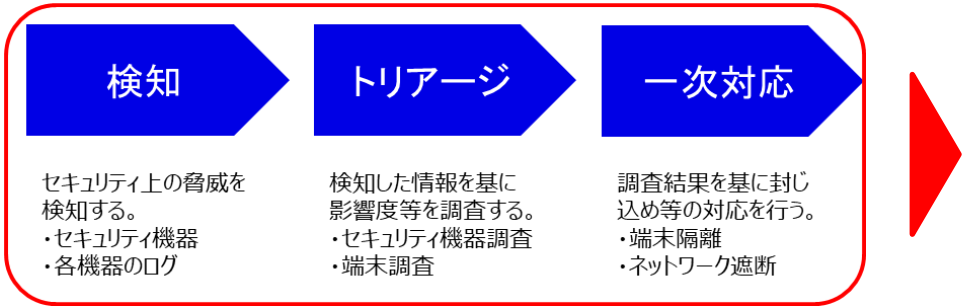
危ないものを発見できる	脅威を早期に分析できる	リスクを早期に取り除ける	事象の原因究明ができる	リスクへの対策ができる
=	=	=	=	=
検知	**トリアージ**	**一次対応**	**解析**	**対応**

適切なセキュリティ運用（検知～一次対応）

セキュリティ運用の大部分が「検知～一次対応」となる。目的は以下の通り。

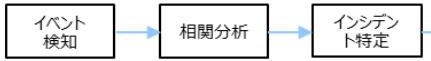
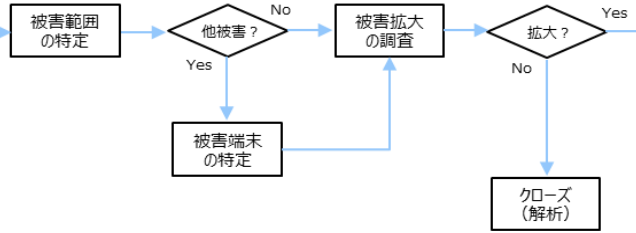
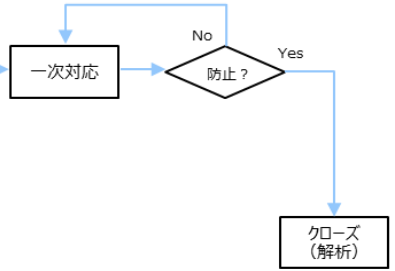
① 被害事象（影響範囲等）の特定
② 拡散防止（被害拡大防止）

セキュリティのインシデント（事象）として何が発生しているか。また、影響範囲を特定して、被害拡大の防止を行う。一次対応では「該当通信の遮断」「端末の隔離」等により拡散防止を行う。



被害の事象が特定され、拡散（被害の拡大）が止められた状態にする。

「検知～一次対応」のフロー例

検知	トリアージ	一次対応
		
【イベント検知】 セキュリティ機器のイベント検知。 **【相関分析】** セキュリティ機器のイベントを相関的に分析。 **【インシデント特定】** 相関分析の結果を基に発生しているインシデントを特定する。	**【被害範囲の特定】** 特定されたインシデントに対して、実際の被害が発生しているか。また、他に同じ事象が発生していないかを調査する。 **【被害端末の特定】** 同じ事象が発生している被害端末を特定する。 **【被害拡大の調査】** インシデントの被害が拡大しているのか、収束しているのかを調査する。	**【一次対応】** 被害拡大を防ぐために通信の遮断や端末の隔離等を行う。

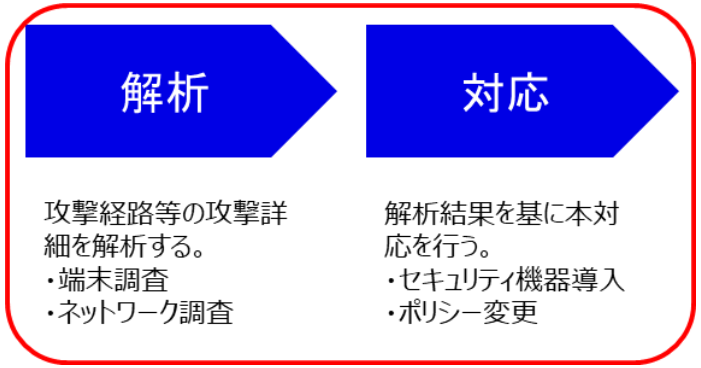
適切なセキュリティ運用（解析～対応）

「解析～対応」は必要に応じて実施されるのが一般的となる。目的は以下の通り。

① 被害事象の詳細特定

② 復旧・対応

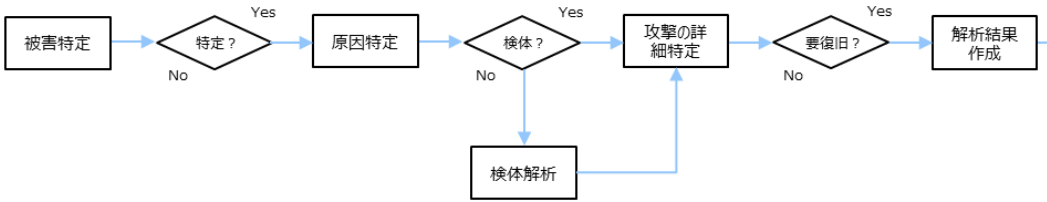
一次対応で被害拡大を防止した後に、実際の侵入経路や被害状況の詳細を調査し、該当システムの復旧や対応を行う。対応については、今後同様の攻撃被害を防止する対策検討も含まれる。



侵入経路や被害の詳細を把握し、復旧や対応を行う。

「解析～対応」のフロー例

解析



【被害特定】
被害（情報漏えい、踏み台、ボット、マルウェア感染、システム停止等）の範囲や時間等を含めて詳細を特定する。

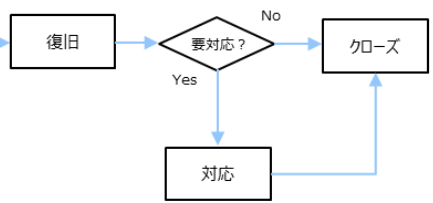
【原因特定】
インシデントを引き起こした原因（マルウェアの感染、Exploit、URLアクセス等）を特定する。

【攻撃の詳細特定】
攻撃の詳細をMITREのATT&CKベースで特定を行う。

【解析結果の作成】
解析した結果を報告書として作成する。

【検体解析】
マルウェアの検体解析を行う。

対応



【復旧】
被害を受けたシステムの復旧を行う。

【対応】
今後被害を受けないための対応（ポリシー変更、セキュリティ機器の導入等）を行う。

セキュリティ運用イメージ

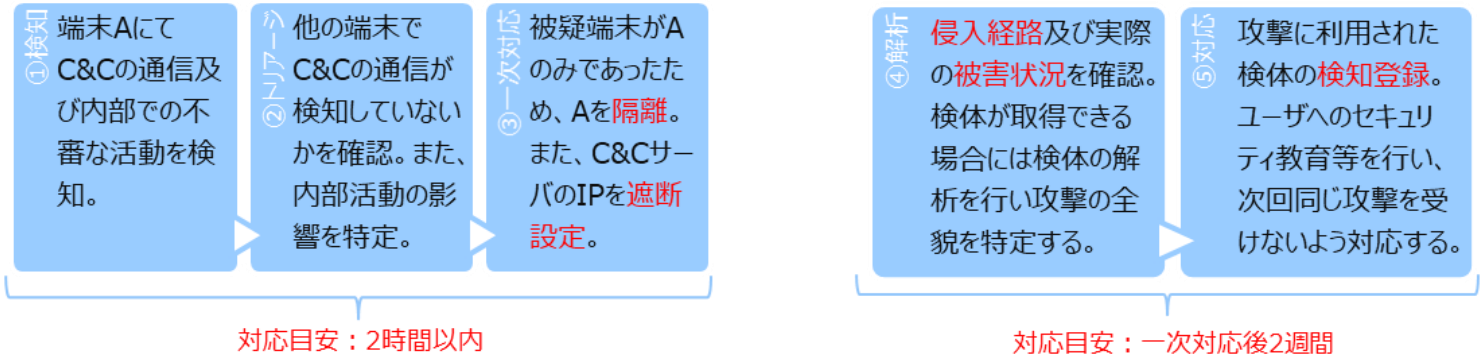
セキュリティ運用のイメージは以下の通り。

■インシデント概要

端末Aがメールの添付ファイル（エクセル）を開き、マルウェア（RAT）に感染。AD等の内部サーバに対して脆弱性攻撃や不正ログインの試行を行う。攻撃は成功せず、他のPCに同様の攻撃を行った。

■セキュリティ機器の検知

・ RATによる通信（シグネチャによる検知）・C&C通信（脅威情報による検知）・ 内部の不審な通信



3. 適切なセキュリティ運用を構築するには

適切なセキュリティ運用を構築するには

適切なセキュリティ運用を構築するには、セキュリティ範囲を把握する「事前準備」から開始する必要がある。構築するにあたってのフローは以下の通り。

- 事前準備
  事前準備では自社で行うセキュリティ運用の範囲やレベルを把握・決定することが目的となる。この部分を専門企業に丸投げしてしまうと、“適切”な運用は作れない。
- 運用構築
  運用構築では事前準備で決定した範囲を踏まえて、具体的な“作業”に落とすことが目的となる。この部分は専門企業の助けが大いに役に立つ。
- 運用・改善
  専用製品の使用、サービス利用する場合には“効果”の測定を行う。

構築役割のイメージ

	事前準備	運用構築	運用・改善
 自社担当者	自社が必要なセキュリティ運用を特定する。 ・対象インシデントの特定 ・クライテリアの作成 ・オペレーション範囲の特定	事前準備で特定した内容を踏まえて運用を構築。 ・対応体制の構築 ・セキュリティ対応のゴール設定 ・セキュリティ運用手順の作成	セキュリティ運用を行う。 もしくは運用サービスを受ける。 ・手順通りの運用実施 ・運用の見直し ・運用改善
 専門企業	専門家として、上記の特定に関して助言や内容の妥当性確認を行う。	上記の内容を専門家として助言と妥当性確認、セキュリティ運用手順の作成もしくは作成支援を行う。	運用の確認。もしくは運用サービスを提供する。 ・手順通りの運用実施 ・運用の見直し支援 ・運用改善支援

4. 事前準備

適切なセキュリティ運用を構築する事前準備

上記の適切なセキュリティ運用を構築するには、「自社に必要なセキュリティ運用」を確認する必要がある。ポイントは以下の通り。

① 範囲（スコープ）	何を
② クライテリア（基準）	どのレベルで
③ 対応内容	どうやって

① 範囲（スコープ）

範囲とは、セキュリティ運用の対象とする範囲（スコープ）を指す。
つまり、セキュリティ運用を“何のため”に“どのくらい”実施するか決めることになる。

(a) セキュリティ領域の範囲

(b) システムの範囲

(c) インシデントの範囲

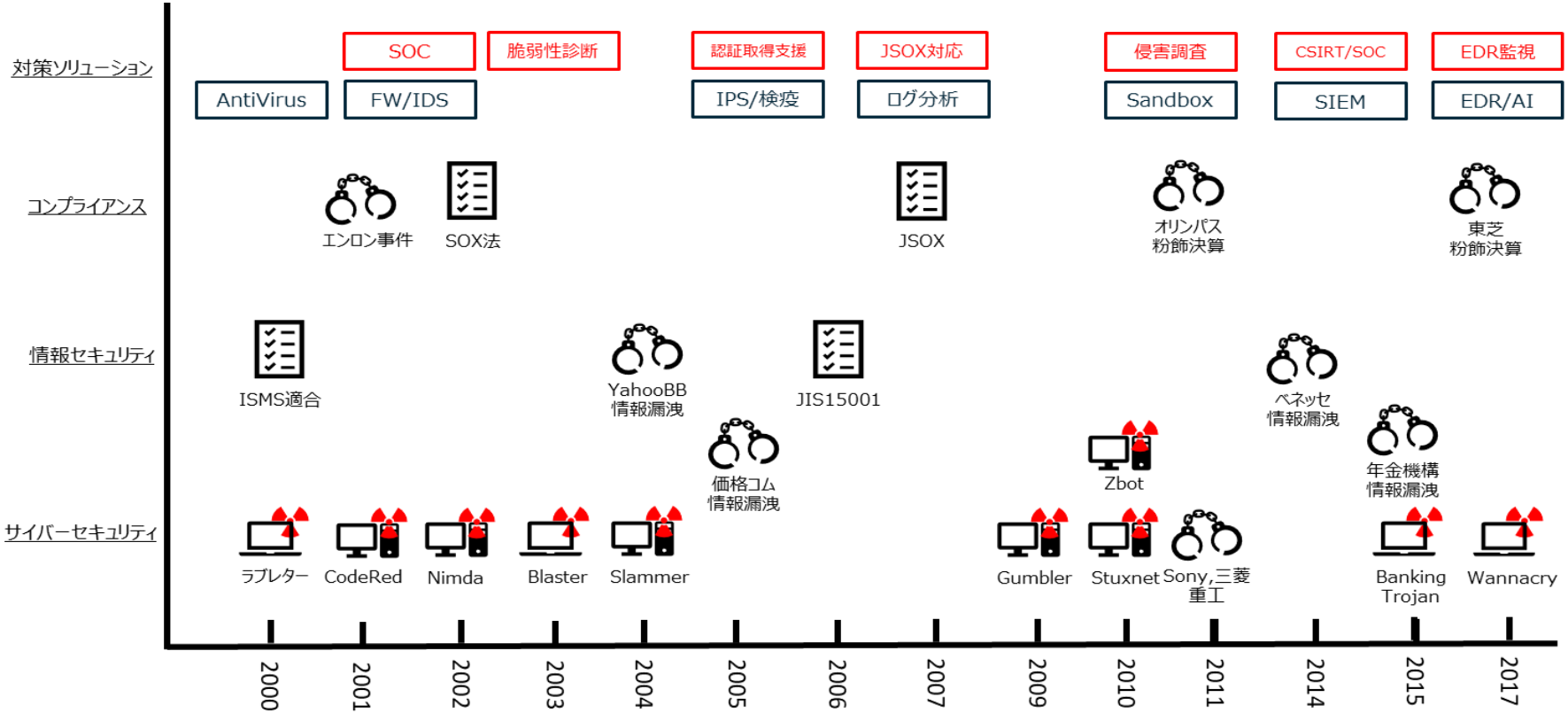
(d) 対応の範囲

（a）セキュリティ領域の範囲

■ セキュリティ領域

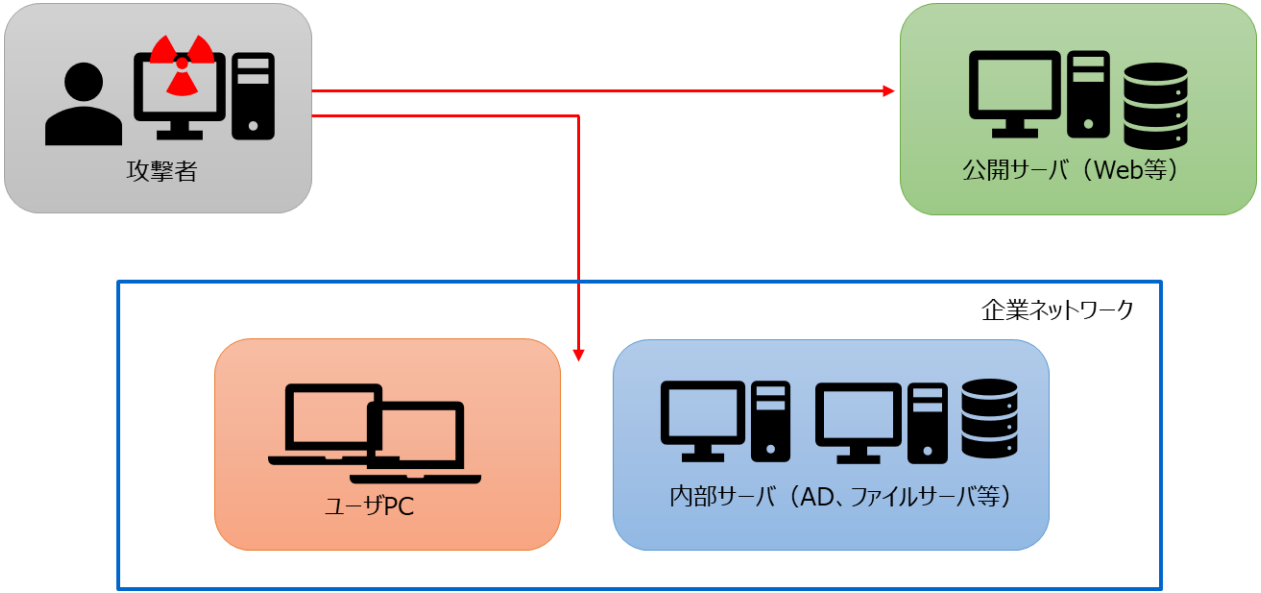
	内容	ソリューション
コンプライアンス・JSOX	広義のセキュリティ領域。事業継続の阻害なるリスクを取り除くことが目的。	・システム監査（JSOX） ・BCP
情報セキュリティ	個人情報を含む機微情報を守ることが目的。日本ではPマーク、ISMS認証取得により対応するケースが多い。	・Pマーク/ISMS認証取得支援 ・リスクアセスメント ・ログ分析システム
サイバーセキュリティ	攻撃者によるサイバー攻撃に対して防御を行うことが目的。標的型攻撃やバンキングトロジャン、ランサムウェアなど、攻撃は多岐に渡る。	・アンチウイルス製品 ・標的型攻撃対策製品（ATD等） ・IDS/IPS ・SIEM ・EDR

（参考）Security History



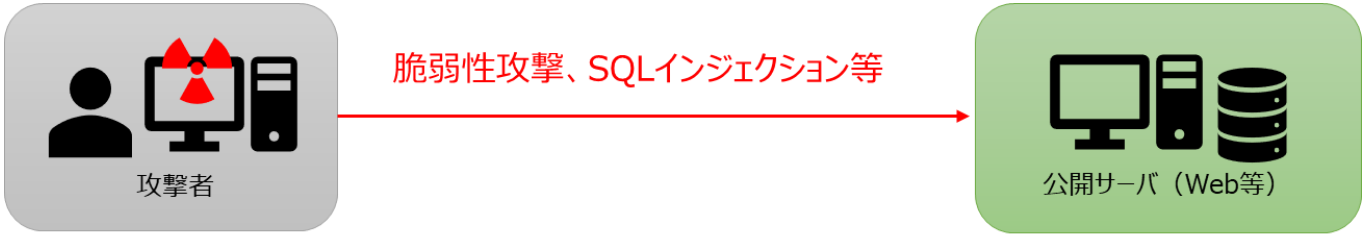
（b）システムの範囲

システム範囲は、大きく分けて「公開サーバ」「内部サーバ」「ユーザPC」の3種類となる。それぞれの用途や環境を理解することにより“対象となるリスク”を理解することができる。



公開サーバ

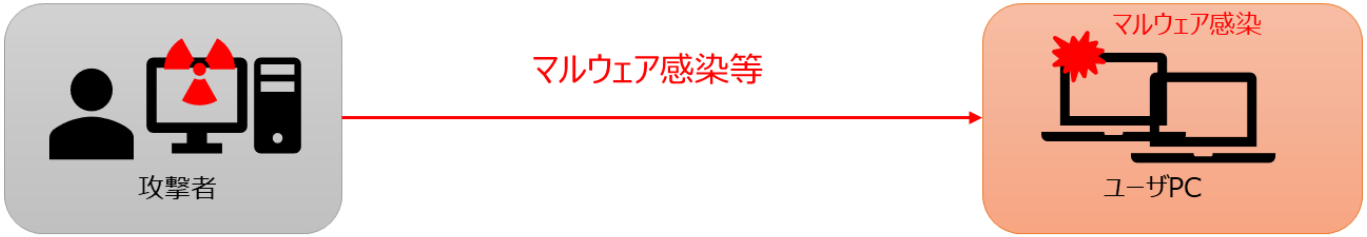
公開サーバは、Webサーバやメールサーバといった外部公開が前提となっているサーバシステムを指す。基本的にインターネット上のどこからでも接続が可能であるため、直接攻撃される可能性が非常に高い。また、攻撃形態として、脆弱性を突いた直接的な攻撃が多い。



種別	Webサーバ、メールサーバ、DNSサーバ、DBサーバ等
脅威(リスク)	外部公開しているため、脆弱性攻撃といった直接的な攻撃が脅威となる。サーバに個人情報等を保存している場合には情報漏えいのリスクがあり、更に不特定多数の人がアクセスするため、不正なファイルやスクリプトを埋め込まれることで加害者になる可能性もある。
備考	クラウド利用によりセキュリティ対策が変化している。

ユーザPC

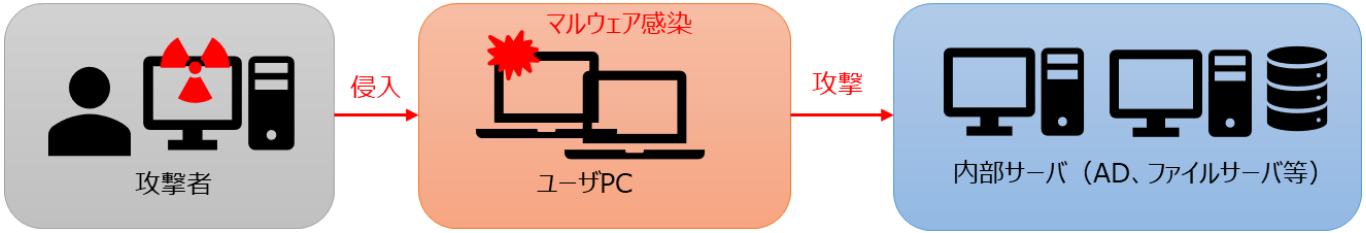
ユーザPCは、社員が利用するユーザ用PCを指す。メールによる外部とのやり取りや、Webページの閲覧、USBメモリの使用といったデータ通信の活動によりマルウェア等の感染の可能性が高い。また、リモートから不正操作されることで別のユーザPCや内部サーバを攻撃する拠点となることも多い。



種別	ユーザ用PC
脅威(リスク)	マルウェア感染が最も大きいリスクとなっている。マルウェアも内部でデータを不正取得するだけでなく、RATと呼ばれるリモートツール、ランサムウェアのようなデータ暗号化を行うもの。更に銀行口座を不正取得するバンキングトロジャンと多岐に渡る。また、ボットのように外部攻撃に利用されることも多い。
備考	標的型攻撃の7割はメールによる感染。但し、昨今では添付ファイルによる直接感染ではなく、別サイトからダウンロードする形で感染することが多い。

内部サーバ

内部サーバは、社内のイントラで使用する内部用サーバを指す。ドメイン管理のADサーバやファイルサーバ、イントラ用Webサーバ等、アクセス制限された状態で利用される。そのため、攻撃者から直接攻撃をされる可能性は低く、マルウェア等に感染したユーザPCを経由して攻撃を受けることが多い。



種別	ADサーバ、メールサーバ、ファイルサーバ、Proxyサーバ、DBサーバ、会計システム等のアプリケーションサーバ等。
脅威(リスク)	ファイルサーバや会計システム等、公開サーバよりも機微な情報が保存されているため情報漏えいした場合、企業として大きなダメージを受ける可能性が高い。また、内部システムのため、セキュリティ対策が公開サーバよりも弱いことが一般的であり、Windowsの脆弱性等を利用した攻撃を受けやすい。
備考	内部サーバへの直接侵入の可能性は低い。

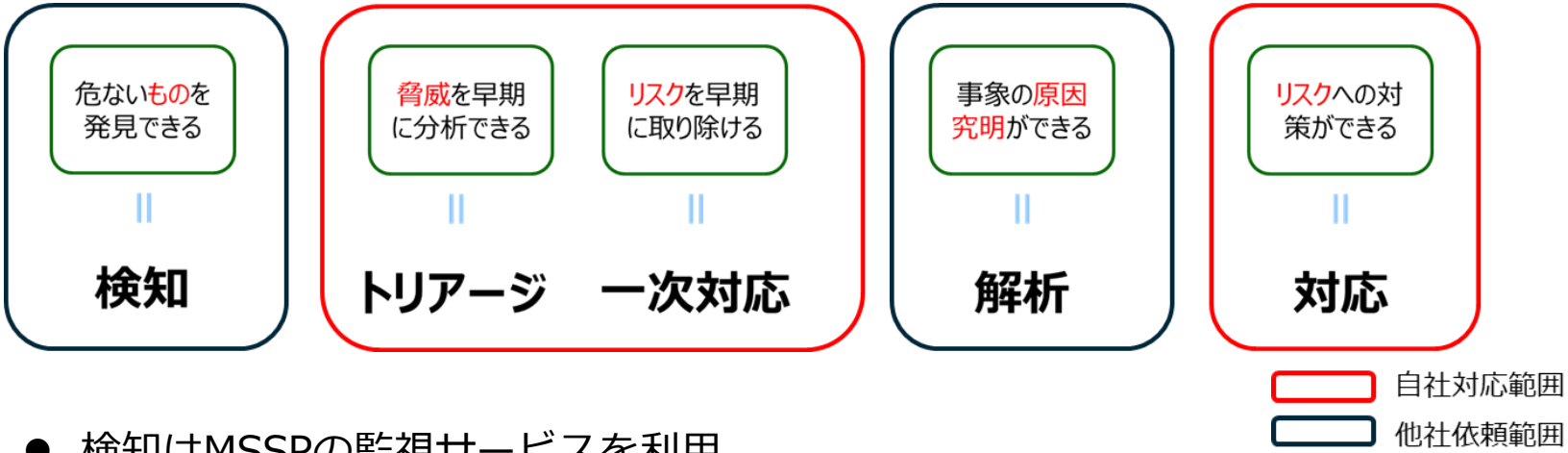
（c）インシデントの範囲

インシデントの範囲は、対象とするセキュリティ脅威となる。各セキュリティ範囲でのインシデント及びシステム範囲毎のインシデントは以下の通りとなる。

	インシデント	解説
コンプライアンス・JSOX	・不正会計 ・インサイダー取引 ・不正送金	コンプライアンスやJSOX等の会計監査に関するインシデント。不正会計やインサイダー取引等、内部統制上の問題によるセキュリティインシデントが対象となる。
情報セキュリティ	・メール/FAXの誤送信 ・個人情報の目的外利用 ・PC/USBメモリの紛失 ・システム設定不備による情報漏えい	PマークやISMSといった情報セキュリティ規格における準拠違反や人的ミスによる情報漏えい等のセキュリティインシデントが対象となる。マルウェア感染等も広義にはこちらに含まれるが、システム部分はサイバーセキュリティに記載している。
サイバーセキュリティ	・マルウェア感染 ・標的型攻撃による情報漏えい ・不正アクセスによる情報漏えい ・ランサムウェア感染 ・バンキングトロジャンによる金銭奪取 ・不正ログインによる情報漏えい	サイバーセキュリティに関するセキュリティインシデントが対象となる。コンプライアンスや情報セキュリティとの違いは攻撃者が意図的にインシデントを引き起こしていることが大きく異なる。

（d）対応の範囲

対応の範囲は、セキュリティ運用時にどこまで対応するかの範囲となる。
具体例は以下の通り。



- 検知はMSSPの監視サービスを利用
- トリアージ（端末・サーバの確認）は自社。実際にツールを使った調査も実施
- 一次対応も自社。隔離・遮断等を実施
- 解析は専門企業に依頼
- 対応は自社で実施

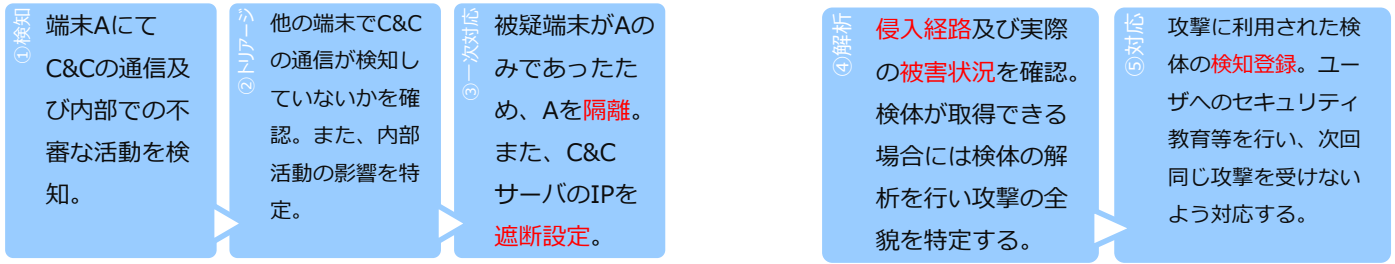
② クライテリア（基準）

クライテリアとは、セキュリティ運用の対応基準を指す。つまり、セキュリティ運用の“重要度（優先度）”を決めることになる。以下は具体例となる。

Severity	考え方	必要な対応
Critical	個人情報を含む機微情報が不正に奪取される。ランサムウェアが拡散して、業務がストップするなど、致命的なインシデントが発生。早期な調査や対応や、場合によってフォレンジック等の詳細な調査も検討が必要となる。	・影響範囲特定 ・被害拡大防止 ・侵害調査
High	個人情報が不正に奪取される。Webサイトが改ざんされるといった企業に大きなダメージを与える可能性があるインシデントが発生。早期な調査や対応が必要となる。	・影響範囲特定 ・被害拡大防止 ・侵害調査
Medium	マルウェアの感染や外部公開サーバへの脆弱性攻撃が発生。企業に大きなダメージ与えるものではないが、影響有無を含めて調査が必要となる。	・影響範囲特定 ・被害拡大防止
Low	スキャン等、攻撃の準備段階、もしくは実際の攻撃だが影響が無い検知を想定している。	・影響範囲特定

③ 対応内容

対応内容とは、“誰”が“どのように”実施していくかを決定する。具体的には以下の通りとなる。



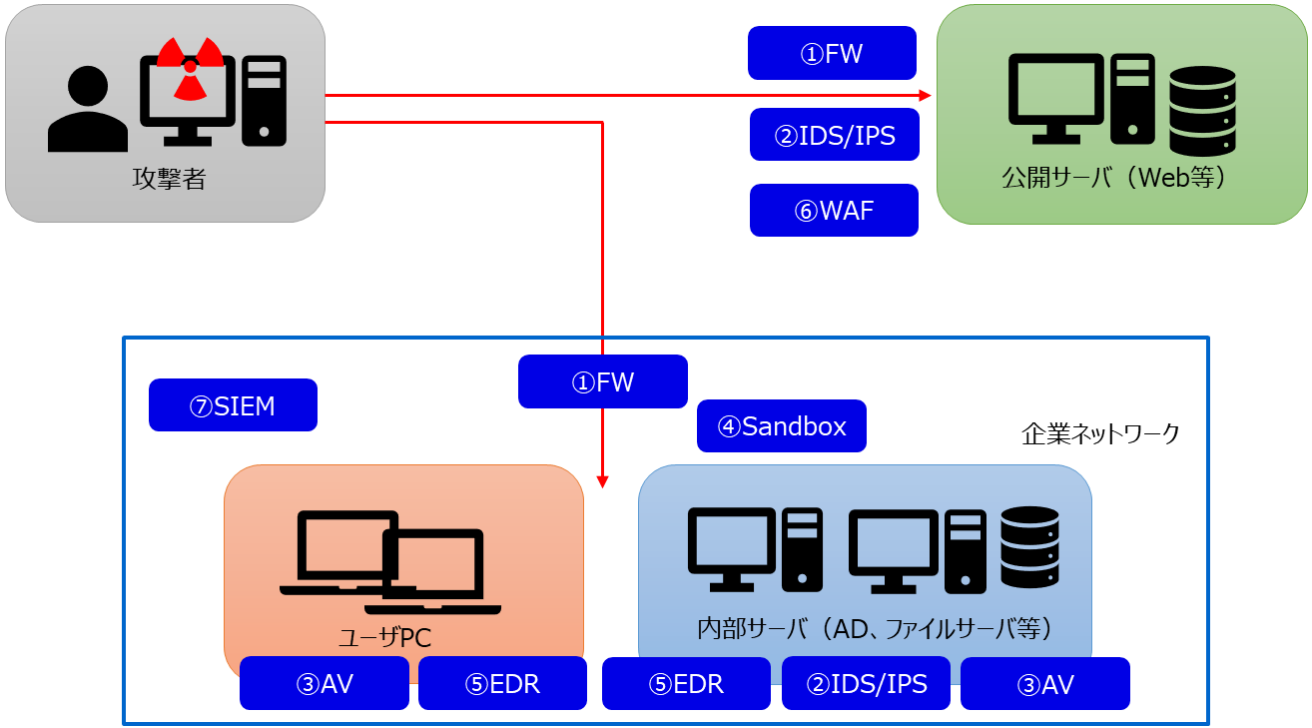
① 社外SOCで検出。Medium以上はトリアージを行うためにCSIRTチームにアラートを送付する。
② CSIRTチームが、リモートで端末の調査を行う。侵害が確認された場合には、一次対応を行う。
③ CSIRTチームから情報システム部に依頼をして、遮断・隔離設定を行う。
④ 専門企業に解析依頼を行う。
⑤ 解析結果を踏まえて、CSIRTチームが対応策を作成し、情報システム部が設定を行う。

事前準備のまとめ

項目		内容	備考
① 範囲	セキュリティ領域	「サイバーセキュリティ領域」を対象とする。	
	対象システム	対象システムは「内部サーバ」と「ユーザPC」を対象とする。	
	インシデント	サイバーセキュリティインシデントを対象とする。 ・標的型攻撃 ・ランサムウェア感染 ・マルウェア感染等	
	対応	検出、解析はMSSP及び専門企業に依頼。 トリアージ及び一次対応、対応を自社で実施する。	
② クライテリア	対応基準	対応基準は「Critical」「High」「Medium」「Low」の4段階。	
③ 対応内容	対応レベル	「Medium」以上はトリアージを実施。トリアージはリモートで実施し、侵害を確認した場合には一次対応として隔離・遮断を行う。	トリアージと一次対応は別組織で実施。

補足（セキュリティ機器の把握）

セキュリティ運用を構築するにあたり、自社で導入しているセキュリティ機器の把握も重要となる。



5. 運用構築

運用構築の進め方

運用構築で最も重要なものは「目的」を踏まえて、作業を明確化すること。

対象としたインシデントをどうやって見つけるのか。見つかったインシデントはどのように「情報」を持っているのかを考慮する。

検知したインシデントから影響範囲（どのような被害があるか、被害範囲はどのくらいか）を調査する手順や判断ポイントを明確にして、一次対応につなげる。

トリアージの結果、誰がどのように一次対応するのかを明確にする。また、実際に対応後に切り戻す手順等も考慮する。

運用構築の進め方（具体例）

事前準備で対象のインシデント（標的型攻撃、ランサムウェア感染、マルウェア感染）を決めたので、この内容をベースに進めていく。また、対象は「トリアージ」「一次対応」「対応」となるが、「検知」は必須であるため、記載し、「対応」は解析結果によるため、対象外とする。

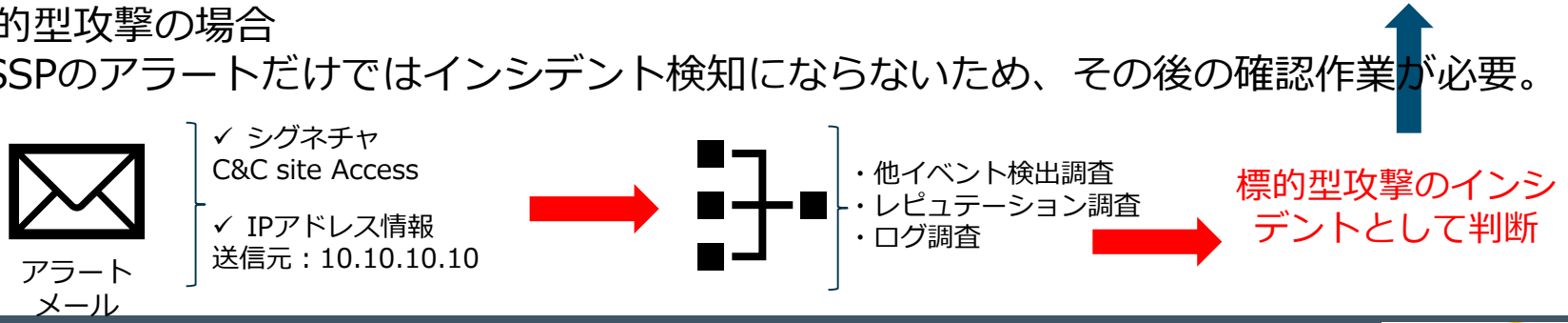
項目	実施内容	ポイント
検知	標的型攻撃、ランサムウェア感染、マルウェア感染の検知条件を作成する。また、検知条件に応じたクライテリアの設定を行う。	MSSPの検知がトリガーとなるため、検知内容をベースに各インシデントとして判断するための条件を作成する。
トリアージ	標的型攻撃、ランサムウェア感染、マルウェア感染の検知後、どのように調査を進めていくか具体的にフロー、手順（プレイブック）に落としていく。	調査内容をプロセスとしてまとめ、どのような情報（データ）やツールを使うか決定する。また、調査結果からどのような一次対応を行うかまで手順化する。
一次対応	トリアージの結果、実際に隔離や遮断を行う手順を作成する。	トリアージの結果から、アウトプットして得られる情報（IPアドレス等）を踏まえて作業手順とする。

検知

MSSPからのアラートをトリガーにした場合、内容が各セキュリティ機器のシグネチャベースになる可能性が高い。そのため、どのアラート（シグネチャ）がどのインシデントのトリガーとなるのかを決める必要がある。

■ マルウェア感染、ランサムウェア感染の場合
MSSPのアラートそのものがインシデント検知に直結となる。

■ 標的型攻撃の場合
MSSPのアラートだけではインシデント検知にならないため、その後の確認作業が必要。



トリアージ

トリアージでは、セキュリティのインシデント（事象）として何が発生しているか。また、影響範囲を特定して、被害拡大の防止を行う。運用を構築する上で、各インシデントを検知後に実施する作業内容を列挙し、フローや手順（プレイブック）にまとめる必要がある。

- 運用フロー
  インシデントを検知後、どのように作業を進めるかの運用フロー。分岐により、最終的な一次対応までの内容をまとめる。

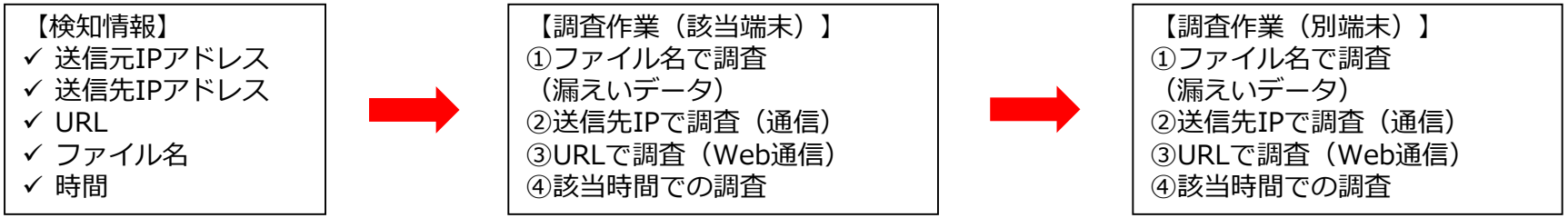
- 運用手順（プレイブック）
  運用フローをベースに、実際にどのような作業を行うかをまとめる。作業をプロセス化することで、汎用的に使えるようにする。

- プロセス表
  運用手順（プレイブック）から呼び出される実施作業。アウトプットまで想定することで、より現実的な内容とする。

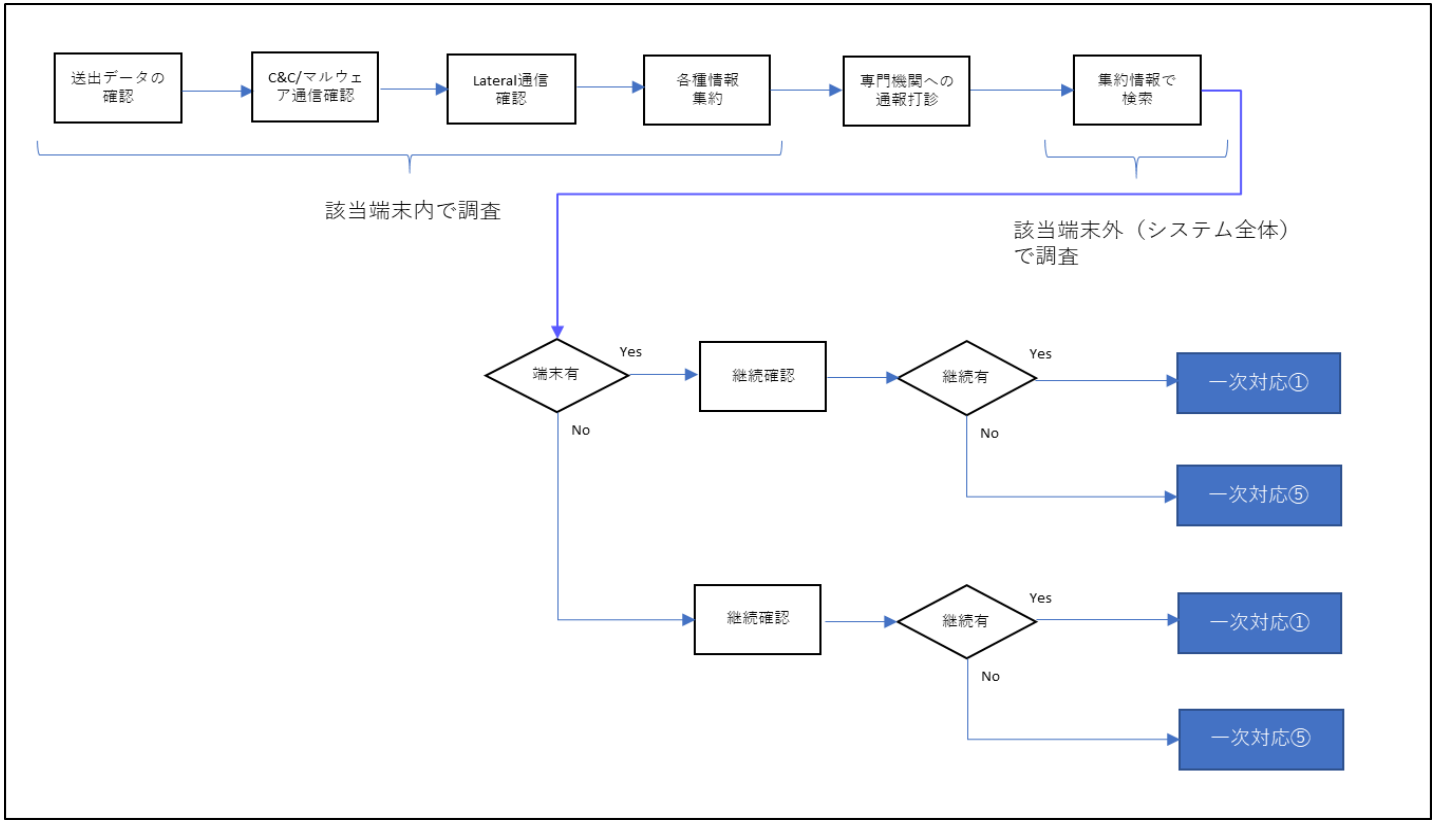
キーポイント

トリアージの手順を作成するキーポイントは以下の通り。

- インシデント検知時にトリアージ必要な情報（Input）を特定する
- 被害範囲を特定するために、調査の順番を考慮する
  （例：情報漏えいであれば情報の特定を最初にする等）
- 該当端末で調査した結果を踏まえ、その他の端末を調査できる手順を作成する
- 調査した結果を踏まえ、その後に何をするかを特定する



運用フロー例（標的型攻撃による情報漏えい）



プレイブック（標的型攻撃による情報漏えい）

【該当端末内の調査】
1. 送出データ（クレジットカード情報等）の確認を行う。確認内容は以下の通り。
- ファイルハッシュ（データがファイルになっていた場合）
- 送信先IPアドレス
- 送信プロセス（送信を行ったプログラムのプロセス）

■ プロセス：1.1 送出データ確認

2. C&C/マルウェア通信の確認を行う。確認内容は以下の通り。
- 送信先IPアドレス（C&Cサーバ のIPアドレス）
- 通信プロセス
- ファイルハッシュ（プロセス起動のファイルが特定できた場合）
- C&Cサーバ関連情報（ドメイン、ロケーション、登録者情報等）

■ プロセス：1.2 C&C/マルウェア通信の確認

3. Lateral通信（横感染）の確認を行う。確認内容は以下の通り。
- 送信先IPアドレス（横感染先）
- 通信プロセス
- ファイルハッシュ（プロセス起動のファイルが特定できた場合）

■ プロセス：1.3 Lateral通信の確認

4. 各種情報（上記）を集約する。

■ プロセス：1.4 取得情報の集約

5. 専門機関への通報について顧客に打診する。

■ プロセス：1.27 専門機関への通報打診

【該当端末外（システム全体）の調査】
6. 集約情報で同じ事象が無いか他端末のログ検索を行う。

■ プロセス：1.5 集約情報の検索

＜分岐＞
① 集約情報により同事象が別端末で確認ができた場合
→ 「7. 攻撃継続確認（事象が確認できた全端末）」に進む

② 集約情報により同事象が別端末で確認できなかった場合
→ 「8. 攻撃継続確認（該当端末のみ）」に進む

7. 攻撃継続確認（事象が確認できた全端末）を行う。

■ プロセス：1.6 攻撃継続確認

① 攻撃の継続が確認できた場合
→ 一次対応①に進む
② 攻撃の継続が確認できなかった場合
→ 一次対応⑤に進む

トリアージ（プレセス例）

#1	Process	#2	Method	Procedure	Output
1.1	送出データ確認	1.1.1	送出データファイルの調査	【送出ファイルが特定できている場合】 ファイル名から該当ファイルのハッシュを取得する。	ファイル名 ファイルハッシュ
		1.1.2	送出データ通信の調査	送出データのファイル名/ファイルハッシュで検索し、送出データ通信の送信先IPアドレス、サービスやポート番号を特定する。	IPアドレス （サービス/ポート番号）
		1.1.3	送出データ送信プロセスの調査	送信先IPアドレスで検索し、送信したプロセスを特定する。	プロセス名
1.2	C&C/マルウェア通信の確認	1.2.1	マルウェアファイルの調査	【マルウェアファイルが特定できている場合】 ファイル名から該当ファイルのハッシュを取得する。	ファイル名 ファイルハッシュ
		1.2.2	C&C/マルウェア通信の調査	該当通信のIPアドレスで検索し、サービスとポート番号を特定する。	IPアドレス （サービス/ポート番号）
		1.2.3	C&C/マルウェア通信プロセスの調査	送信先IPアドレスで検索し、C&C/マルウェア通信プロセスを特定する。	プロセス名

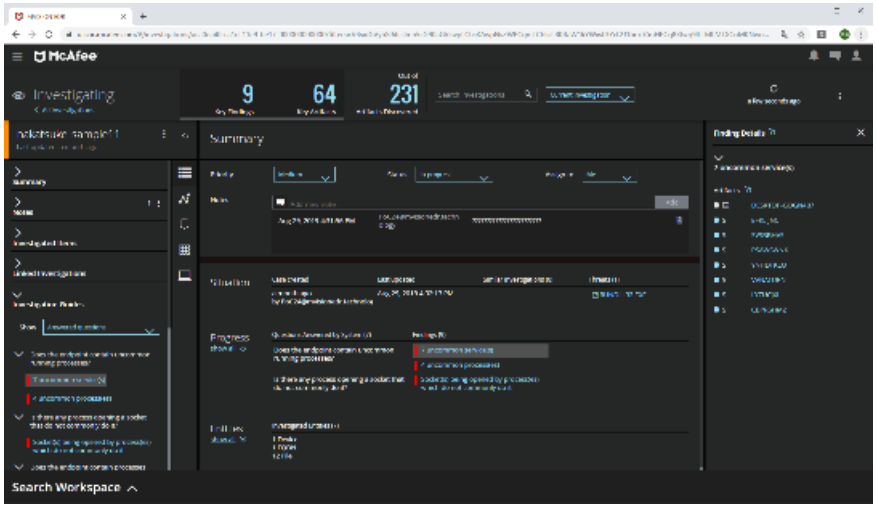
一次対応

一次対応	実施事項	解説	備考
一次対応①	送信先の通信遮断＋隔離	■ プロセス：2.1 通信遮断、2.2 端末隔離 監視対象端末が特定の送信先に対して情報の送信やC&Cサーバへのアクセスを行っているため、送信先（攻撃者のサーバ等）に対して通信遮断を行う。 また、被害端末の隔離を行うことで被害拡大を防止する。	
一次対応②	送信元の通信遮断＋隔離	■ プロセス：2.1 通信遮断、2.2 端末隔離 監視対象端末が不特定多数の端末に対して、不正な通信（ワーム等の内部感染活動）を行っているため、送信元（被害端末）に対して通信遮断を行う。 また、被害端末の隔離を行うことで被害拡大を防止する。	
一次対応③	送信先の通信遮断	■ プロセス：2.1 通信遮断 監視対象端末が特定の送信先に対して情報の送信やC&Cサーバへのアクセスを行っているため、送信先（攻撃者のサーバ等）に対して通信遮断を行う。	

トリアージ作業を補完するMVISION EDR

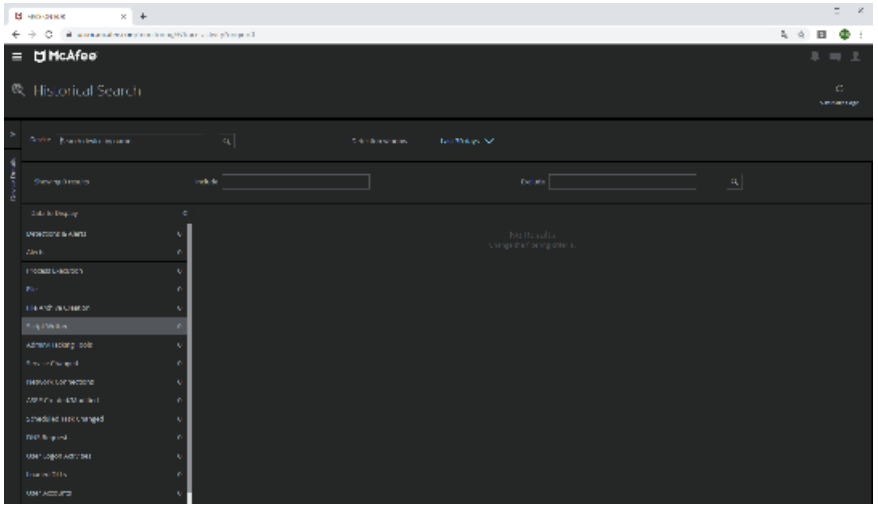
トリアージ作業を保管するツールとして「MVISION EDR」は非常に効果的となる。特にInvestigation機能の「Q&A」を使うことにより、プレイブックで作成する調査を自動的に実施することができる。

【該当端末での調査（手動）】



MVISION EDR Investigation

【システム全体での調査（手動）】



MVISION EDR Historical Search

運用構築のまとめ

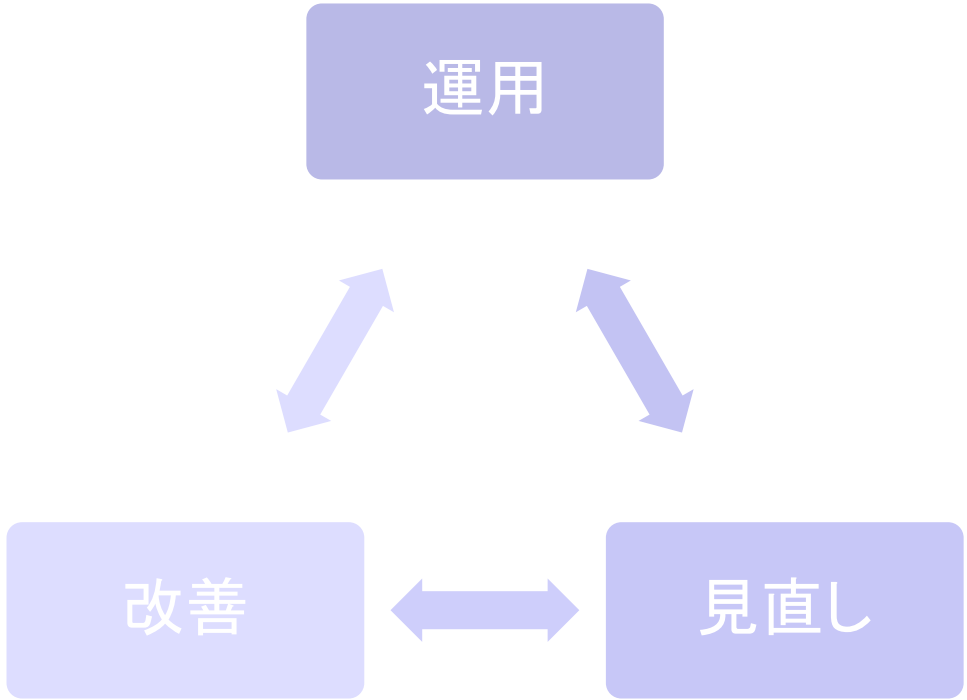
運用構築のポイントは以下の通り。

- インシデントの“特定”が非常に重要となる
- MSSPの監視サービスを利用する場合には、自社で調査を補足する
- トリアージは実際の作業を列挙したうえで、フローや手順に落とす
- トリアージの作業については専用のツール“EDR製品”を使うことで簡略化できる
- MVISION EDRの”Investigation機能”は非常に有効

6. 運用・改善

運用・改善

運用・改善では、構築した運用を実施する。また、実施した運用の見直しを行い、
改善を図っていく。

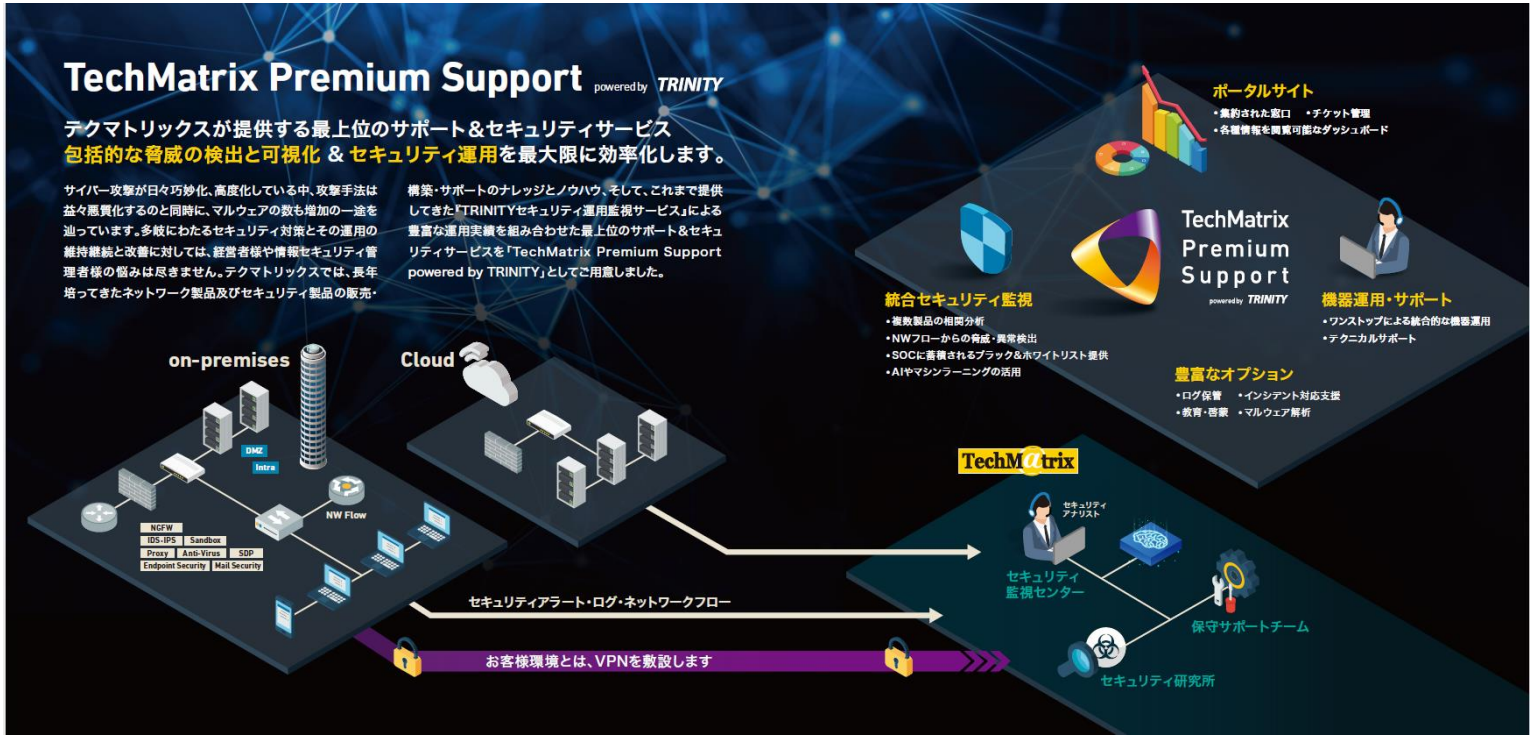


- 運用
  インシデント検知、トリアージ、一次対応の内容を全て実施する。
- 見直し
  作業フローや手順を使った運用を行う上で、不備や不足があるものを調査する。
- 改善
  見直しをした結果を踏まえて、運用の改善を図る。

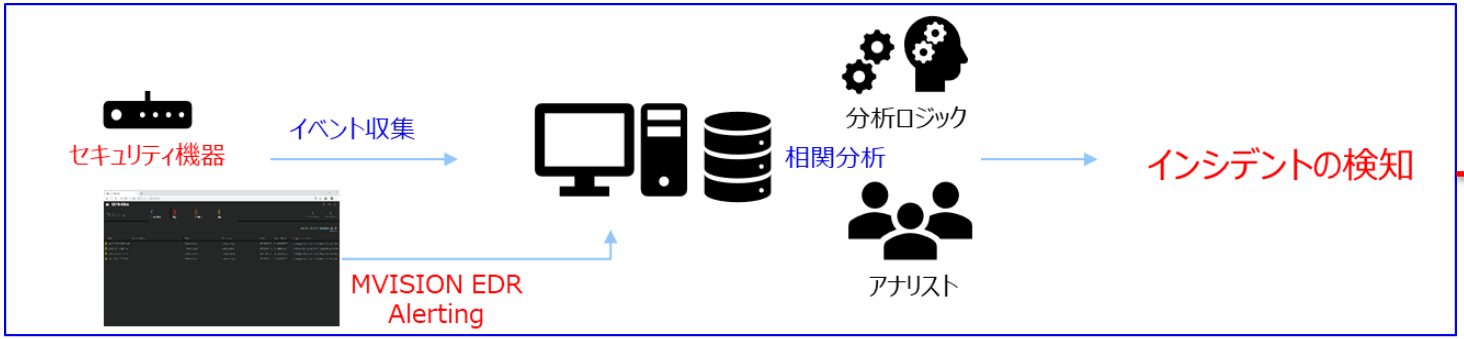
7. TechMatrix Premium Supportとは

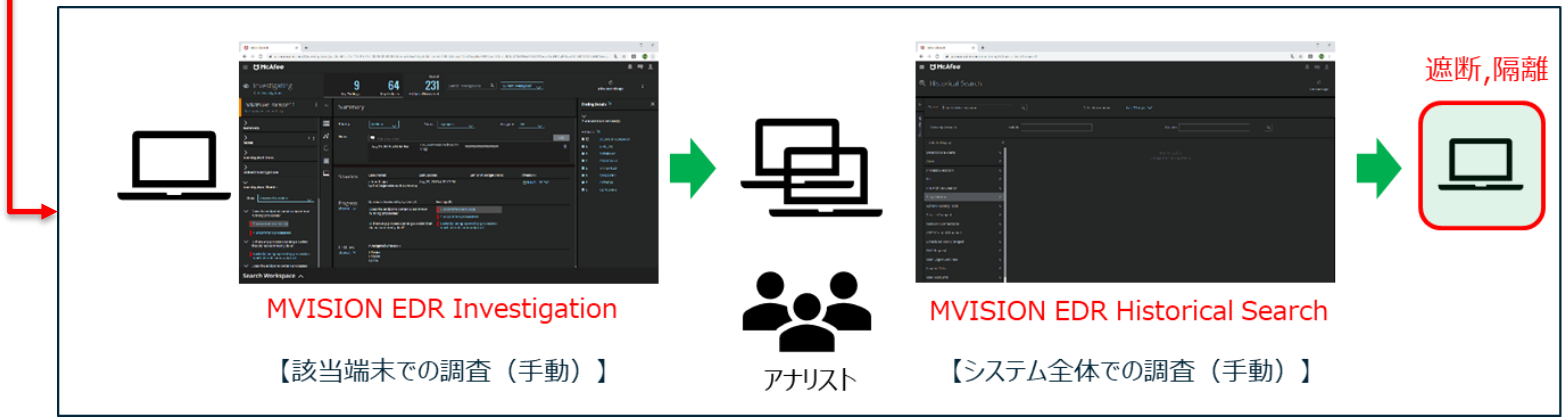
TechMatrix Premium Supportとは

テクマトリックスが提供する最上位のサポート&セキュリティサービス



初動対応オプション





8. 本日のまとめ

運用・改善

本日のまとめは以下の通り。

- 適切なセキュリティ運用を構築するには「自社のリスクを把握する」ことが重要
- 構築には「事前準備」が必要で、それをベースに具体的な運用を構築する
- インシデントを事前に決定すると、より適切な手順が作りやすい
- インシデントの検出は「脅威検知」の中から事前に決めることが重要
- プレイブックは、実施するフローを作成して、プロセス化することでより広範囲な対応が可能となる
- 調査にMVISION EDRを利用することで、プレイブックの実施事項を簡略化できる
- TechMatrix Premium Supportの初動対応オプションで検出・トリアージ・一次対応が可能となる

ご清聴ありがとうございました。

TechMatrix
テクマトリックス株式会社