



cutting through complexity

リスクシナリオに基づくSIEM (セキュリティ脅威検知システム) 導入の事例

KPMGコンサルティング株式会社

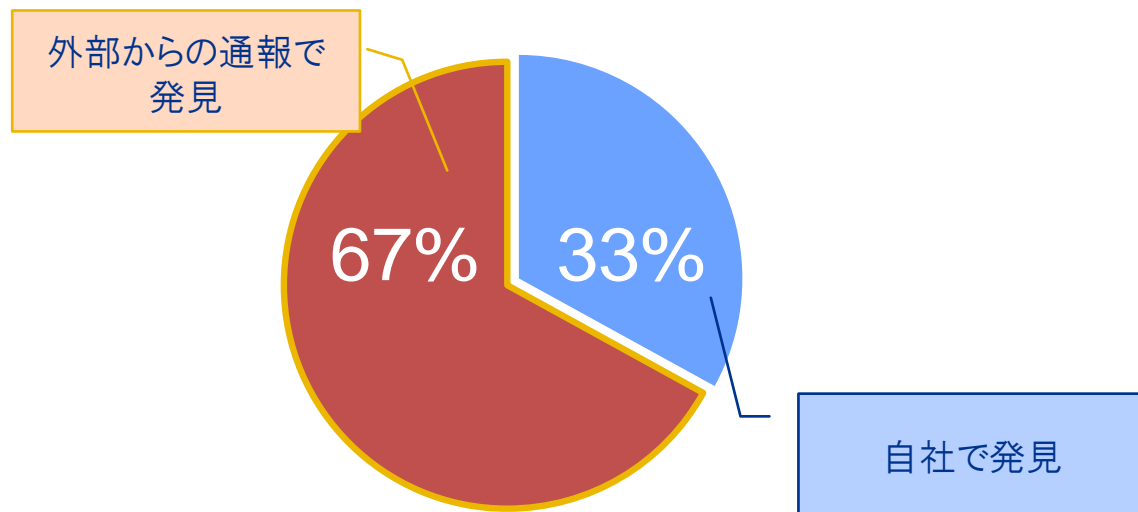
2015年1月20日



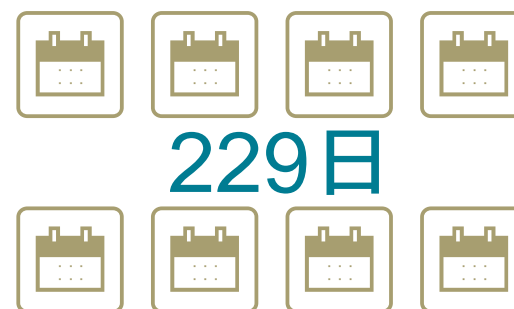
本ご紹介する内容

- これまでのサイバー攻撃に対する対策は、いかにして予防するかに重点が置かれていましたが、時々刻々と進化する攻撃を完全に防御することは困難になってきています。
- そのため、サイバー攻撃が発生することを前提として捉え、攻撃を速やかに発見し対処することが肝要となっていますが、以下の統計のとおり各企業はその実現に苦慮しています。

発見の主体



発見までの日数(中央値)

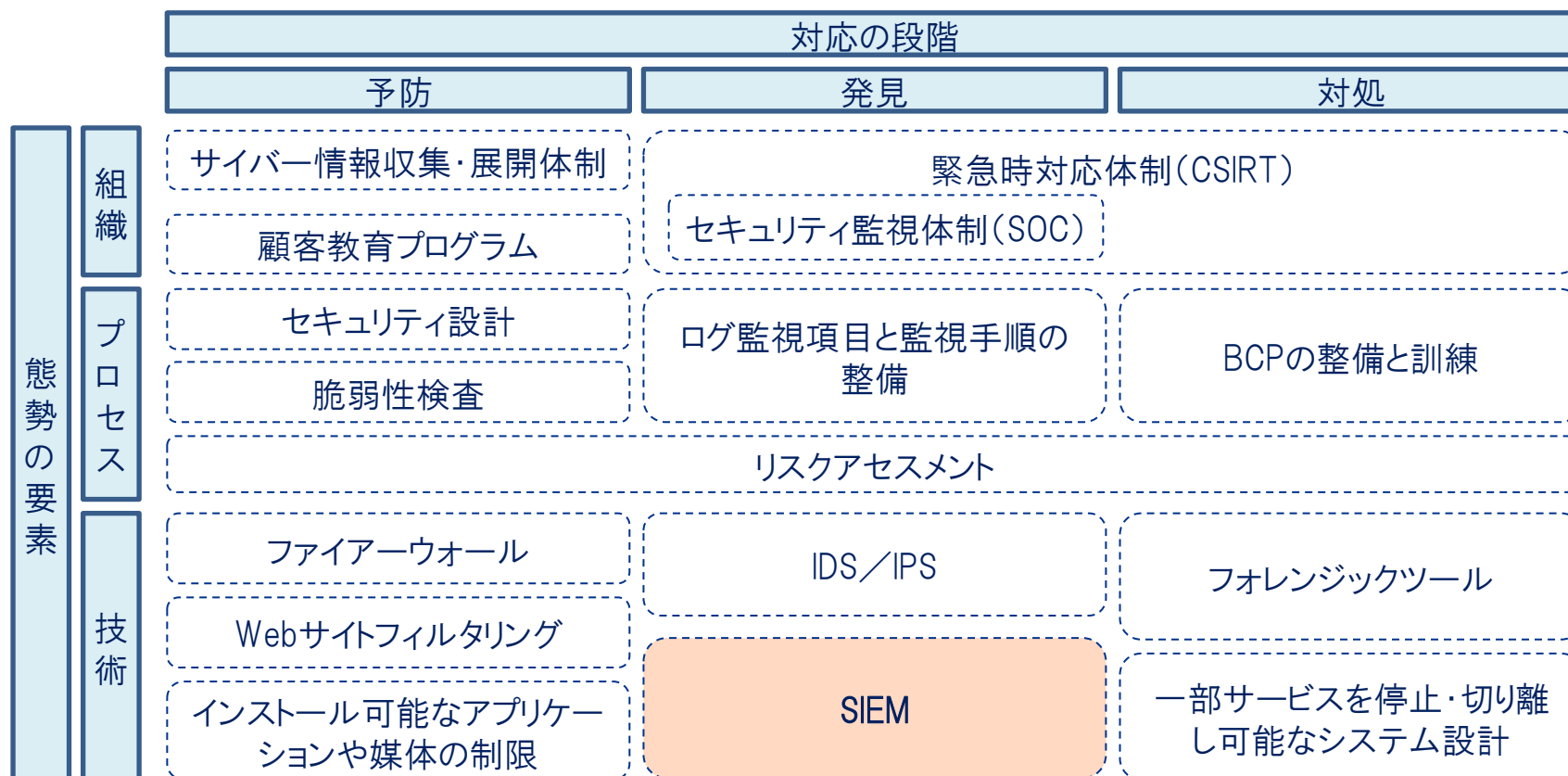


出典：「2014 THREAT REPORT」(Mandiant)

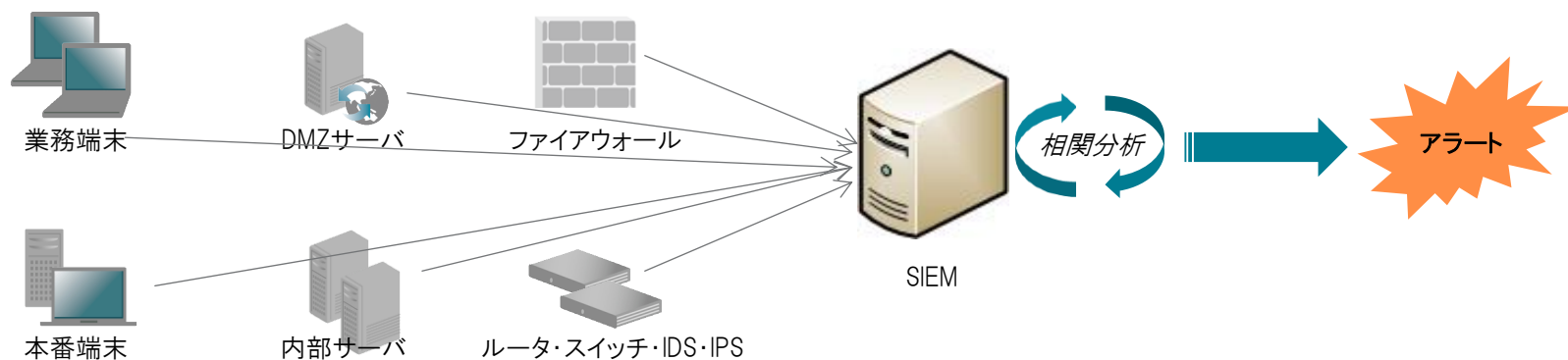
➡ このような背景のもと、昨今重要性が増している“SIEM(セキュリティ脅威検知システム)”の概要と導入を成功させるためのポイント、ならびに支援事例についてご紹介いたします。

企業に求められる活動の全体像とSIEMの位置づけ

- サイバーセキュリティ管理態勢は、組織、プロセス、技術の視点から整理することができます。
- このうち、SIEMは技術的な発見的活動に位置づけられます。



- SIEMとは、Security Information and Event Managementの略称で、サーバやネットワーク機器、各種アプリケーション等から集められたログに基づいて、異常を管理者に通知するシステムのことを指します。



- 従来のログ分析の問題点を解消し、より早く、より正確に攻撃・不正を検出するためのツールとなります。

従来のログ分析の問題点	SIEMの特徴
大量のログを手により網羅的にチェックするのは困難	✓ ネットワーク上の様々なデバイス・アプリケーション等から発生するイベントログを <u>一元的に集約管理し自動的に分析</u> します
内部不正のモニタリング体制を構築することが困難	✓ SIEMを導入する企業の多くは、不正検知対象のインシデントについて、 <u>外部要因と内部要因の両方を対象</u> としています
一度のイベントだけ、もしくは一つのログだけでは、異常であることの確定が困難	✓ 複数のログの <u>相関分析</u> により、ログデータに記録された「いつ、誰が、何を実施した」のかを判別します
ログの分析は日次や月次で実施され、不正検出までのリードタイムが長い	✓ 平時と比較してユーザや外部からの通信の不正な行動を、 <u>リアルタイムに検知</u> します

- 前頁のとおり、SIEMは強力な攻撃発見ツールとなり得るため、現在各企業において導入が進んでいます。
- しかし、その効果を最大限に発揮するために留意すべき事項が存在します。一般的にみられるSIEM導入の失敗要因は以下のとおりです。

【失敗要因】

リスクアセスメント無しにSIEMシステムを導入してしまう

【影響】

- 攻撃を受けやすい経路とそうでない経路を特定しないままSIEMを導入してしまうと モニタリング範囲が膨大となり、結果として費用対効果を最大化できません。
- また、“結局SIEMを入れてどのようなリスクシナリオを検出できるのか？”が曖昧なままプロジェクトが進行してしまうと、経営陣や業務部門から、“SIEMはあらゆる脅威を検出できる魔法の箱である”といった誤解を生んでしまいます。

現在取得しているサーバやネットワーク機器のログをそのまま投入する

- SIEMの相関分析のインプットは各機器のログとなるため、これらログの取得水準が相関分析の精度に大きく影響します。したがって、現在取得しているログ水準が不十分である場合はSIEM導入と並行してシステム開発・設定変更が必要です。
- また、逆に不正検出につながらない過剰なログを取得している場合、それらをSIEMに投入すると ストレージにかかるコストの増大につながります。

SIEMシステムを導入したが、その運用態勢を整備しない

- SIEMは、個社の環境に応じた日々のメンテナンスが肝要となります。そのため、SIEMの異常検知アラートの構成管理やアラートを監視する体制を整備しない限り、SIEMの効果を最大化できません。

- 前頁を踏まえ、求められる対応を以下に整理します。

【失敗要因】

リスクアセスメント無しにSIEMシステムを導入してしまう

現在取得しているサーバやネットワーク機器のログをそのまま投入する

SIEMシステムを導入したが、その運用態勢を整備しない

【求められる対応】

- ✓ 上流工程において、ネットワーク構成やセキュリティ統制を確認し、特に侵入が懸念される攻撃経路を特定する。
- ✓ そのうえで、SIEMで検出するリスクシナリオを明確化する。

- ✓ リスクシナリオを検出するための“取得すべきログ”を把握する。
- ✓ また、“取得すべきログ”に対し、“現在取得できているログ”の水準を確認し、そのギャップを明らかにする。ギャップは、“不正を検出するための重要性”と“対応に係るコスト”の観点から対応優先度を検討する。

- ✓ SIEM製品の導入のみならず、SOCやCSIRTの整備も並行して進める。

SIEM導入時の進め方の全体像(例)

- SIEM導入事例をもとに、進め方の一例を以下にお示します。

■ 実施項目(例)

①: リスクシナリオの洗出しとシステム要件の策定

- リスクシナリオの作成
- 標的となるシステムの特定
- 攻撃経路とSIEM対象ログの特定

②: SIEMシステム・ベンダーの選定

- RFPおよびベンダー選定基準の作成
- 製品選定

③: SIEMシステムの構築・導入時の成果物のレビューとPMO

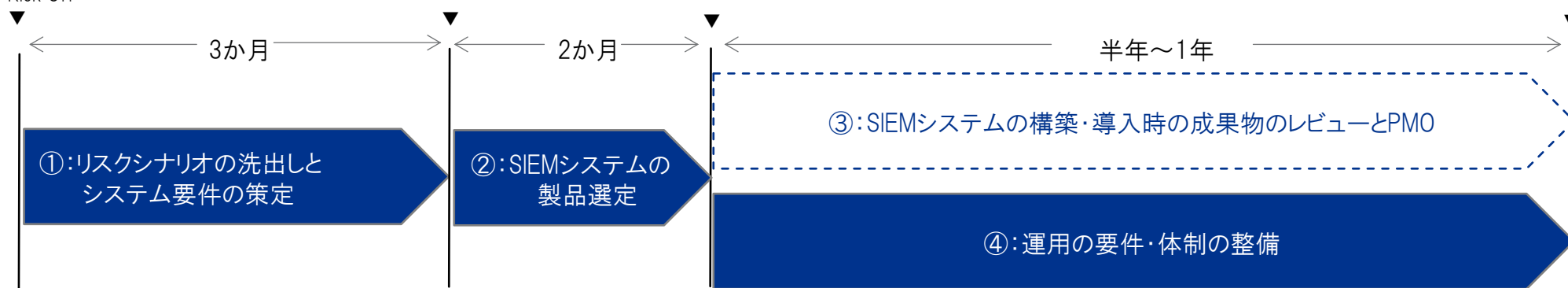
- 検知トリガー・ホワイトリストのレビュー
- 構築・導入等のPMO

④: 運用の要件・体制の整備

- システム・業務の運用要件の策定
- SOC、CSIRTの整備

■ スケジュール(例)

Kick Off

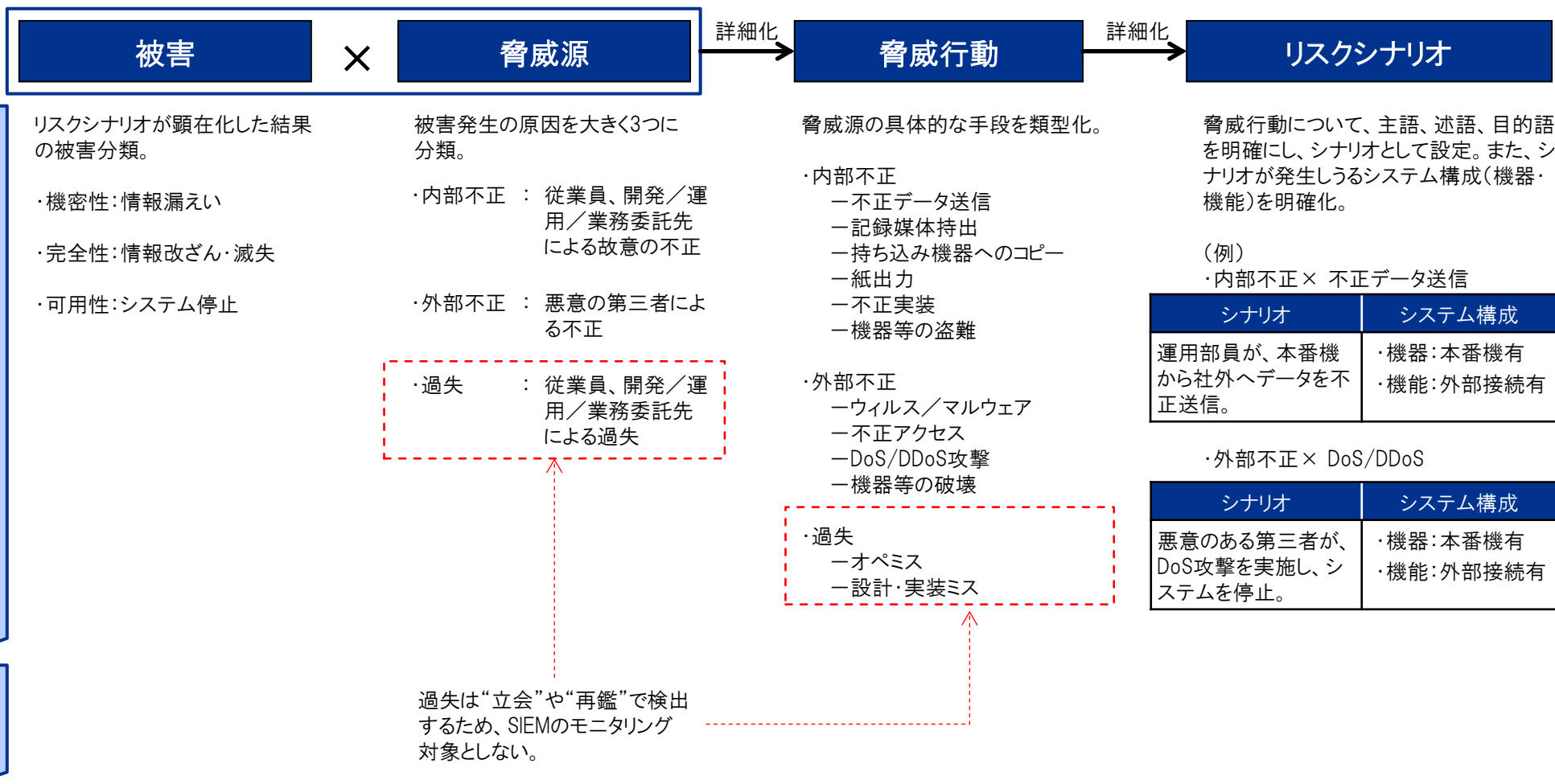


⇒ 項目①、②、④の具体的な実施内容について、次ページ以降ご説明いたします。

①:リスクシナリオの洗出しとシステム要件の策定

1:リスクシナリオの作成

- リスクシナリオについて、網羅性を説明できるよう洗い出した上で、SIEMでカバーすべきシナリオを特定します。



①:リスクシナリオの洗出しとシステム要件の策定

2: 標的となるシステムの特定

- リスクシナリオが顕在化した場合の影響度や攻撃の動機となり得る資産の有無を分析し、標的となる可能性が高いシステムを特定します。
- システム毎の重要度評価が実施されている場合、その情報を起点に作業を進めます。

■ システム重要度評価結果をベースとした対象の一次選定(イメージ)

	A	B	C
機密性	機密性に係るリスクシナリオの対象(候補)		対象外
完全性	完全性に係るリスクシナリオの対象(候補)		対象外
可用性	対象外	対象外	対象外

一次
選定
(例)

絞り込
み(例)

“内部/外部不正の標的となりやすい資産を保有しているかどうか”という目線で絞り込みを実施。

- ・ 個人情報
- ・ 医療情報
- ・ 研究・開発等に係るインサイダー情報(自社／他社) 等

①:リスクシナリオの洗い出しとシステム要件の策定

3:攻撃経路とSIEM対象ログの特定

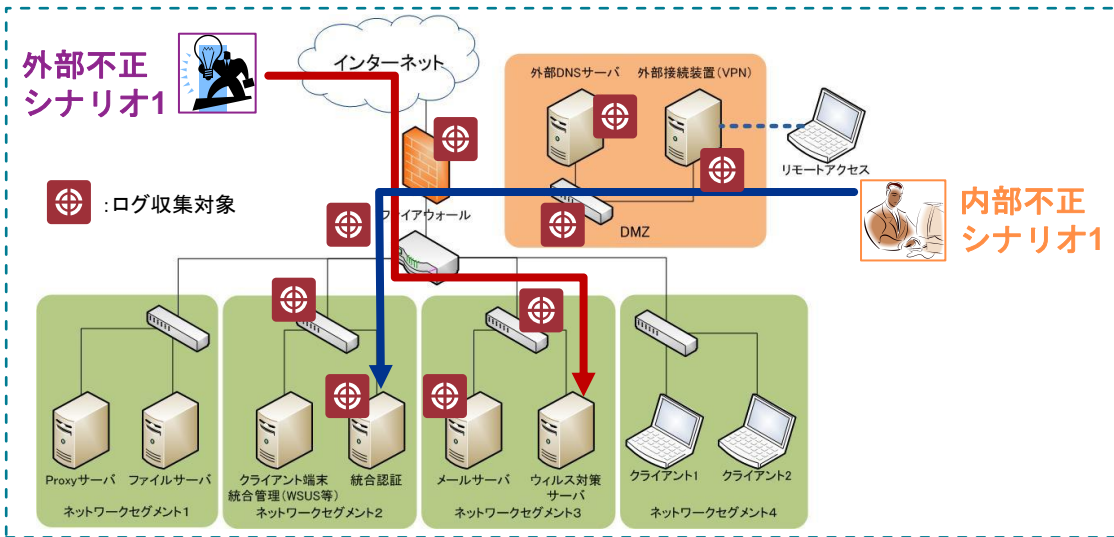
- 標的となるシステムに対する攻撃の経路を特定し、SIEMシステムのモニタリング対象とすべきログを整理します。

① 対象システムのそれぞれについて
構成機器を整理

② ネットワーク構成図上の各機器
の配置状況を確認

③ ネットワーク構成図上で、
各リスクシナリオの侵入経路・
通信経路を確認

④ ログ取得すべき対象と種類を
整理



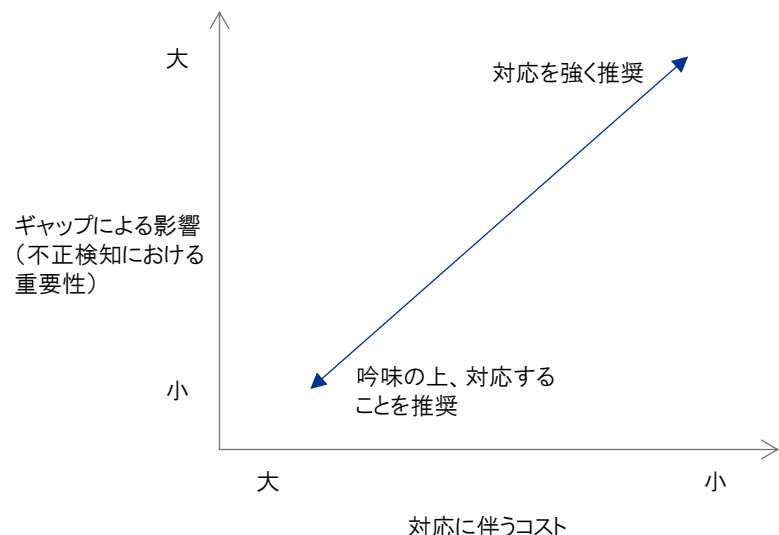
システム名	機器情報				ログ		
	機器種別	名称	メーカー	台数	取得要否	種類	容量(月次)
Aシステム	サーバ	GWサーバ	●●	2	○	syslog, DB log...	XXX MB
	ネットワーク機器	L3スイッチ	●●	4	○	IOS log...	XXX MB
	端末	汎用端末	●●	5	○	windows event log...	XXX MB
	その他	ディスク	●●	3	×	—	—
Bシステム	ネットワーク機器	L2スイッチ	●●	5	×	—	—
	サーバ	Webサーバ	●●	3	○	Apache log...	XXX MB

①:リスクシナリオの洗い出しとシステム要件の策定

4:ログ取得状況の現状評価

- 前頁にて洗い出した“取得すべきログ”に対する現在のログ取得状況を調査いただき、その結果を評価します。

【評価の考え方】



【評価の具体例】

対象システム・ネットワーク	UNIX系システム	
ギャップ	<ul style="list-style-type: none"> ログオン失敗、アカウント作成、アカウント変更、パーミッション変更のログが取得できていません。 	
上記ギャップによる影響 (不正検知における重要性)	大	<ul style="list-style-type: none"> ログオン失敗が記録されていないため、悪意のあるログオン試行(パスワード推測攻撃・ブルートフォースアタックなど)が検出できません。 アカウント作成・変更、パーミッション変更が記録されていないため、ログオン後の不正が疑わしい操作を検出することができません。
対応に伴うコスト (一般的想定)	小	<ul style="list-style-type: none"> OSにおけるログの出力設定により比較的容易に取得が可能と考えられます。 通常の内部システムであれば、ログ量も数MB/日と考えられ、ストレージに対するコストインパクトは小さいものと想定されます。
対応の推奨	強く推奨	重要なUNIX系システムについては、上記ログを取得するようシステム対応することを推奨いたします。

①:リスクシナリオの洗い出しとシステム要件の策定

5:SIEM導入で検出するリスクシナリオの明確化

- 現状のログ取得状況とギャップ事象に対する対応判断を踏まえ、SIEM導入で検出するリスクシナリオを明確化し、プロジェクト内外の関係者と共通認識を形成します。

SAMPLE

リスクシナリオ		被害 (○:あり、 -:なし)			侵入準備 (情報収集、ポート スキャン、ウィルス 作成など)	内部侵入 (ウィルス感染、アカウント取得など)			目的達成 (データ送信、削除、システム停止など)		攻撃維持 (バックドア通信の 維持など)
分類	行動	機密 性	完全 性	可用 性							
外部 不正	メールによるウィルス・マルウェア 感染を契機としたデータ流出	○	-	-	【カバ外】	メール 【カバ外】 SPAM・ウィルスメールフィルタリングのログはクラウドサービスであり取得できない(一部ウィルス駆除ログはノートで取得しているが極めて限定的)。ノートのジャーナルは取得しているがログ量が膨大である一方でSIEM連携する効果が低いと考えられるため連携しない。	ウィルス感染 【カバ外】 アンチウィルスアラートを取得する。	アカウント取得 【カバ外】 Active Directoryを含む重要サーバのOSのログを取得。	データアクセス 【カバ外】 重要サーバのDBログ等 を取得。	データ送信 【カバ外】 ネットワークログ等 を取得。 データ改ざん 【カバ外】 重要サーバのDBログ等 を取得。	バックドア通信 【カバ外】 ネットワークログ等 を取得。
	メールによるウィルス・マルウェア 感染を契機としたデータ改ざん・ 削除	-	○	-							
	メールによるウィルス・マルウェア 感染を契機としたシステム停止	-	-	○					システムアクセス 【カバ外】 重要サーバのOSログを 取得。	システム停止 【カバ外】 死活監視で対応。	
	ウェブからのウィルス・マルウェア 感染を契機としたデータ流出	○	-	-	インターネットからの ポートスキャンなどの 偵察行為は外部データ センターで監視しており、 SIEMにフィードでき ない。	ウェブ 【一部カバ外】 プロキシサーバの情報を 取得する。 なお、XXXのWebプロキシ ログはNATされており活用 できないため、SIEMに連 携しない。			データアクセス 【カバ外】 重要サーバのDBログ等 を取得。	データ送信 【カバ外】 ネットワークログ等 を取得。 データ改ざん 【カバ外】 重要サーバのDBログ等 を取得。	
	ウェブからのウィルス・マルウェア 感染を契機としたデータ改ざん・ 削除	-	○	-							
	ウェブからのウィルス・マルウェア 感染を契機としたシステム停止	-	-	○					システムアクセス 【カバ外】 重要サーバのOSログを 取得。	システム停止 【カバ外】 死活監視で対応。	
	外部記憶媒体・持込機器による ウィルス・マルウェア感染を契機と したデータ流出	○	-	-		機器接続 【一部カバ外】 重要サーバエリアのアクセ ススイッチへの機器接続 はカバ外。 端末のUSBポートの接続 情報は、設置・管理コスト を考慮し、取得しない。			データアクセス 【カバ外】 重要サーバのDBログ等 を取得。	データ送信 【カバ外】 ネットワークログ等 を取得。 データ改ざん 【カバ外】 重要サーバのDBログ等 を取得。	
	・ ・ ・										

②: SIEMシステム・ベンダーの選定

SIEM製品およびベンダー選定では、SIEMシステムの独自性を考慮した製品選定基準を設けることが重要です。

選定基準			選定ポイント
大項目	中項目	小項目	
機能	ログ収集および管理	<ul style="list-style-type: none"> データベースバックアップやその他維持管理に係るアクションの実行中においても、ログソースを収集できる機能を有する。 	<ul style="list-style-type: none"> 安定した運用を実現するために考慮すべきポイントと考えます。
	相関分析	<ul style="list-style-type: none"> さまざまなデータに基づく相関分析機能を有する。(ルール/脆弱性/統計/過去事象/行動) Anti-Virus, IDS/IPS等ベンダーから受ける最新の脅威・ゼロデイ情報を収集する機能を有する。 	<ul style="list-style-type: none"> 様々な相関分析を実施可能であることにより、インシデントをより確実に発見可能です。
	ダッシュボード	<ul style="list-style-type: none"> 機器固有のフォーマット/形式に依存せず、ユーザが理解しやすい様なフォーマット/形式でイベントが表示される。 リアルタイムで発生するイベントがすべて表示される機能を有し、各イベントを選択した際にその詳細が表示される機能を有する。 	<ul style="list-style-type: none"> 様々な機器から収集した情報が分散することなく、一元的に表示される視認性の良さを確認する必要があります。
	イベント/インシデント管理	<ul style="list-style-type: none"> イベント情報収集時に、イベントを生成したシステムおよびユーザ情報等を収集している。 	<ul style="list-style-type: none"> イベント発生源を特定できる情報を保持することで、迅速にインシデントの分析が可能です。

SAMPLE

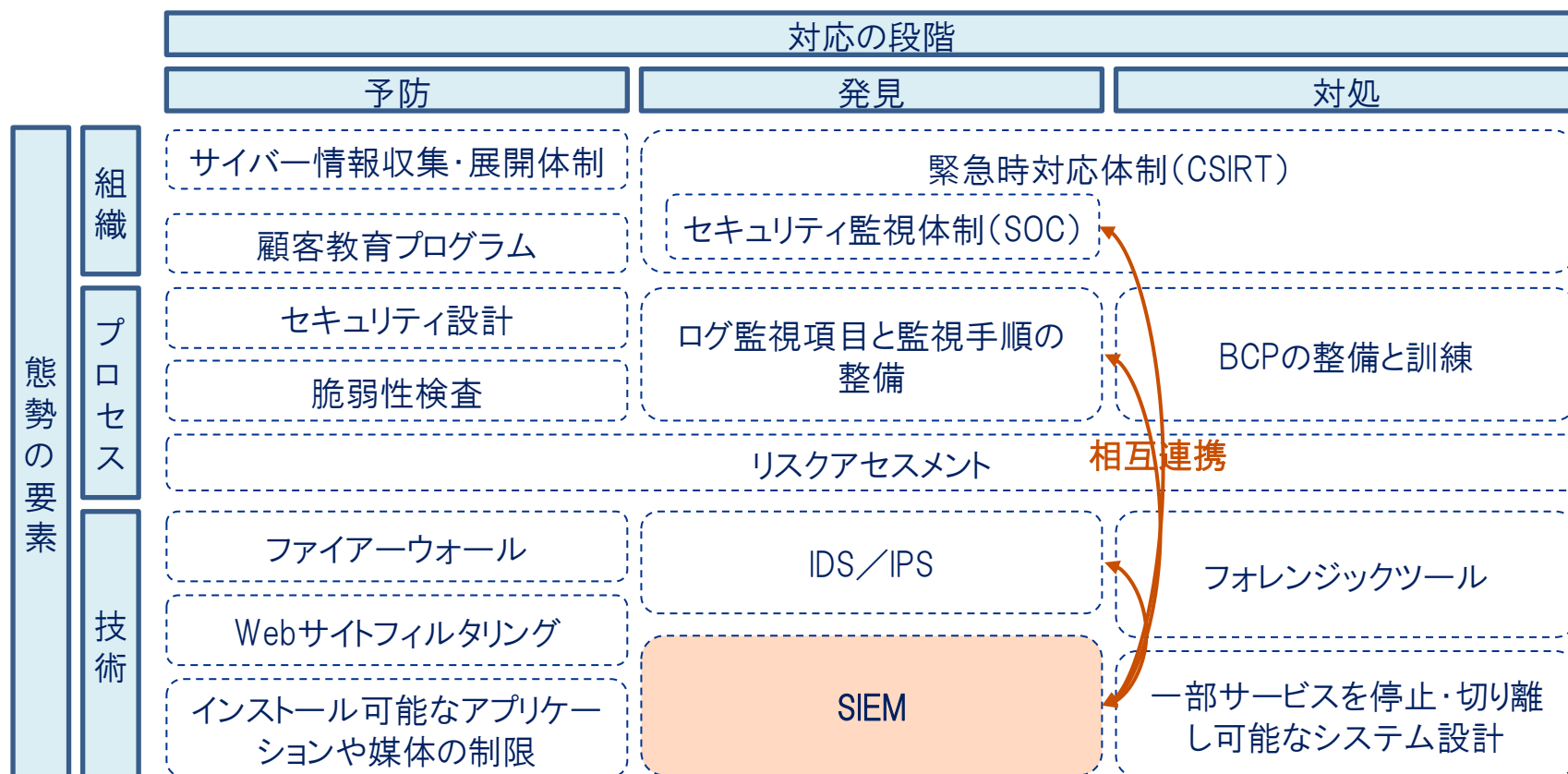
②: SIEMシステム・ベンダーの選定

SAMPLE

選定基準			選定ポイント
大項目	中項目	小項目	
システム要件	ストレージ	<ul style="list-style-type: none"> 生データおよび正規化データの両方を保存することができる。 オンライン、アーカイブ、バックアップ用の階層化されたストレージを有する。 ストレージに保存されたログソースはすべて暗号化されている。 	<ul style="list-style-type: none"> 製品によってはストレージの暗号化に対応していないものがあります。
	可用性	<ul style="list-style-type: none"> ログソース収集機器が停止した場合に、自動で代替のログソース収集機器に切り替わる、もしくは代替の仕組みでログソース収集が維持される仕組みを有する。 ストレージの不具合が発生した際に、リカバリー可能なストレージ構造および容量を有する。 	<ul style="list-style-type: none"> システム停止等、緊急時における対応が用意されている必要があります。
	拡張性	<ul style="list-style-type: none"> SIEMシステムの導入計画に合った拡張性を有する。 	<ul style="list-style-type: none"> 収集対象とする装置の種類および機種、対応プロトコル等が貴社の要求条件と合致している必要があります。
	セキュリティ	<ul style="list-style-type: none"> IPv6に対応している。また、ベンダーはIPv6への切替実施時にサポート体制を有する。 暗号化による通信は256bit以上の暗号で暗号化されており、今後のトレンドに合わせて適切な暗号方式が選択できる。 貴社に実装されている認証方式をサポートしている。 データ定義言語(DDL), データ操作言語(DML), データ制御言語(DCL)等、データベースに対する行動が記録・保存される。 不正ログインを防ぐ機能を有しており、またログイン行動を追跡できる機能を有する。 	<ul style="list-style-type: none"> 常に有効な暗号方式を採用できることで、セキュアな環境を維持できます。 貴社の利用方法に合った認証方式をサポートすることで、運用性を向上させることができます。
サポート		<ul style="list-style-type: none"> ベンダーは導入した製品のすべての機器に対して最新のパッチが当てられていることを確認している。 ベンダーはSLAを提示し、定期的にSLAに対する評価レポートを提示している。 ベンダーまたはSOC受託ベンダーは、以下の各工程についてサポートを提供している。 -システム設定作業、インシデント対応手順、日常の運用手順、SOC技術者育成および育成資料の提供、業務報告・改善手順、データ保存・廃棄ルールおよび手順、SOCの事業継続管理体制構築、セキュリティパッチの適用・最新化 ログ収集・分析に関して、相関分析ルールのアップデート等の継続的な最適化支援がある。 	<ul style="list-style-type: none"> 構築のみならず、その後の運用までをサポートしている。 SIEMの有効活用のためには、運用者による継続的な分析の最適化が必要です。

④:運用の要件・体制の整備 企業に求められる活動の全体像とSIEMの位置づけ

- サイバーセキュリティ管理態勢は、組織、プロセス、技術の視点から整理することができます。
- このうち、SIEMは技術的な発見的活動に位置づけられますが、組織・プロセスの発見的活動と連携し総合的に発見的能力を構築することが重要です。

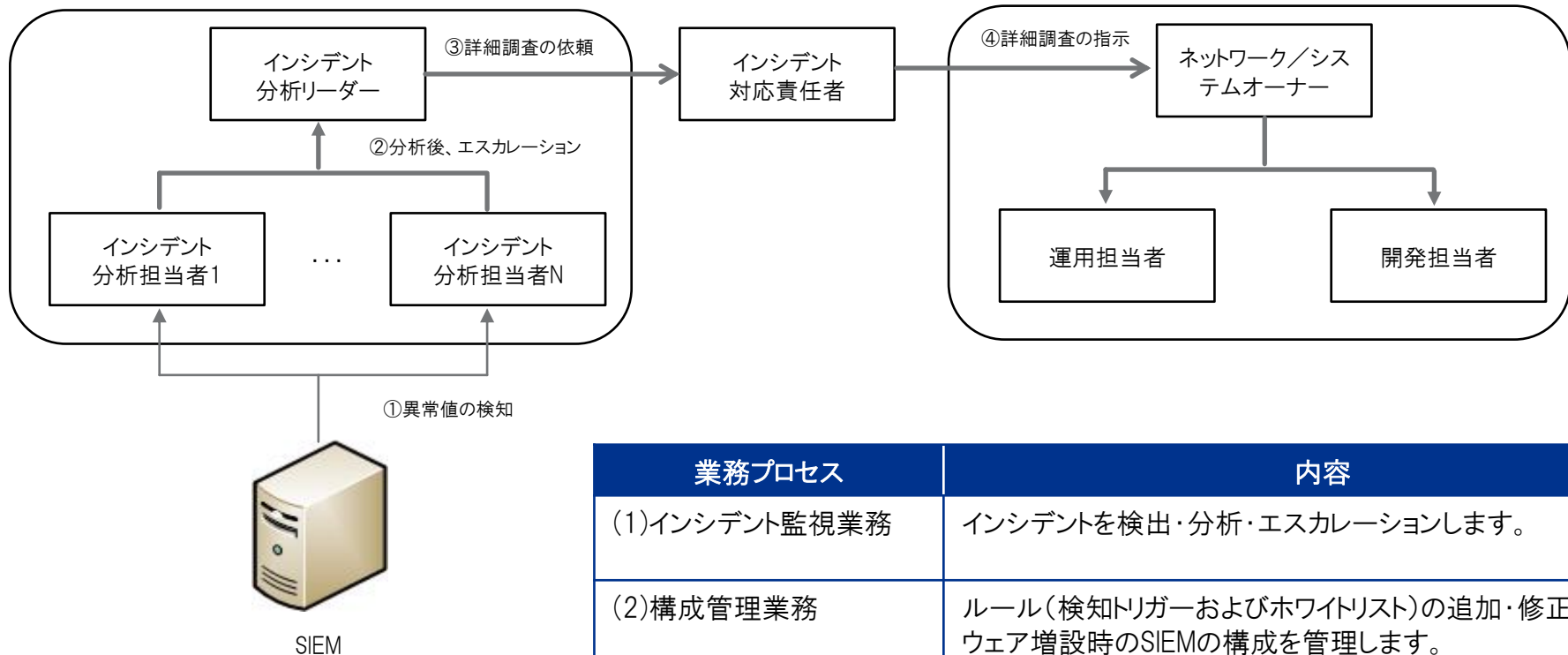


④:運用の要件・体制の整備

SIEMの運用態勢

- (1)インシデント監視、(2)構成管理、(3)チーム運営などの業務運営が必要です。

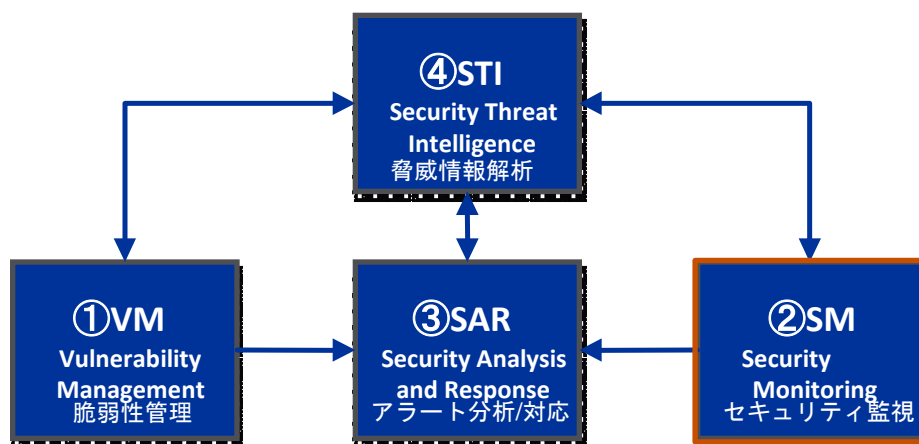
■SIEMの運用態勢(例)



業務プロセス	内容
(1)インシデント監視業務	インシデントを検出・分析・エスカレーションします。
(2)構成管理業務	ルール(検知トリガーおよびホワイトリスト)の追加・修正やハードウェア増設時のSIEMの構成を管理します。
(3)チーム運営業務	要員の教育・リソース(人的、サーバー等)管理・インシデント対応責任者とのコミュニケーション管理等の業務を運営します。

- CSIRTに求められる機能は4つに大別できます。
- そのうち、SIEM/SOCは②SM(セキュリティ監視)に該当する機能と考えられます。

CSIRTの全体像



- ① VM(脆弱性管理)
公開されている種々の脆弱性情報に対するパッチの適用状況やポートの開放状況等について把握し、一括管理する仕組みを指します。
- ② SM(セキュリティ監視)
SIEMなどのツールを用いて、SOCによりセキュリティ情報を監視します。
- ③ SAR(アラート分析／対応)
セキュリティ監視において検知したアラート情報を分析し、脅威の発生有無／影響範囲などを分析し、必要な対応を行います。
- ④ STI(脅威情報解析)
競合や別の業界等、自社の外部で発生している攻撃情報などを収集し、自社における脅威や耐性を把握します。

- これまでサイバー攻撃に対しては、予防的な対策を中心に各社対応を進めてこられましたが、攻撃手法が時々刻々と進化するなか、完全に防ぎきることが困難となりつつあります。そのため、攻撃が発生することを前提として捉え、攻撃を速やかに発見し対処することが肝要となっています。
- SIEMはより早く、より正確に攻撃・不正を検出するために有効なツールとなり得ます。ただし、その効果を最大化するためには、導入時に以下の点についてご留意いただく必要があります。
 - SIEMで検知したいリスクシナリオを明確にする
 - 標的となるシステム(=リスクシナリオが顕在化すると困るシステム)の優先順位を付ける
 - 攻撃経路を特定し、SIEMで監視すべきポイントと、監視すべきログを特定する
 - 監視すべきログが現在取得できているかどうかを調査し、不足していればSIEM導入と並行して開発・設定を進める
 - SIEMの特性を踏まえた製品選定基準を用いてプロダクトを選定する
 - SIEMを運用するSOCおよびCSIRTの整備を並行して進める



cutting through complexity

お問合せ先

山下 雅和(ディレクター)

KPMGコンサルティング株式会社

TEL : 03-3548-5305

masakazu.yamashita@jp.kpmg.com

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供しよう努めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

© 2015 KPMG Consulting Co., Ltd., a company established under the Japan Company Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name, logo and 'cutting through complexity' are registered trademarks or trademarks of KPMG International.