



## 企業の危機管理担当者が把握すべきサイバーセキュリティ最前線

Deloitte Tohmatsu Risk Services 丸山満彦  
2018年08月31日

# About Deloitte Cyber Risk

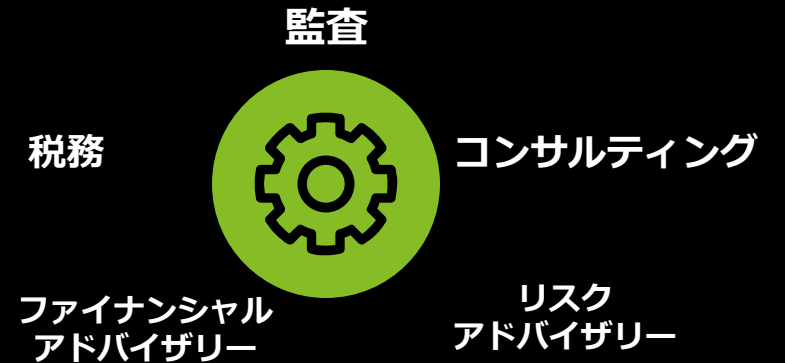
# Deloitteとは

Deloitte（デロイト）は、**監査**、**コンサルティング**、**ファイナンシャルアドバイザーサービス**、**リスクアドバイザー**、**税務**およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。

**全世界150を超える国・地域**のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを Fortune Global 500® の8割の企業に提供しています。

“Making an impact that matters”を自らの使命とするデロイトの**約263,900名の専門家**からなります。

グローバル収入は**388億ドル/4.4兆円**（2017年）



**150を超える国・地域**

**約263,900名の専門家**

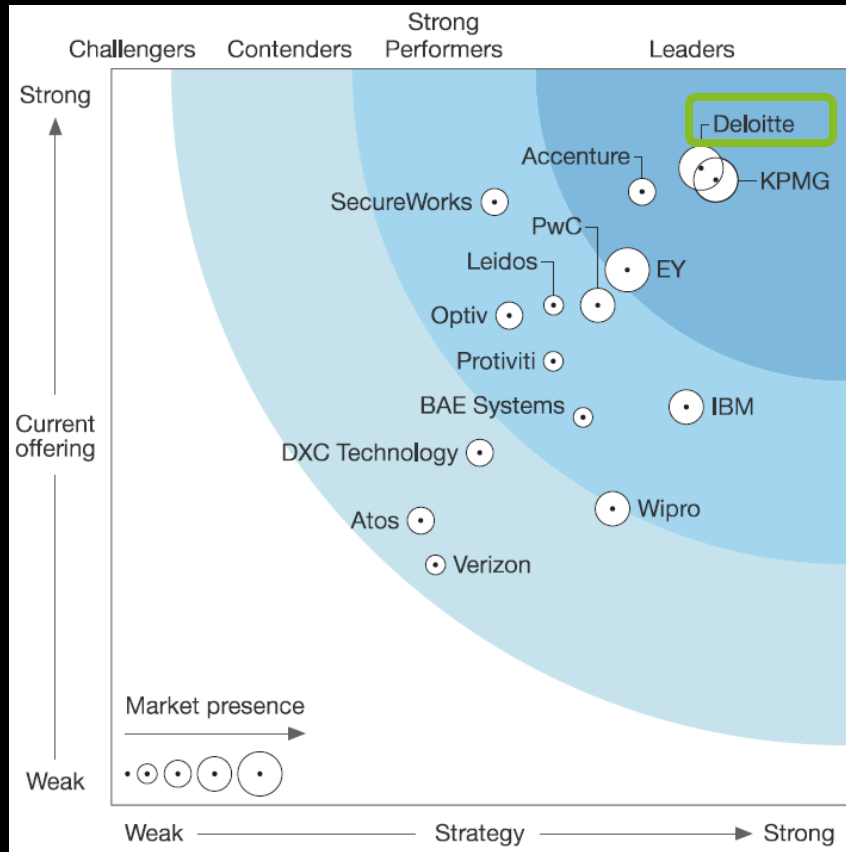


**収入は388億円/4.4兆円**

# Deloitteは、最先端かつ高度なナレッジを有していると評価されています

## Forrester

情報セキュリティサービスコンサルティングにおいてデロイトは世界的なリーダーです



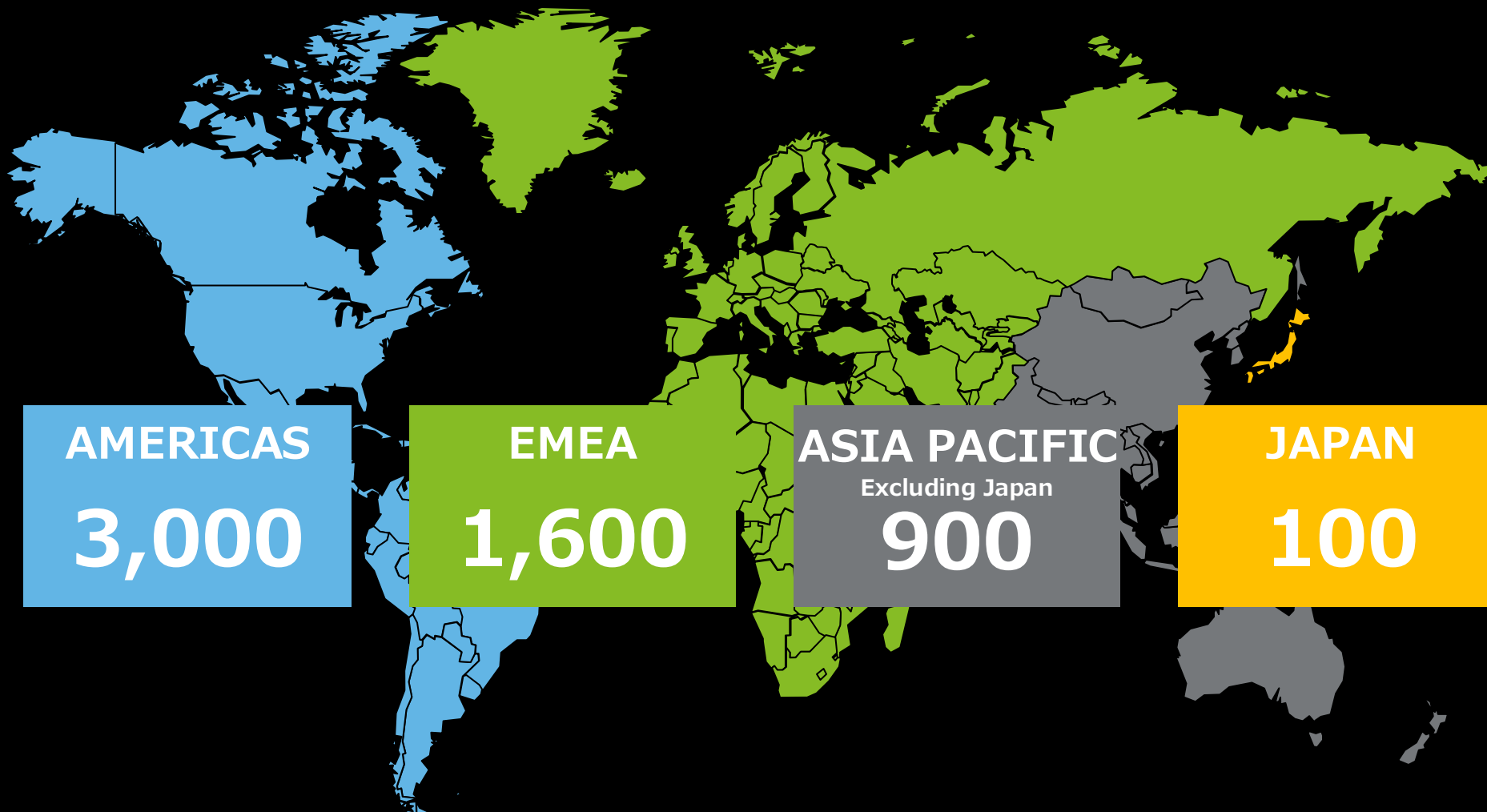
## Gartner

デロイトは、セキュリティコンサルティングサービスの業務収入およびマーケットシェアで連続して世界1位となったと発表

Top Vendors	2015 Revenue	2016 Revenue	2015 Market Share	2016 Market Share	2015-2016 Change in Share	2015-2016 Change in Revenue
<b>Deloitte</b>	<b>2,506</b>	<b>2,857</b>	<b>15.2%</b>	<b>16.0%</b>	<b>0.9%</b>	<b>14.0%</b>
EY	1,882	2,036	11.4%	11.4%	0.0%	8.2%
PwC	1,653	1,947	10.0%	10.9%	0.9%	17.8%
KPMG	1,519	1,610	9.2%	9.0%	-0.2%	6.0%
IBM	726	731	4.4%	4.1%	-0.3%	0.6%
Accenture	566	601	3.4%	3.4%	-0.1%	6.2%
Booz Allen Hamilton	472	482	2.9%	2.7%	-0.2%	2.1%
HPE*	100	388	0.6%	2.2%	1.6%	288.0%
Optiv Security	323	373	2.0%	2.1%	0.1%	15.5%
BAE Systems	254	290	1.5%	1.6%	0.1%	14.2%
Leidos	157	285	0.9%	1.6%	0.7%	82.1%
Capgemini	249	280	1.5%	1.6%	0.1%	12.6%
Wipro	207	251	1.3%	1.4%	0.2%	21.1%
BT	204	240	1.2%	1.3%	0.1%	17.5%
Atos	229	239	1.4%	1.3%	0.0%	4.4%
Corporation Service Company(CS)	177	196	1.1%	1.1%	0.0%	10.7%
Verizon	178	171	1.1%	1.0%	-0.1%	-3.6%
RSA	154	144	0.9%	0.8%	-0.1%	-6.6%

# 5,000名を超える専門家がグローバルにサービスを提供しています

サイバーセキュリティサービス専任者数（2017年10月時点）



# サイバーインテリジェンスセンター（CIC）を開所しました

**CYBER**INTELLIGENCE  
center

## サイバーインテリジェンスセンターの概要

### ■ Cyber Intelligence Center (CIC) とは

- セキュリティインテリジェンスを活用し、お客様のインフラストラクチャをサイバー攻撃から守ります
- 世界20ヶ国以上に拠点を構え、グローバル規模のサービスを提供しています

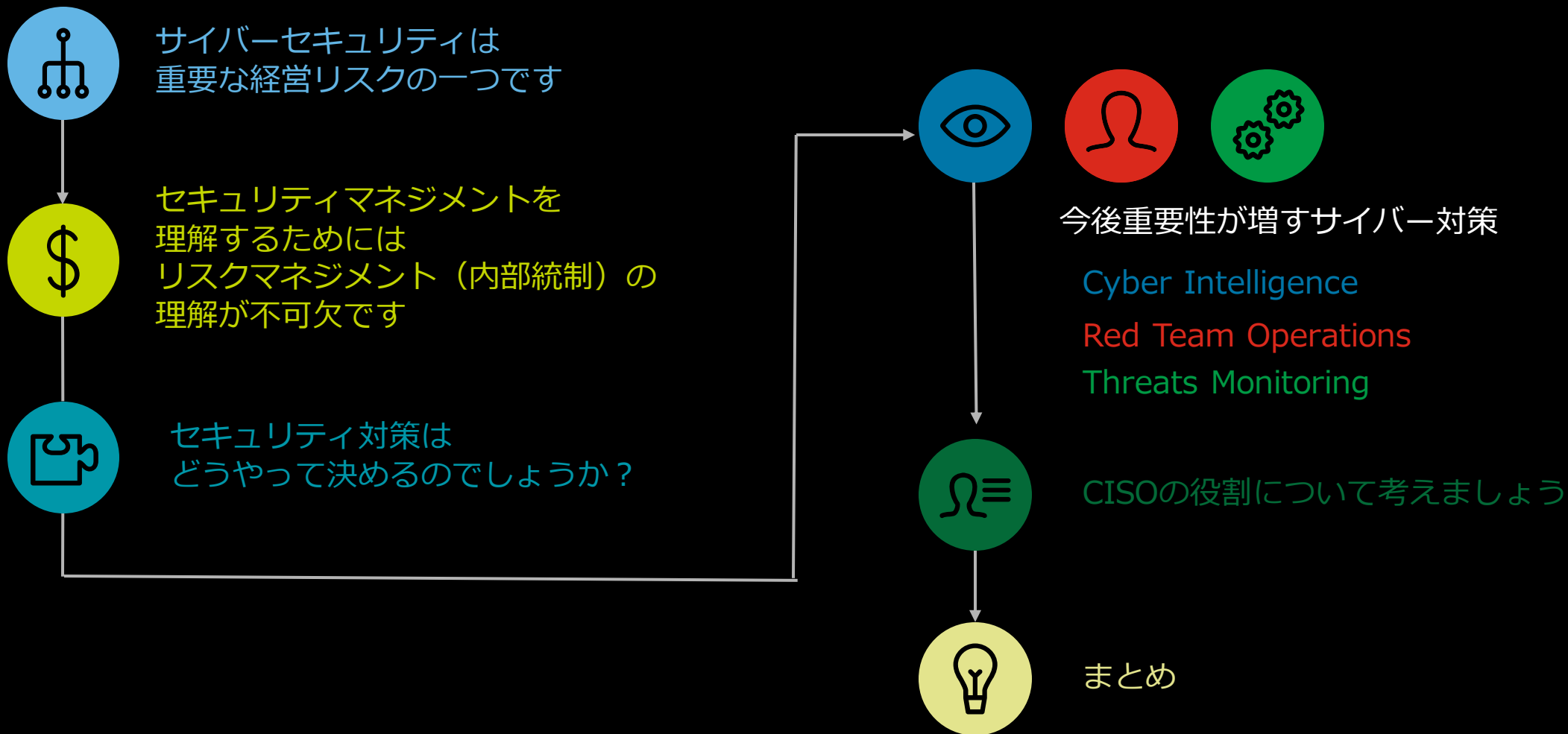
### ■ CICの特長

- 各国で収集・分析した非常に高度なサイバーインテリジェンスを提供します
- 境界デバイスだけでなく、Proxy・Active Directory・エンドポイントセキュリティ製品等も分析対象とし、お客様のインシデント・レスポンス工数を低減します

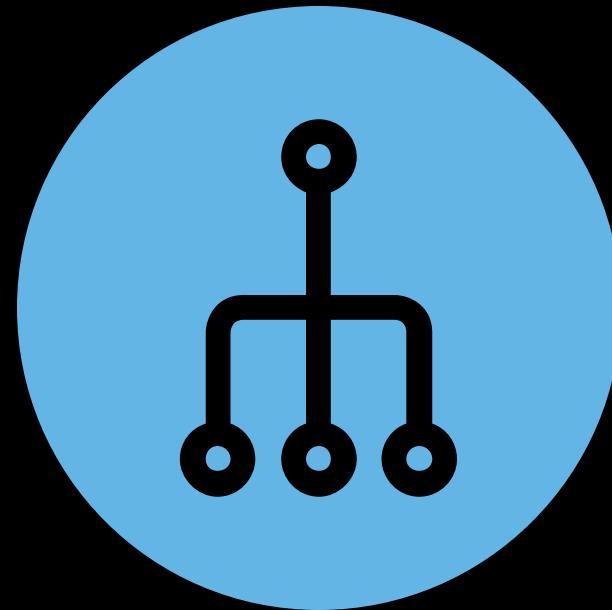


# Agenda

## 企業の危機管理担当者が把握すべきサイバーセキュリティ最前線



**サイバーセキュリティは  
重要な経営リスクの一つです**





# サイバーリスクはITの課題ではなくビジネスの課題です

## 組織を守る必要性和新しい戦略を採用する必要性のバランス



サイバー脅威から  
組織を守る



新しいビジネスモデルや  
新しい戦略を採用する

サイバーリスクはITの課題ではなく  
ビジネスの課題で——そして  
戦略的に避けられない緊急事項です。

リーダーは、まずデジタル革新に伴うチャンスとリスクについて  
絶えず理解するよう努め、  
そのうえで  
「サイバー脅威から組織を守る必要性」と、  
「デジタル技術を活用して未来の成功の基礎を築く、  
新しいビジネスモデルや新しい戦略を採用する必要性」  
とのバランスを取らなければなりません。

# 世界の経営者はサイバーセキュリティを重要な経営リスクの一つとみています

ダボス会議の「The Global Risks Report 2018」によると、世界の経営者はCyber Attackの脅威は大きいと認識されているといえます。

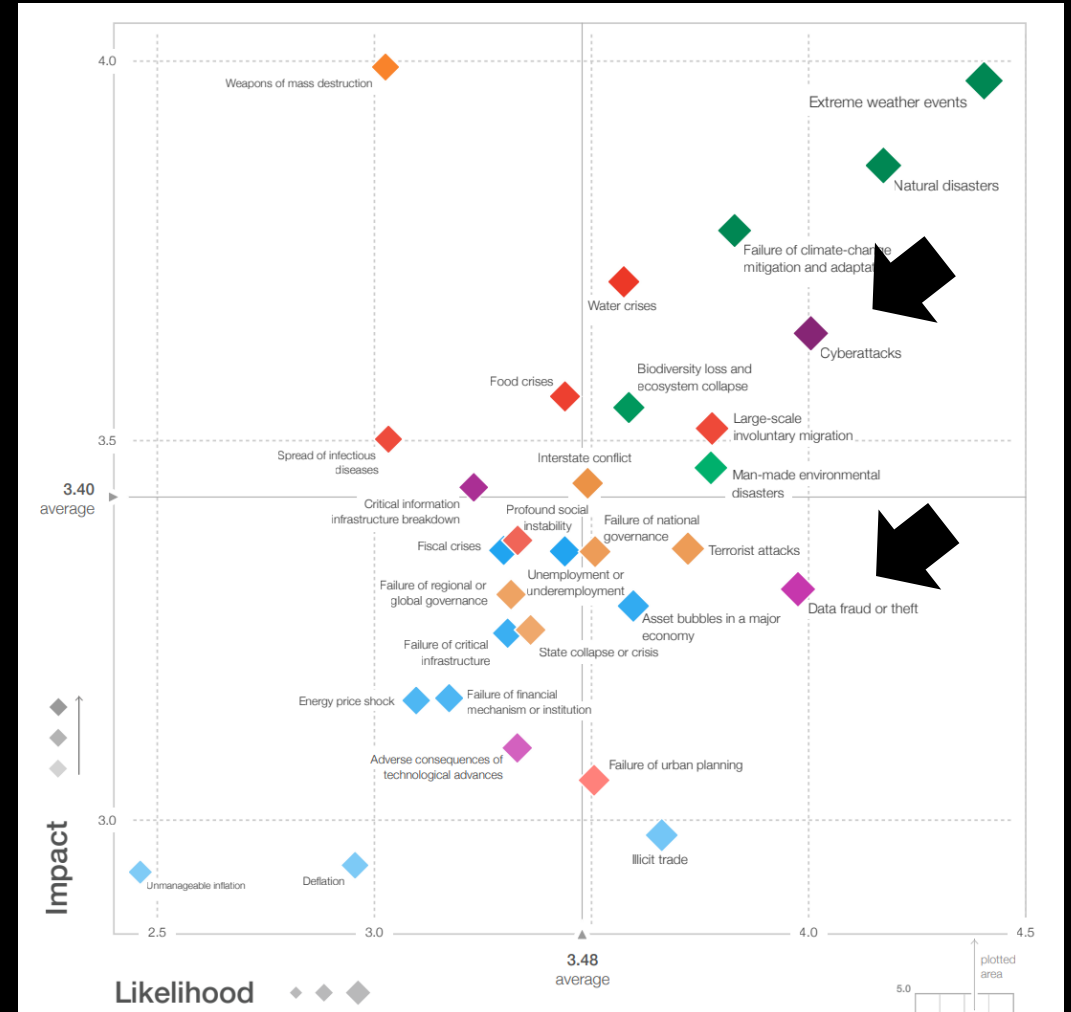
## 最も発生可能性が高いとされたリスク

- ・ 異常気象
- ・ 自然災害
- ・ **サイバー攻撃**
- ・ **データ詐欺・データ盗難**
- ・ 気候変動緩和・適応への失敗

## 最も負のインパクトが大きいとされたリスク

- ・ 大量破壊兵器
- ・ 異常気象
- ・ 自然災害
- ・ 気候変動緩和・適応への失敗
- ・ 水の危機

## The Global Risks Landscape 2018



# 経済産業省もサイバーセキュリティ経営ガイドラインを公表しています

サイバーセキュリティ経営ガイドライン

Ver 2.0

経済産業省

独立行政法人 情報処理推進機構

- 企業のITの利活用は、グローバルな競争をする上で企業として必須の条件。
- サイバー攻撃は年々高度化、巧妙化してきており、深刻な影響を引き起こす事件が発生している。
- さらには、国民の社会生活に重大な影響を及ぼす可能性のある攻撃も発生している。
- 社会に対して損害を与えてしまった場合、経営責任や法的責任が問われる可能性がある。
- セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要である。
- このように、サイバー攻撃が避けられないリスクとなっている現状において、**経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務である。**

# 「経営者が認識すべき3原則」を理解することが重要です

## 経営者が認識すべき3原則



経営者の  
リーダーシップ



ビジネス全体



利害関係者との  
コミュニケーション

	3原則	説明
(1)	経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要	経営者はリーダーシップをとってサイバー攻撃のリスクと企業への影響を考慮したサイバーセキュリティ対策を推進するとともに、企業の成長のためのセキュリティ投資を実施すべきである。
(2)	自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要	自社のサイバーセキュリティ対策にとどまらず、サプライチェーンのビジネスパートナーや委託先も含めた総合的なサイバーセキュリティ対策を実施すべきである。
(3)	平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要	平時からステークホルダー（顧客や株主など）を含めた関係者にサイバーセキュリティ対策に関する情報開示を行うことなどで信頼関係を醸成し、インシデント発生時にもコミュニケーションが円滑に進むよう備えるべきである。

経営者は、サイバーセキュリティ対策を実施する上での責任者となるCISO等に対して重要10項目を指示すべきです

## サイバーセキュリティ経営の重要10項目

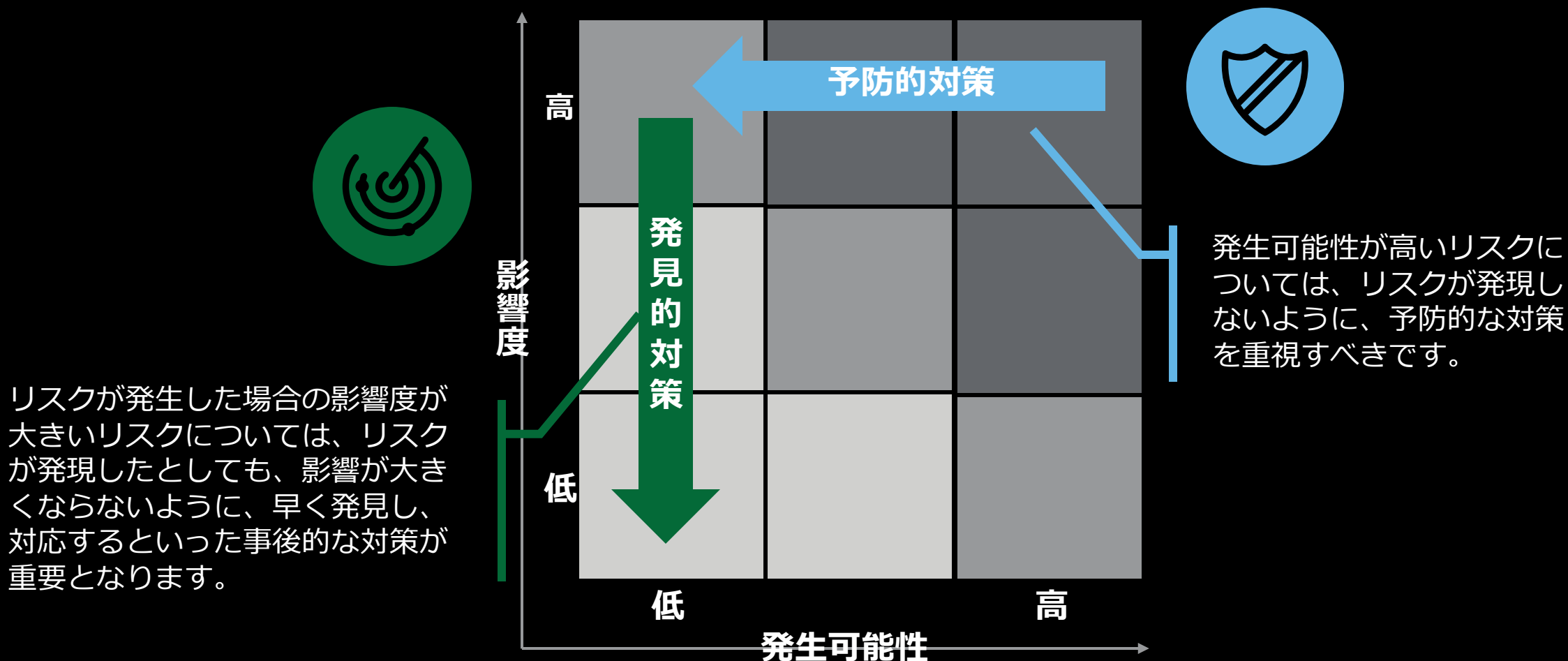
		指示	重要10項目
 <p>経営者がリーダーシップをとったセキュリティ対策の推進</p>	サイバーセキュリティリスクの管理体制構築 	1	サイバーセキュリティリスクの認識、組織全体での対応方針の策定
		2	サイバーセキュリティリスク管理体制の構築
		3	サイバーセキュリティ対策のための資源（予算、人材等）確保
	サイバーセキュリティリスクの特定と対策の実装 	4	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
		5	サイバーセキュリティリスクに対応するための仕組みの構築
		6	サイバーセキュリティ対策におけるPDCAサイクルの実施
	インシデント発生に備えた体制構築 	7	インシデント発生時の緊急対応体制の整備
		8	インシデントによる被害に備えた復旧体制の整備
サプライチェーンセキュリティ対策の推進		9	ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
ステークホルダーを含めた関係者とのコミュニケーションの推進		10	情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

セキュリティマネジメントを  
理解するためには  
リスクマネジメント（内部統制）の  
理解が不可欠です



# サイバーセキュリティは組織をとりまくリスクの一つです

リスクマネジメントの一般的な考え方を援用することで他のリスクマネジメントと一体運営ができます



# セキュリティについての最適解を芸術的に求める必要があります

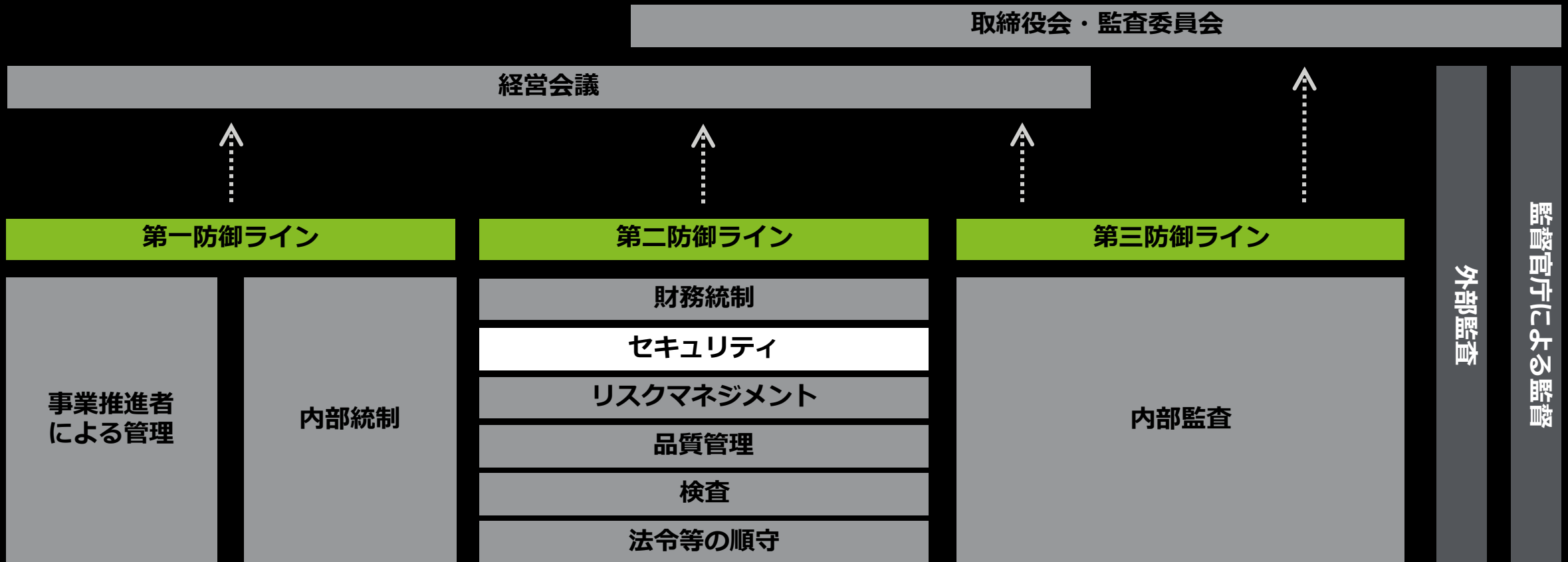
セキュリティ対策をどこまでするかに一般解はありません





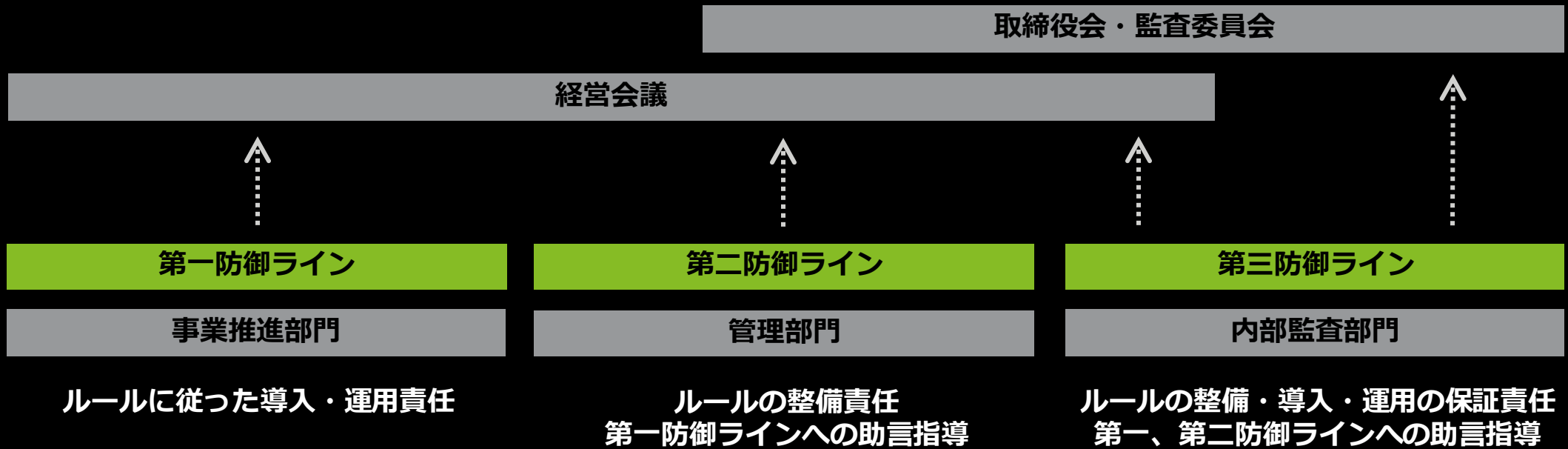
# セキュリティ対応もThe Three Lines of Defense Modelで考えるとよいでしょう

それぞれの役割を考えがえましょう



出典：THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL  
(The Institute of Internal Auditors, 2013年1月)

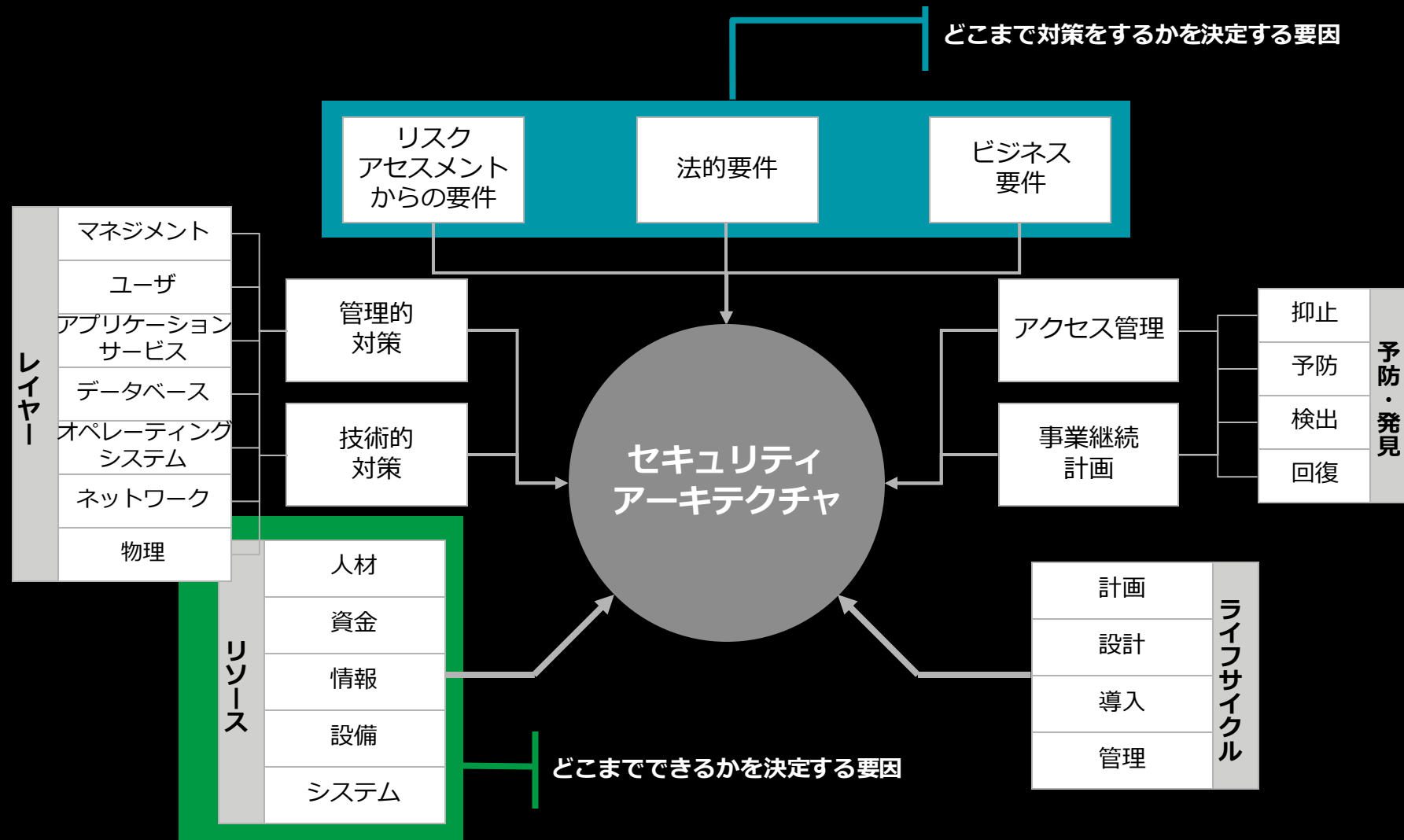
# セキュリティ対応は誰が何をすべきでしょうか？



セキュリティ対策はどうやって  
決めるのでしょうか？

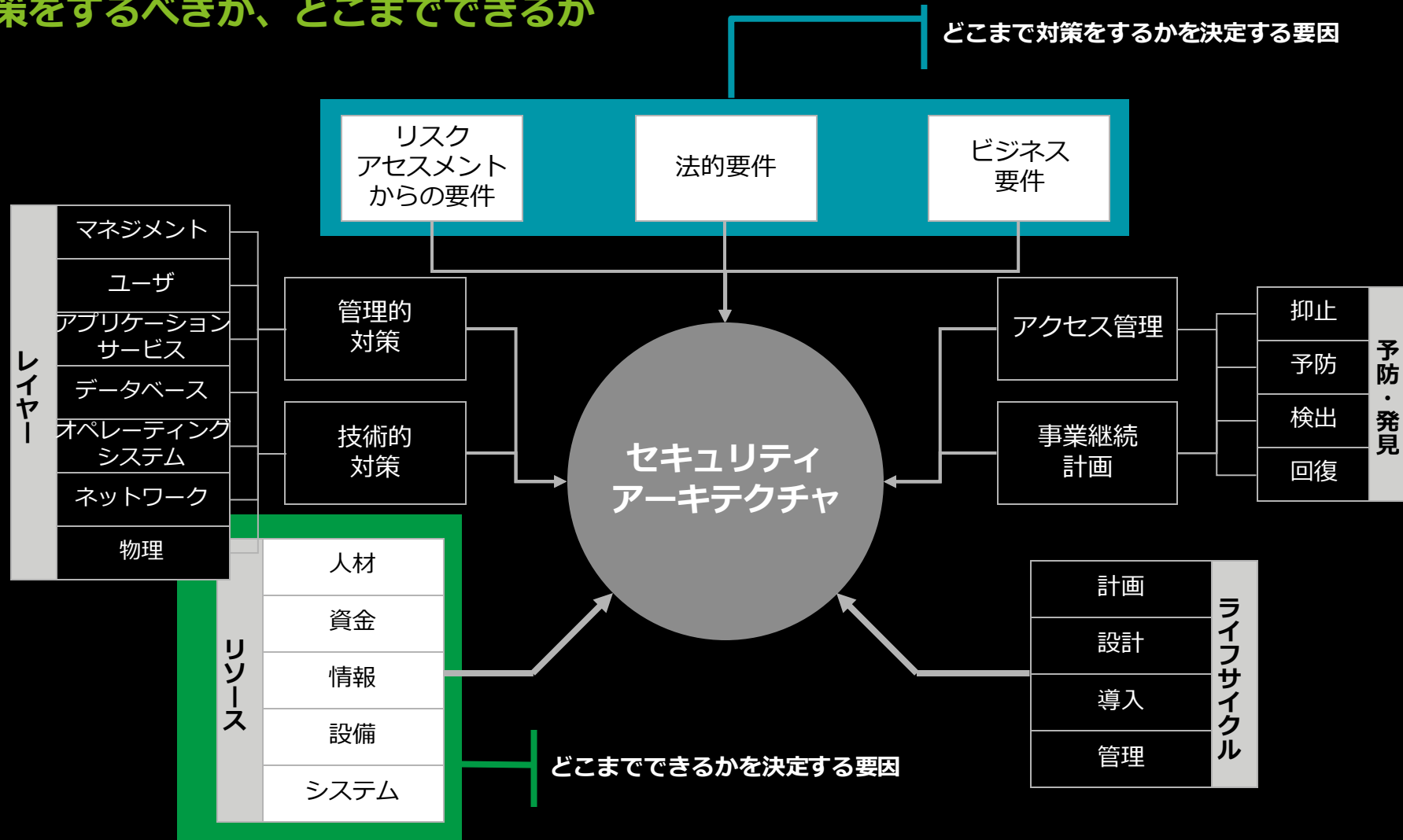


# セキュリティ対策を決める際の考慮事項



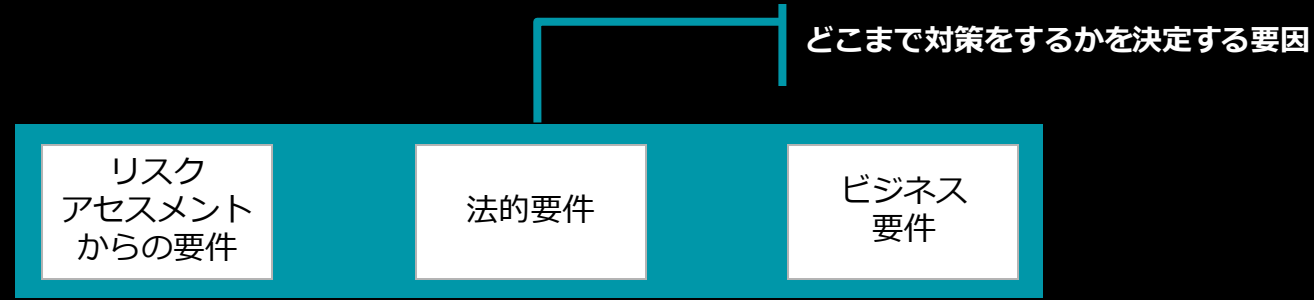
# セキュリティ対策を決める際の考慮事項

どこまで対策をするべきか、どこまでできるか



# セキュリティ対策を決める際の考慮事項

## どこまで対策をするべきか



リスクアセスメントを実施し、固有リスクー対策により軽減されたリスク＝残留リスクとし、  
残留リスク<許容リスク  
となるまでセキュリティ対策を実施する。

というのが教科書的であるが、一般的には基本的に実施すべき対策（ISO/IEC27002やNIST SP800-53等を参考にしきめることが多い）を実施し、なお不足すると考えられる場合に、追加の対策を実施することが多い。

法律やクライアントから要求されている場合等（**ビジネス要件**）には、要求された対策を実施する必要があります。

決められた対策をすべて実施すべきとは限りません。例えば、1年で廃棄するシステムのために多額の費用をかけて追加のセキュリティ対策を実施すべきではないかもしれません。

このような**例外対応**についての承認手続きを決めておくことは重要です。

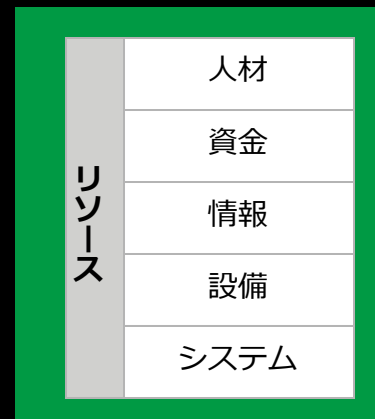
# セキュリティ対策を決める際の考慮事項

## どこまでできるか（理想通りにはできない）

どこまでセキュリティ対策をするのかについては、リスク等に応じて、セキュリティ対策を決定することはできるが、それらの対策を導入・運用するにあたっては、

- 人材
- 資金
- 情報
- 設備
- システム

等の制限があります。



どこまでできるかを決定する要因

必要があるとして決められた対策を100%実現できている組織は実際には少ないはずで

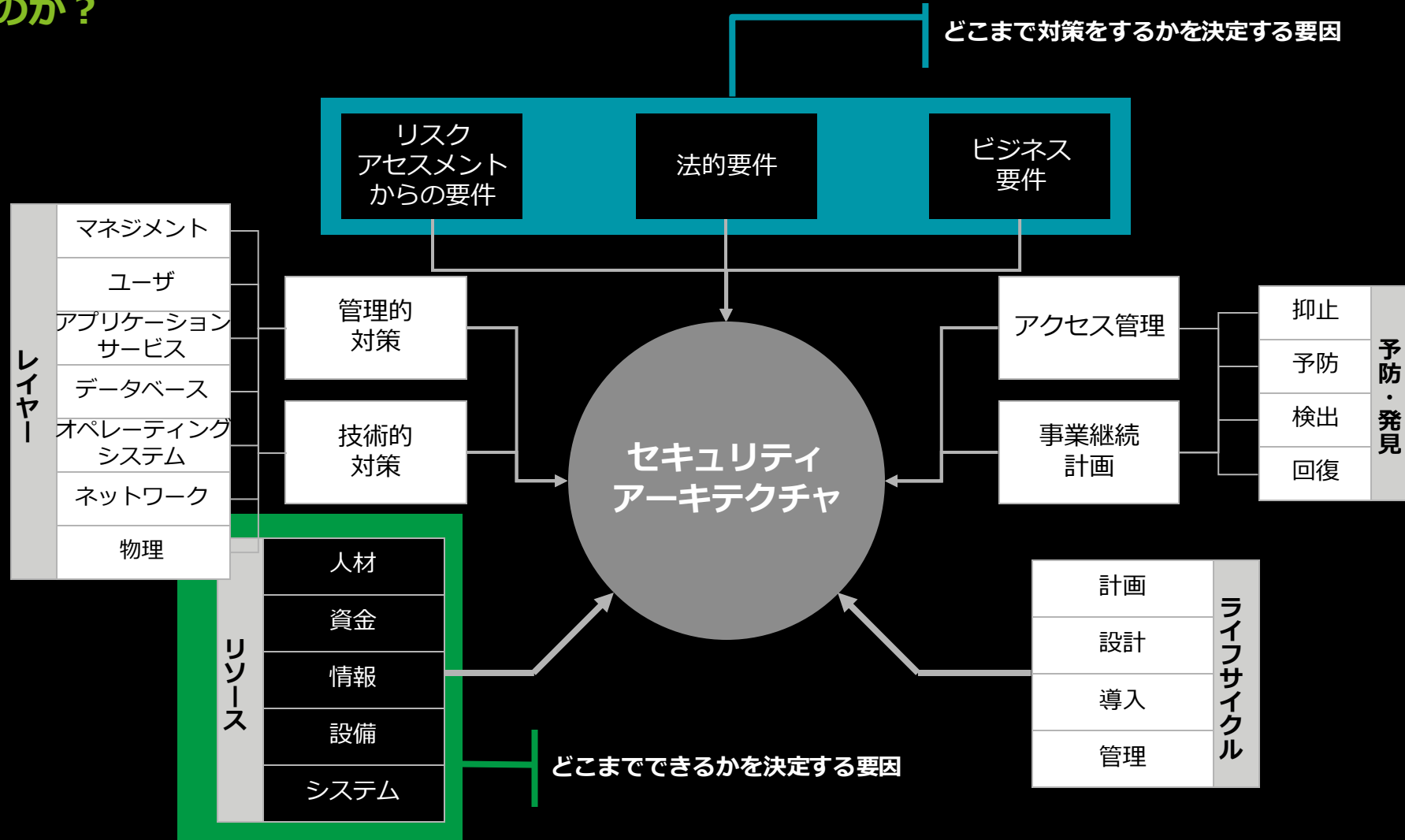
人材、資金、情報、設備、システム等のリソースによる制約があるからです。

重要なことは、守られていないことにより、どのようなリスクが残留しているかを把握し、そのリスクの発現の発見、対応といった補完的な対策をいかにうまく行うのか。

また、それでも損害が発生した場合に備えて、利害関係者とどのようなコミュニケーションをとるかを決めておくことです。

# セキュリティ対策を決める際の考慮事項

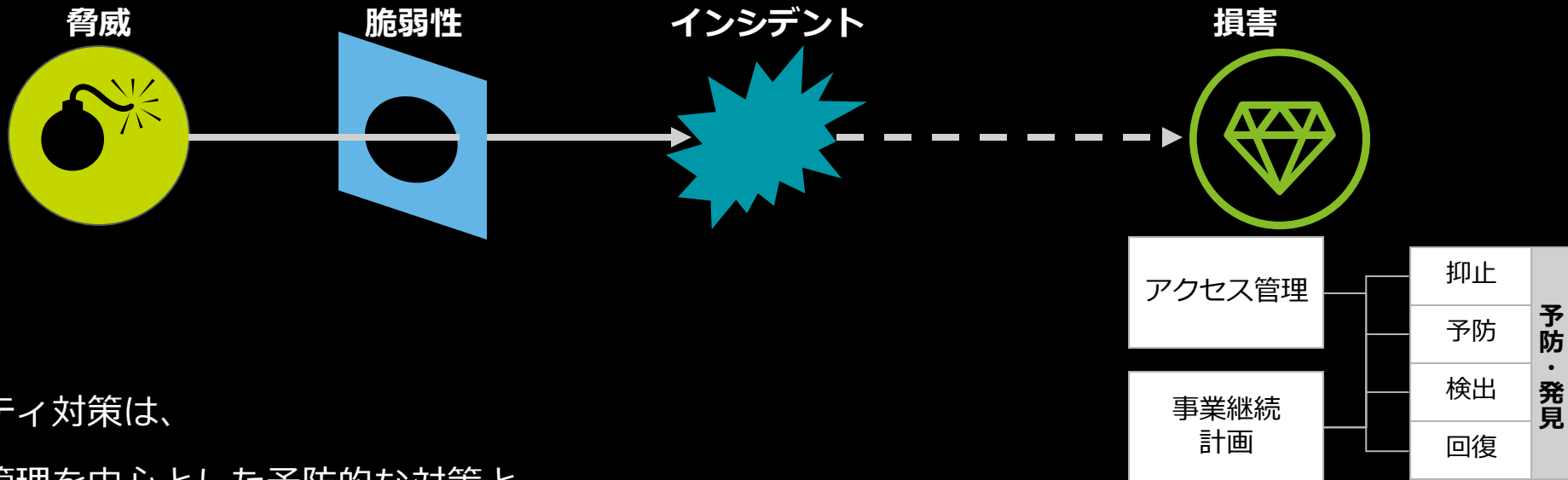
## どこで守るのか？





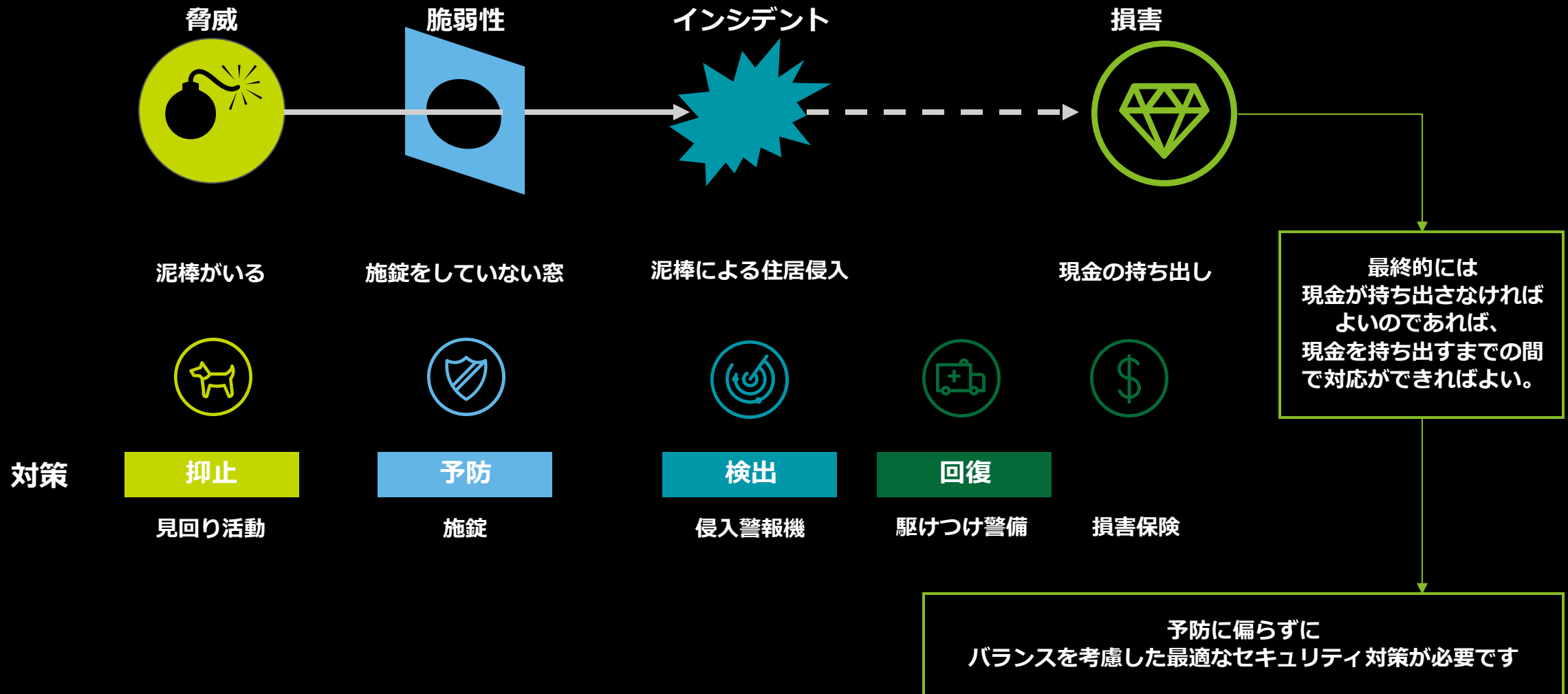
# セキュリティ対策を決める際の考慮事項

## 抑止・予防・検出・回復の観点



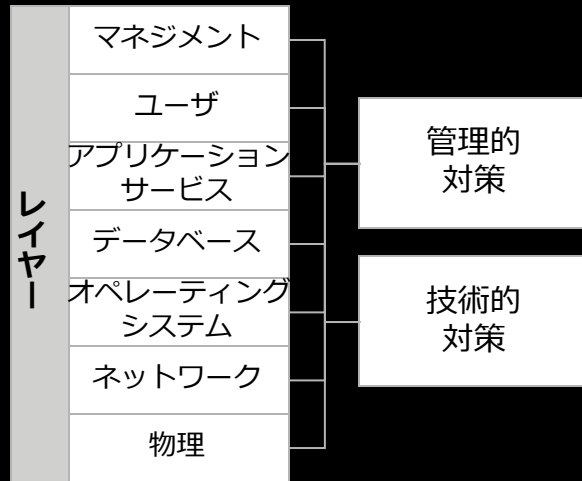
セキュリティ対策は、  
アクセス管理を中心とした予防的な対策と  
事業継続計画を意識した発見的な対策に大別される。  
後者は危機管理ともつながる対策です。

# 身近なことにたとえてみましょう



# セキュリティ対策を決める際の考慮事項

## 組織的対策、人的対策、物理的対策、技術的対策



個人情報保護法のガイドラインの安全管理措置は、

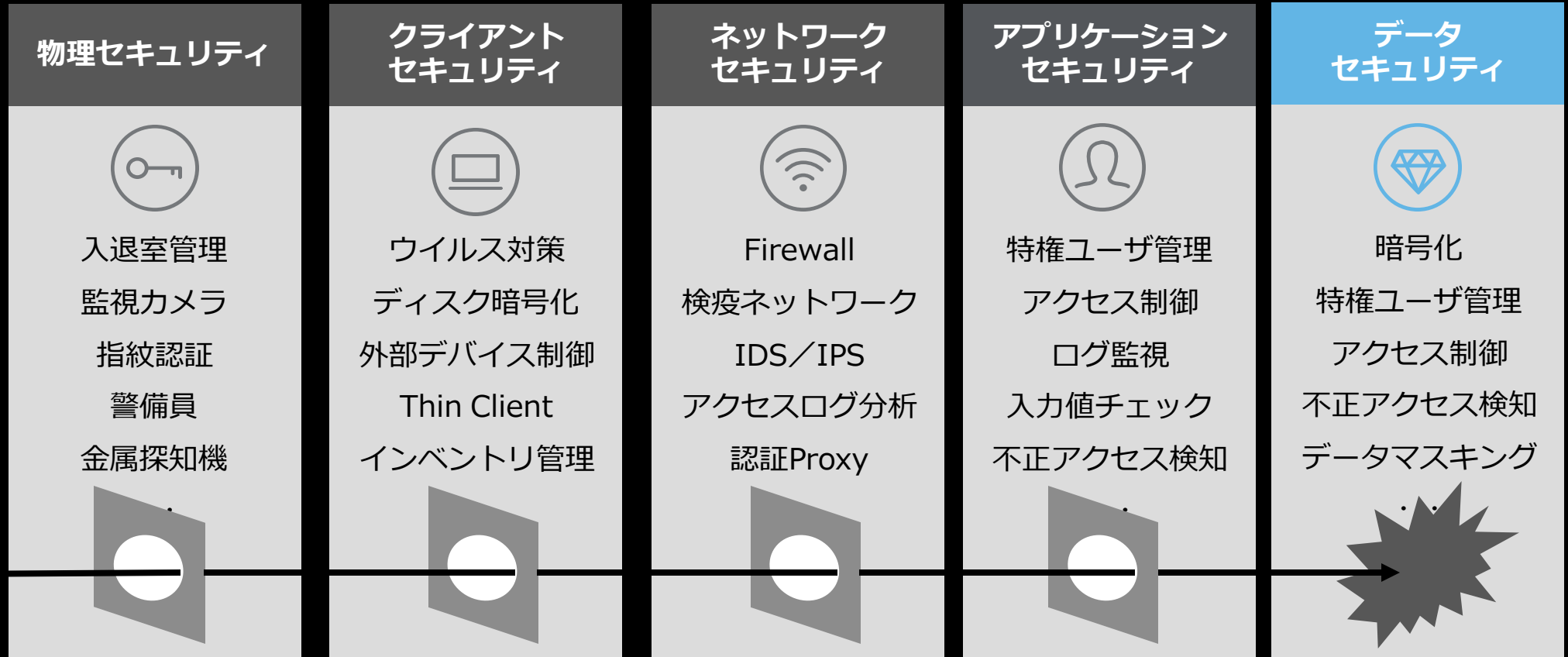
- 組織的対策
- 人的対策
- 物理的対策
- 技術的対策

と分けられているが、

その発想はこのレイヤー的な発想です。

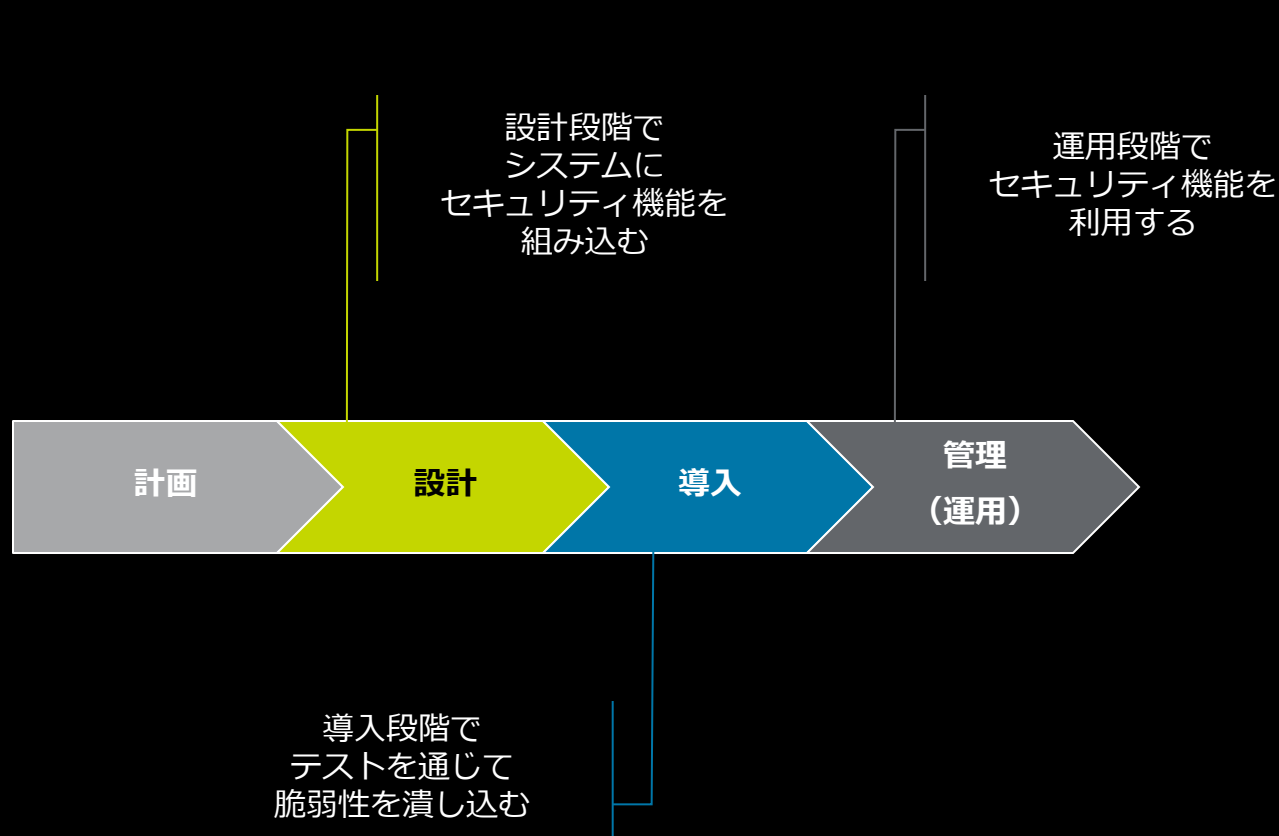
# セキュリティ対策は多層的に考える必要があります

## 情報漏えいを考えた場合



# セキュリティ対策を決める際の考慮事項

## ライフサイクル全体でセキュリティ対策を考える

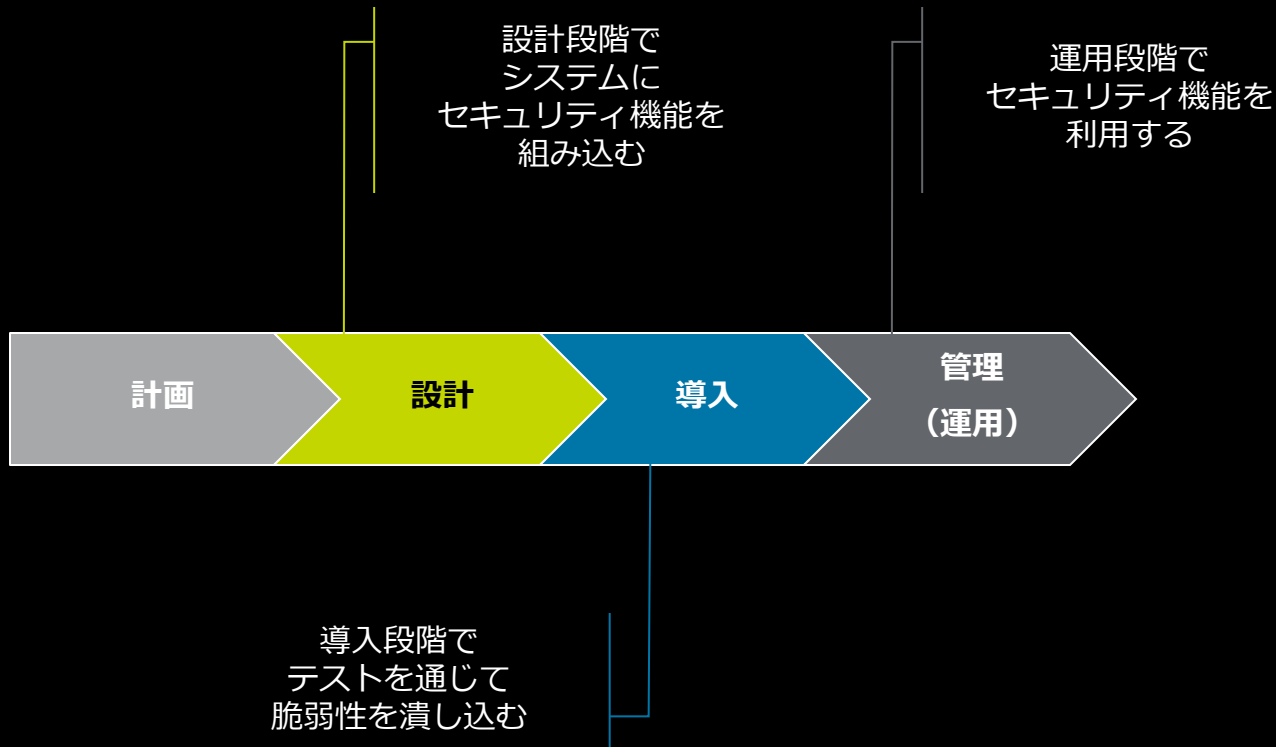


製品、プラントや工場設備の情報システムなど、運用時におけるセキュリティ対策の導入がむづかしいシステム等では、運用を開始するまでの設計段階でセキュリティ対策を実装することが重要である。

計画	ライフサイクル
設計	
導入	
管理	

# できる限り上流でリスクを減らすことが重要となります

## IoT/ICS時代はSecurity by Designの重要性が増します



**ライフサイクル全体で考える必要があります。**

運用に頼りがちであるが、上流で対策ができるのであれば、コストは下がります。

また工場や設備等の場合は、

連続稼働が前提で、仕様変更がオペレーションの品質に影響が及ぶ可能性が高いため、

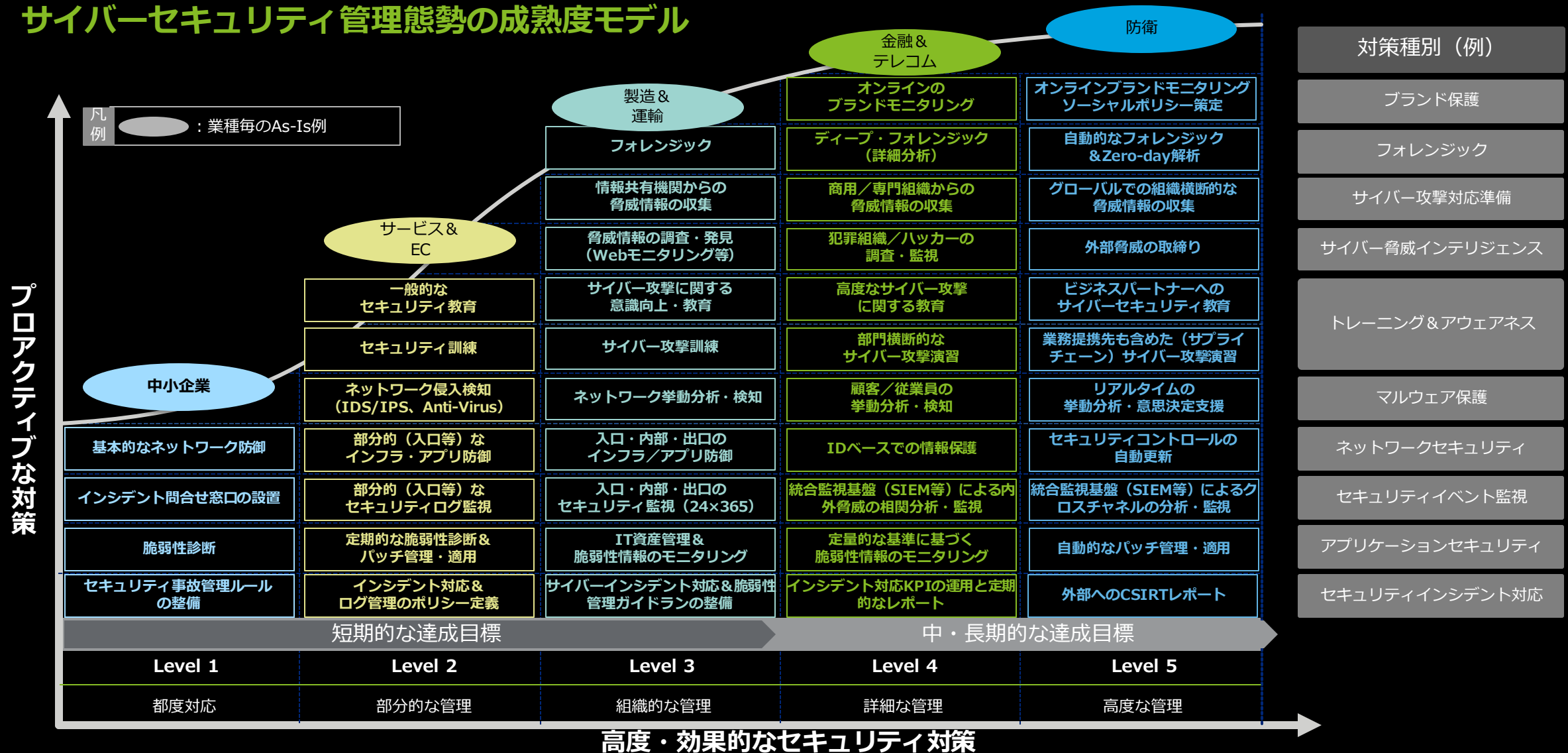
設計段階で必要なセキュリティ機能を実装し、

導入段階でテストを通じて脆弱性を潰し込み、

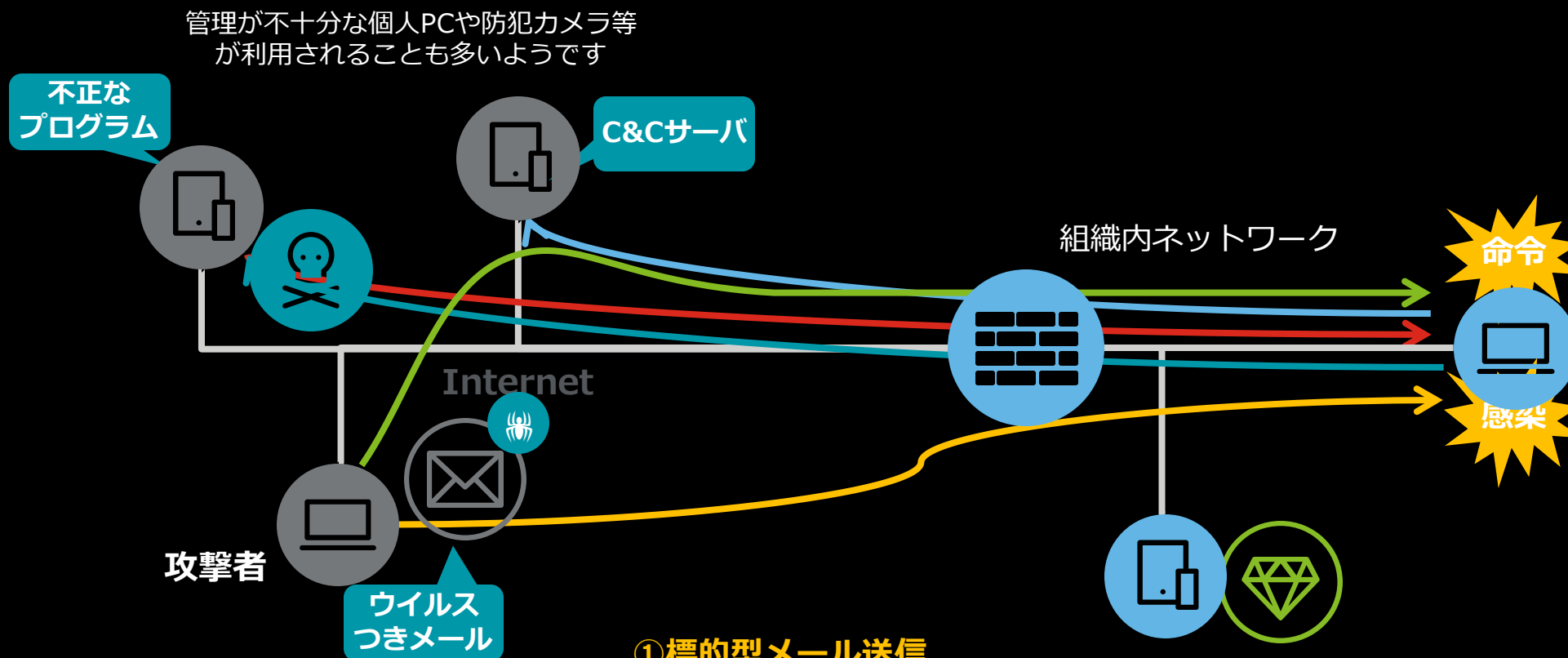
運用段階までに、セキュアなシステムを作り込むことの重要性が高まってきています。

# 【ご参考】デロイトのサイバーセキュリティ管理態勢 成熟度モデル 組織の特性に応じて目指すべきレベル (To-Be) を決定することが重要です

## サイバーセキュリティ管理態勢の成熟度モデル



# 標的型攻撃による攻撃手法を理解しましょう（ただし、一例です）



- ① 標的型メール送信
- ② 組織内で感染し更なる不正プログラムを要求
- ③ 不正プログラムをダウンロード
- ④ C&Cサーバ等攻撃者の用意した外部サーバと接続
- ⑤ 外部サーバ経由で指令が送信される
- ⑥ 組織内の機密情報等が漏えいする



# 空白の時間があります（１）

## 侵害時の痕跡

The screenshot shows the Windows Registry Viewer window. The left pane displays the tree structure of the registry, with 'Session Manager' expanded to show 'AppCompatCache'. The right pane shows the details for the 'AppCompatCache' value, which is a REG\_BINARY type with a value of 'EE 0F DC BA EA 03 00 00 78 00 00 0...'. Below the registry details, a list of recent file operations is visible, with one entry highlighted in red:

Name	Type	Value
(Default)	REG_SZ	(value not set)
AppCompatCache	REG_BINARY	EE 0F DC BA EA 03 00 00 78 00 00 0...

2015/07/15 に Rdws.exe ( Emdivi ) が実行

File Name	Date	Time	Source
¥[893C40C2-C02D-4807-876D-F4DD8078930F]¥GoogleUpdateSetup.exe	2015/05/16	02:59:52	+9: ¥??¥C¥Users¥...¥AppData¥Local¥Google¥Update
¥[893C40C2-C02D-4807-876D-F4DD8078930F]¥GoogleUpdate.exe	2015/07/15	19:46:56	+9: ¥??¥C¥Users¥...¥AppData¥Local¥Temp¥Low¥Rdws.exe
¥chrome.exe	2015/07/15	04:06:23	+9: ¥??¥C¥Users¥...¥AppData¥Local¥Temp¥CR_E64F7.tmp

2015/12/16 15:53:05.1 +9 242 KB SYSTEM¥ControlSet001¥Control¥Session Manager¥AppCompatCache ¥Windows¥System32¥config¥system

## 空白の時間があります（２）

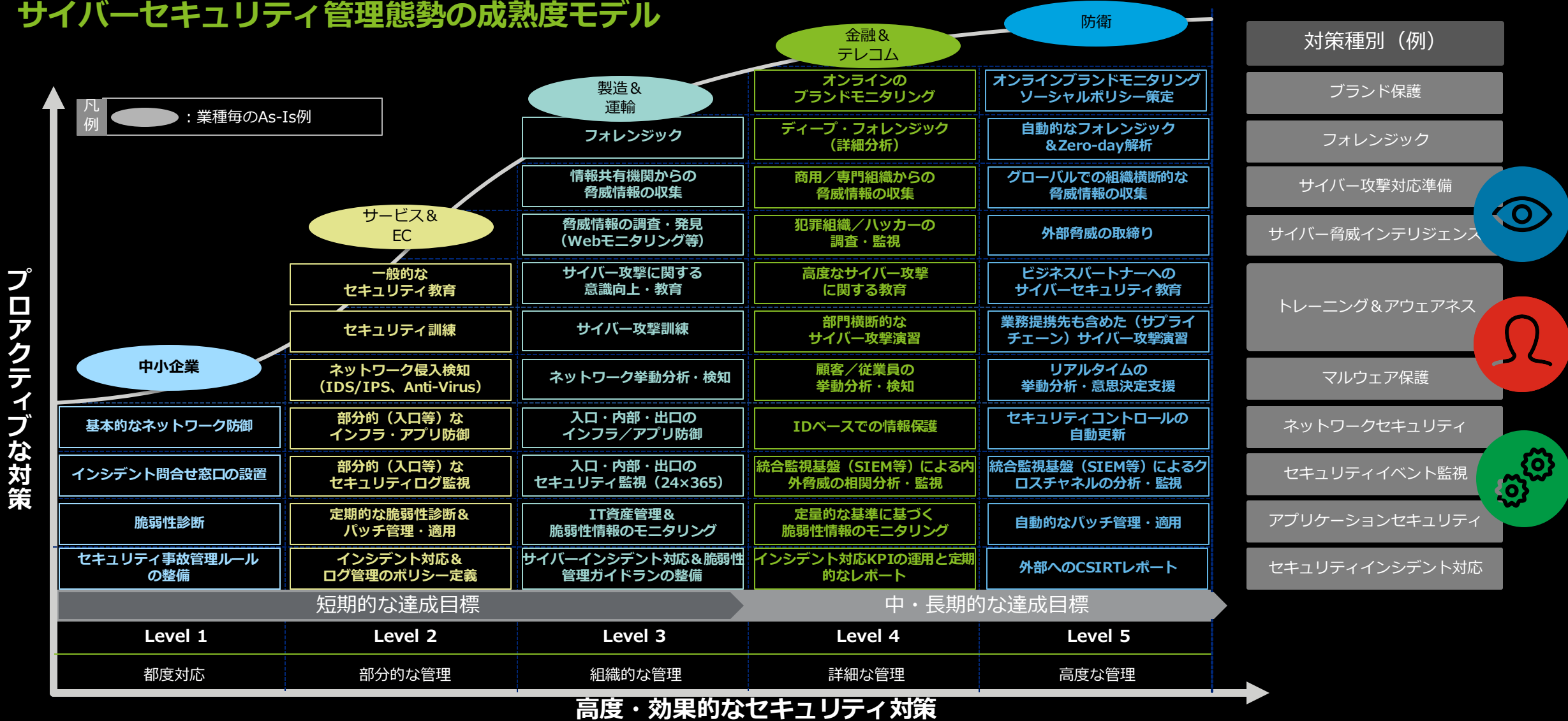
### ウイルス対策ソフト対応時

```
OnAccessScanLog.txt ×
3319 2015/07/22 22:09:53 EXTRA.DATの検出シグネチャ数 = なし
3320 2015/07/22 22:09:53 EXTRA.DATの検出シグネチャ名 = なし
3321
3322 2015/07/23 22:26:09 エンジンのバージョン = 5700.7163
3323 2015/07/23 22:26:09 AntiVirus DATバージョン = 7870.0
3324 2015/07/23 22:26:09 EXTRA.DATの検出シグネチャ数 = なし
3325 2015/07/23 22:26:09 EXTRA.DATの検出シグネチャ名 = なし
3326 2015/07/24 12:58:09 削除 NT AUTHORITY\SYSTEM C:\Windows\system32\wbem\wmiprvse.exe
C:\Users\ \AppData\Local\Temp\Low\Rdws.exe-Artemis!2345AE36972F (トロイの木馬)
3327
3328 2015/07/25 4:53:53 エンジンのバージョン = 5700.7163
3329 2015/07/25 4:53:53 AntiVirus DATバージョン = 7871.0
3330 2015/07/25 4:53:53 EXTRA.DATの検出シグネチャ数 = なし
3331 2015/07/25 4:53:53 EXTRA.DATの検出シグネチャ名 = なし
3332
3333 2015/07/26 0:49:52 エンジンのバージョン = 5700.7163
3334 2015/07/26 0:49:52 AntiVirus DATバージョン = 7872.0
3335 2015/07/26 0:49:52 EXTRA.DATの検出シグネチャ数 = なし
3336 2015/07/26 0:49:52 EXTRA.DATの検出シグネチャ名 = なし
3337
```

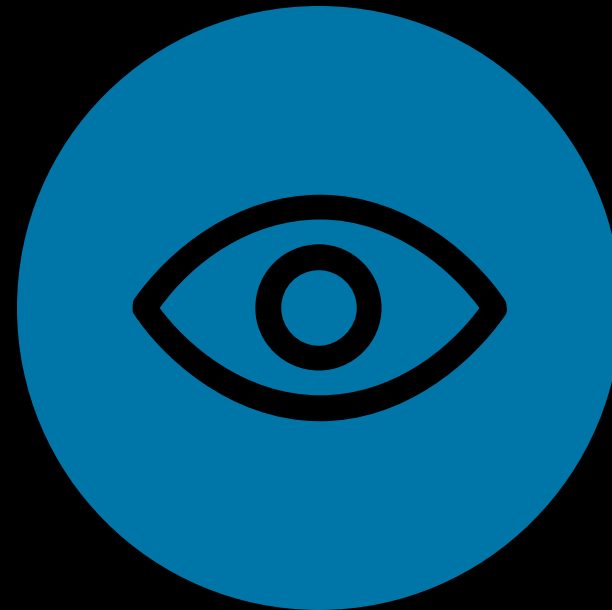
2015/07/24 にウイルス対策ソフトが対応

# 今後重要性がますますサイバー対策例を簡単に説明していきます

## サイバーセキュリティ管理態勢の成熟度モデル



# 今後重要性が増すサイバー対策（1） Cyber Intelligence



## 「予兆をつかむ」ことが必要です

嵐が来る前に、どのくらいの強さの嵐が、いつ来るのかわかれば被害を抑えることができます。



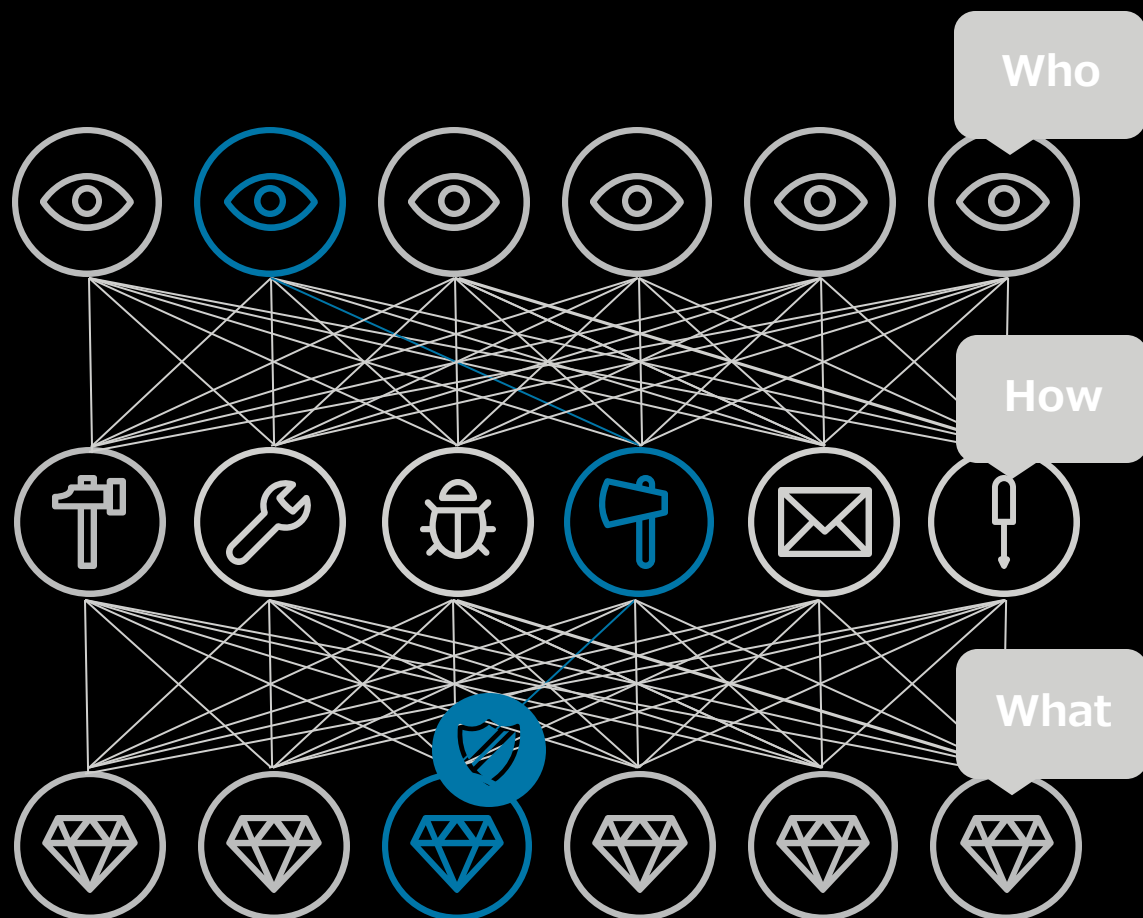
**Intelligence**

**Threat Actor Analysis**

**Threat Hunting**

# インテリジェンスなくしてどうして戦えますか？

## 誰がどうやって何を狙っているのかを知ろう



金融機関、政府機関、防衛産業、重要インフラ事業者、知財が重要な製造業等でサイバーインテリジェンスの導入が進んでいます。

限られた経営資源（人員・予算・設備）を使って全てのシステムにおける、全ての脅威に対応することはできません。

したがってサイバーセキュリティに関する対策や、インシデントの検出・対応を効率的に実施するためには、事前に攻撃者の目的・対象組織・傾向・主な攻撃手法等に関する情報を入手し、戦略的な意思決定を行う必要があります。

インフォメーションをインテリジェンス化することにより意思決定を迅速かつ適切に行えるようになります。

# 意思決定に役立つサイバーインテリジェンスが必要です

## インフォメーションからインテリジェンスへ

### インフォメーション（生の情報）

- 評価や分析が行われていない「生」の情報
- 信頼性の低いものや不完全なものが混在
- クライアントが意思決定にそのまま役立てるのは困難

### 情報処理・分析・生成

### インテリジェンス（高度な分析の結果）

- インフォメーションを処理し、クライアントの意思決定に役立つ形にした情報
- 一定以上の信頼性を保持
- クライアントによる活用が容易



利用者の  
利用目的に合わせて  
情報を分析し  
活用できる形にします






複数ソースによる  
確認による  
一定以上の  
信頼性のある情報



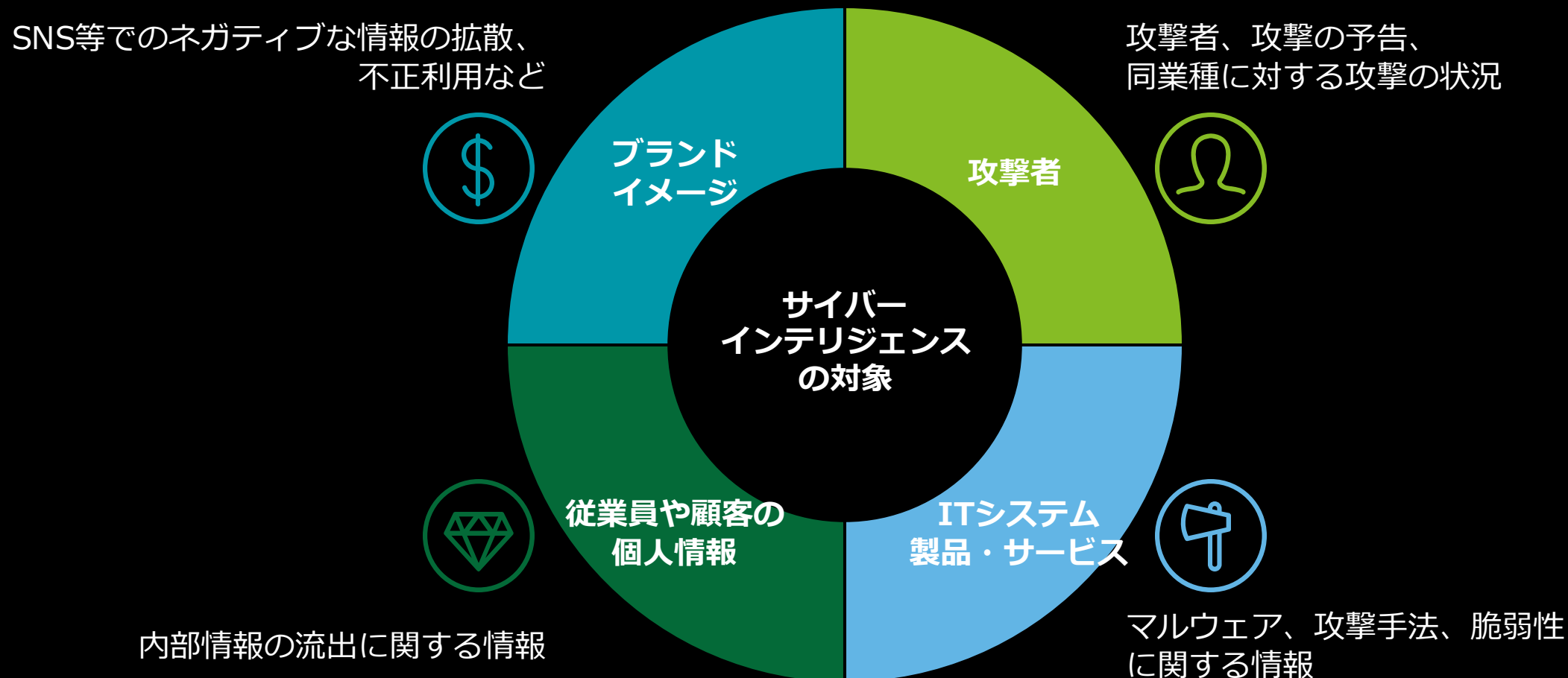
# インテリジェンスは階層が存在しそれぞれに特性があります

## インテリジェンスの階層区分

階層区分	利用者	インテリジェンスの内容
 <b>戦略的 インテリジェンス</b>	<b>経営層</b>	<b>セキュリティ施策の前提となるリスク評価に大きく影響する情報</b> <ul style="list-style-type: none"><li>■ 新しいタイプの脅威の出現</li><li>■ 攻撃技術の急速な進展など</li></ul>
 <b>作戦的 インテリジェンス</b>	<b>マネジャー層</b>	<b>自組織への攻撃の可能性を予見し、被害防止に役立つ情報</b> <ul style="list-style-type: none"><li>■ ITシステムや製品・サービスに影響するマルウェアや攻撃手法の動向</li><li>■ 同業他社に対する攻撃の手口</li><li>■ 自社を標的としている攻撃グループの動向</li></ul>
 <b>戦術的 インテリジェンス</b>	<b>スタッフ層</b>	<b>リスクの発見・評価に役立つ具体的な情報</b> <ul style="list-style-type: none"><li>■ マルウェアの通信先や不正なWebサイトのURLやIPアドレス</li><li>■ 自社・自組織における影響度が分析された脆弱性情報</li></ul>

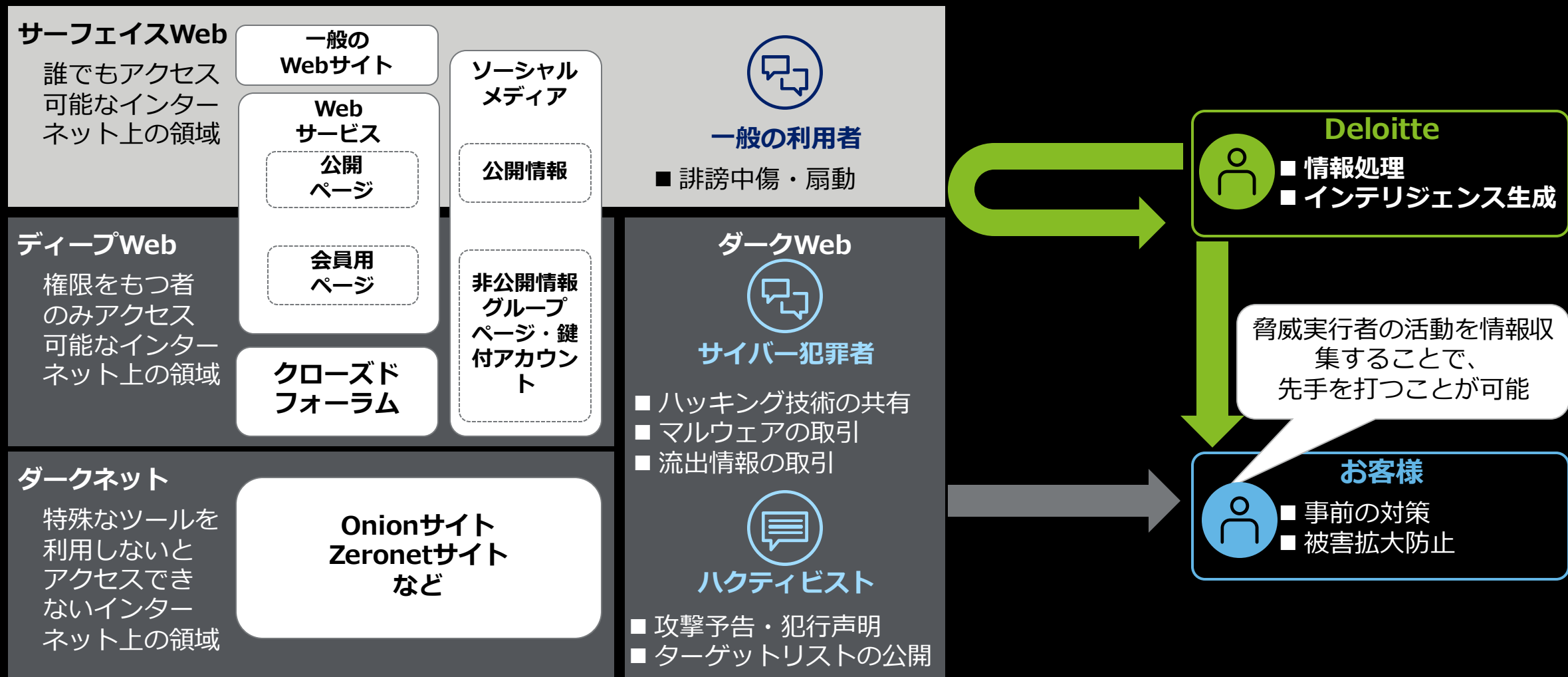


# サイバーインテリジェンスには主に4つの対象があります



# 【参考】特定のツールが必要なWeb等のダークWebの情報も必要かもしれません

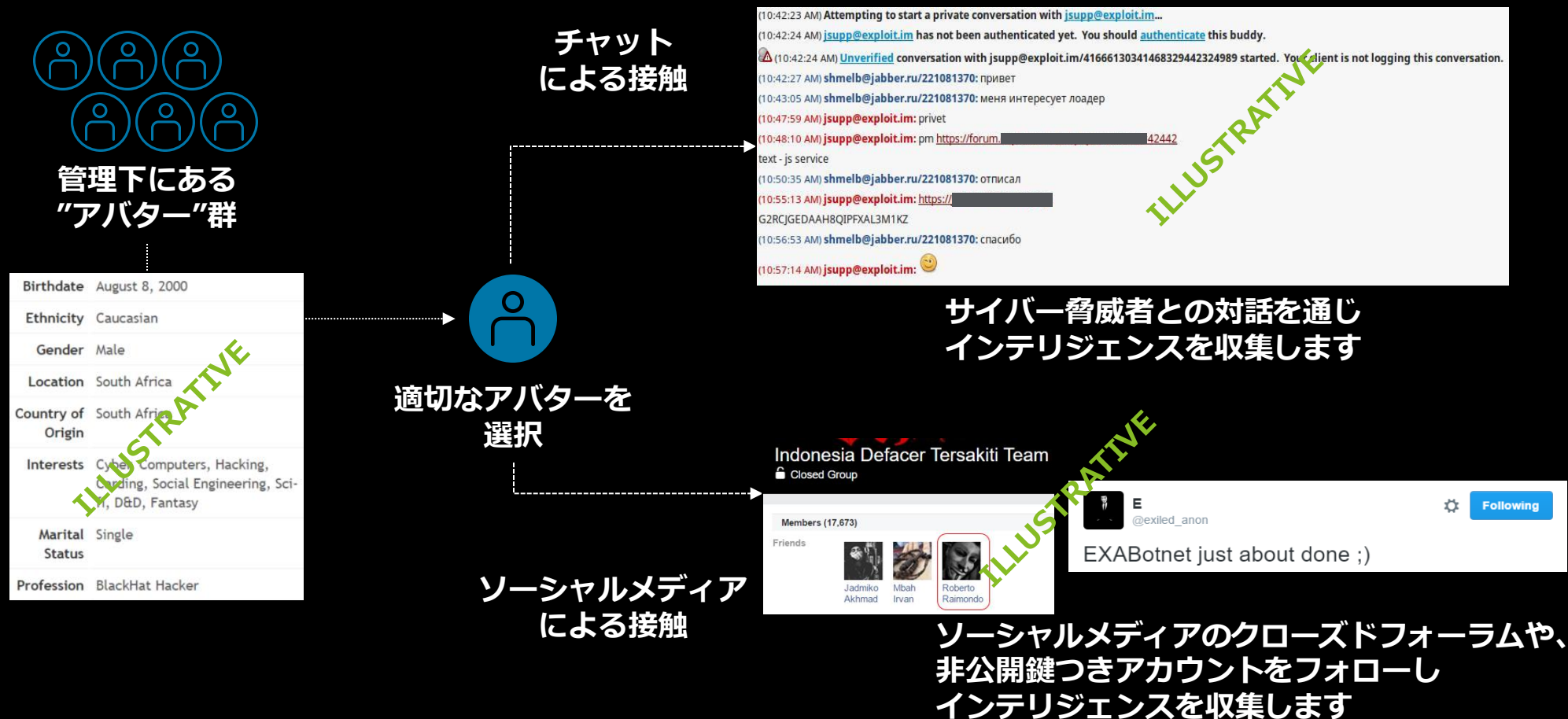
## インテリジェンス提供のソースとなるインターネット領域区分



# 【参考】アバターを用いたヒューミントによる高度なインテリジェンス

## 情報収集手法のイメージ

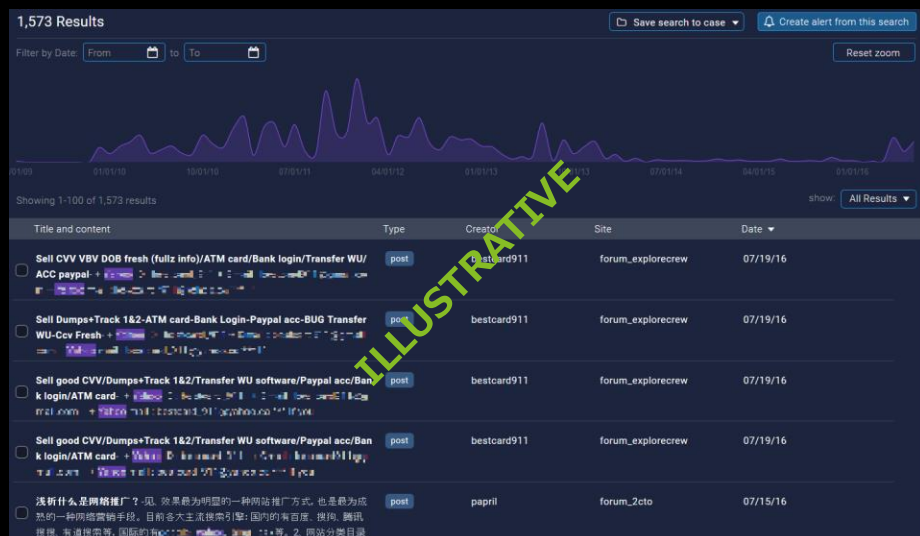
### ■プロファイリングに基づき作成された“アバター”（仮想人格）の活用



# 【参考】 ツールを併用したSNS、ダークWebからの情報収集、分析

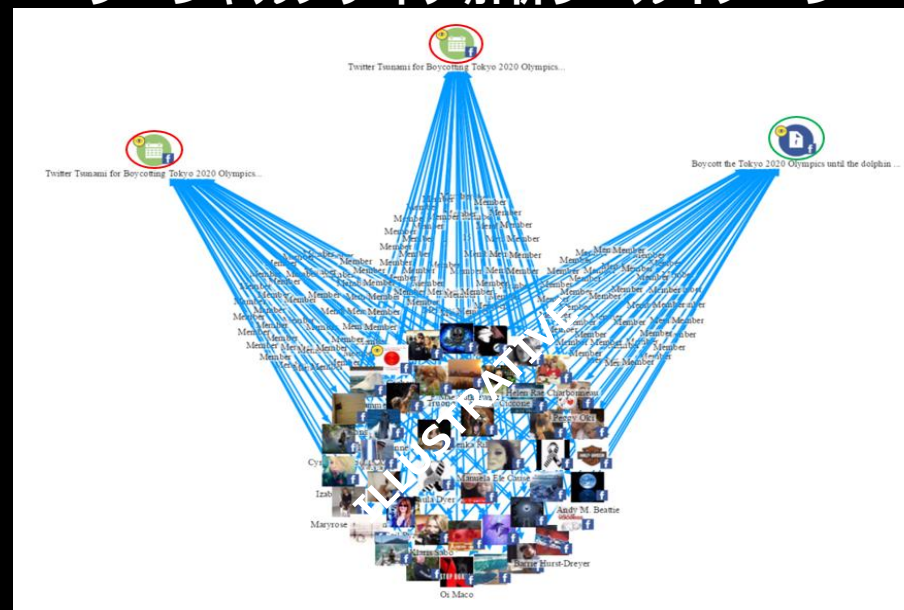
## 情報収集手法のイメージ

### ■ 情報収集ツールイメージ



- 通常のインターネット検索ではヒットしないダークネットやディープウェブを自動巡回し、情報を収集
  - 収集した情報に対し、検索、キーワードによるアラート設定が可能
- 闇取引における販売者や情報発信者の動向を日時別にモニターすることで、販売者、情報発信者のプロファイリングを行うことが可能

### ■ ソーシャルメディア解析ツールイメージ



- インターネット上に作成したアバターを用い、メンバーを限定しているソーシャルメディアのフォーラムに潜入
- 潜入後、解析ツールを用いてフォーラム参加メンバー間のリンク関係やリスクの高いフォーラムに参加しているメンバーを抽出
- 特定されたアカウントの継続的監視・分析

# 今後重要性が増すサイバー対策 (2)

## Red Team Operations



# 攻撃者の視点から防御の穴を把握する



出所：米国空軍 <https://www.flickr.com/photos/39513508@N06/29470349646/>

攻撃者が次々と新しい手法を使って、攻撃を変えてきています。

防御者の視点だけでなく、**攻撃者の視点**から防御の穴、対応力の不備を見つけることが重要です。

94%

94%のクライアントに侵入できました。

70%

70%のクライアントは、攻撃を受けたことの発見や対応ができませんでした。

1day

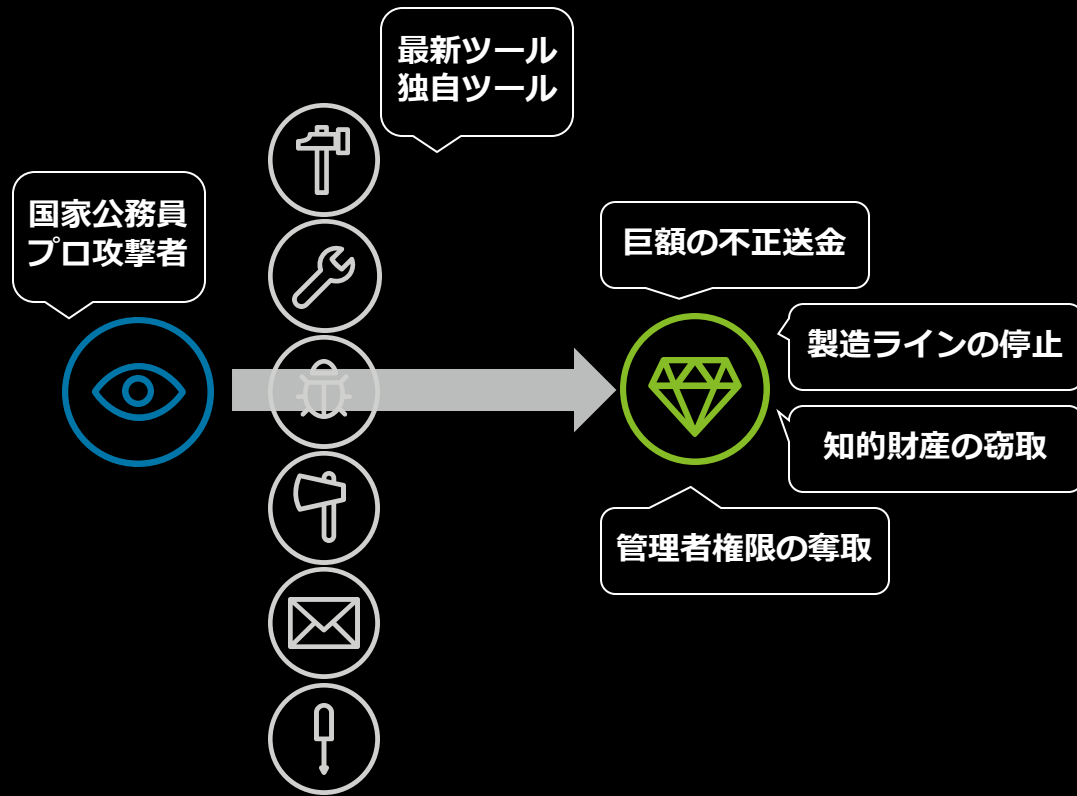
偵察フェーズから、入り口となるデバイス上の権限を奪取し、クライアントのネットワークに最初にアクセスするまでの所要時間は平均して1日でした。

6days

偵察のフェーズを終え、攻撃目標を攻略するまでの所要時間は、平均して6日間でした。

# Red Team Operationsのサービスとは何か？ なぜ必要か

## 本気の攻撃者が本気で狙いにくる



現実的なシナリオに基づいたインシデントのシミュレーションによって、サイバー攻撃への対応（予防・発見）力を評価するセキュリティテストの手法です。

組織のあらゆる要素をスコープに入れ、シナリオに基づくアプローチを行うことから、従来の「脆弱性テスト」よりも実践的な評価が可能です。

組織のサイバーセキュリティの実力および課題を可視化することにより、サイバー攻撃への対応力高度化を促進します

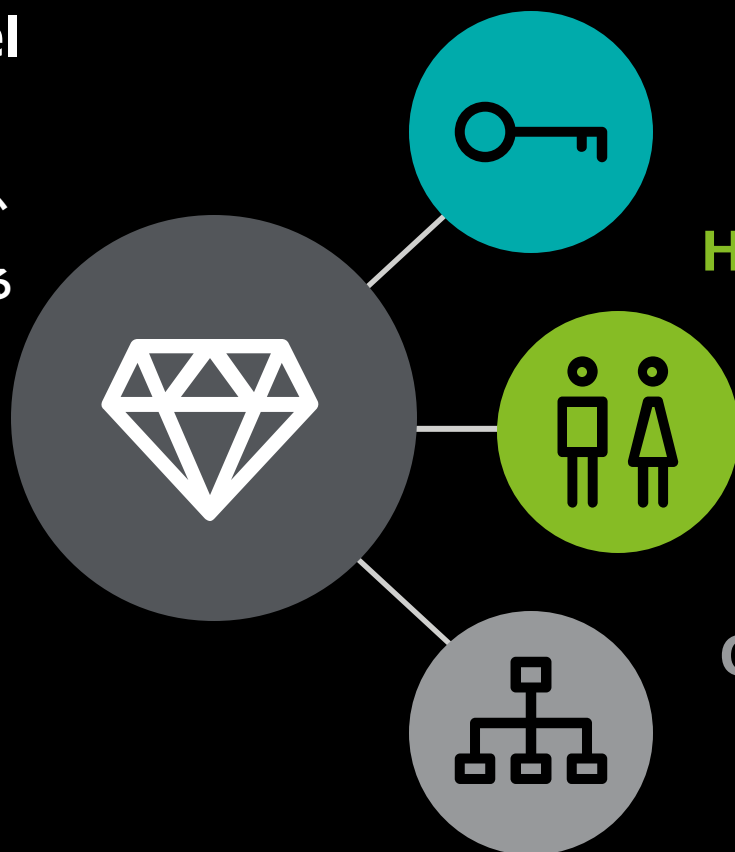


# 実際の攻撃手法に則り、サイバー攻撃耐性を評価します

## Red Team Operationsの概要

### Crown Jewel (攻撃目標)

情報窃取、不正取引、  
システム停止等の  
攻撃目標を設定する



### Physical

執務室に物理的に侵入し、不正機器の設置や、紙・電子媒体の取得を試みる

- ・ 社内LANへ不正アクセスポイントやネットワークスニファの設置、観葉植物等への監視カメラ設置 等

### Human

従業員を通じて、認証情報の取得や、端末へのテスト用マルウェアの感染を試みる

- ・ 不正テストサイトへの誘導、電話やメールによる誘導 等

### Cyber

外部ネットワークから内部ネットワークへ侵入する

- ・ 脆弱性を利用した攻撃、パスワード攻撃 等

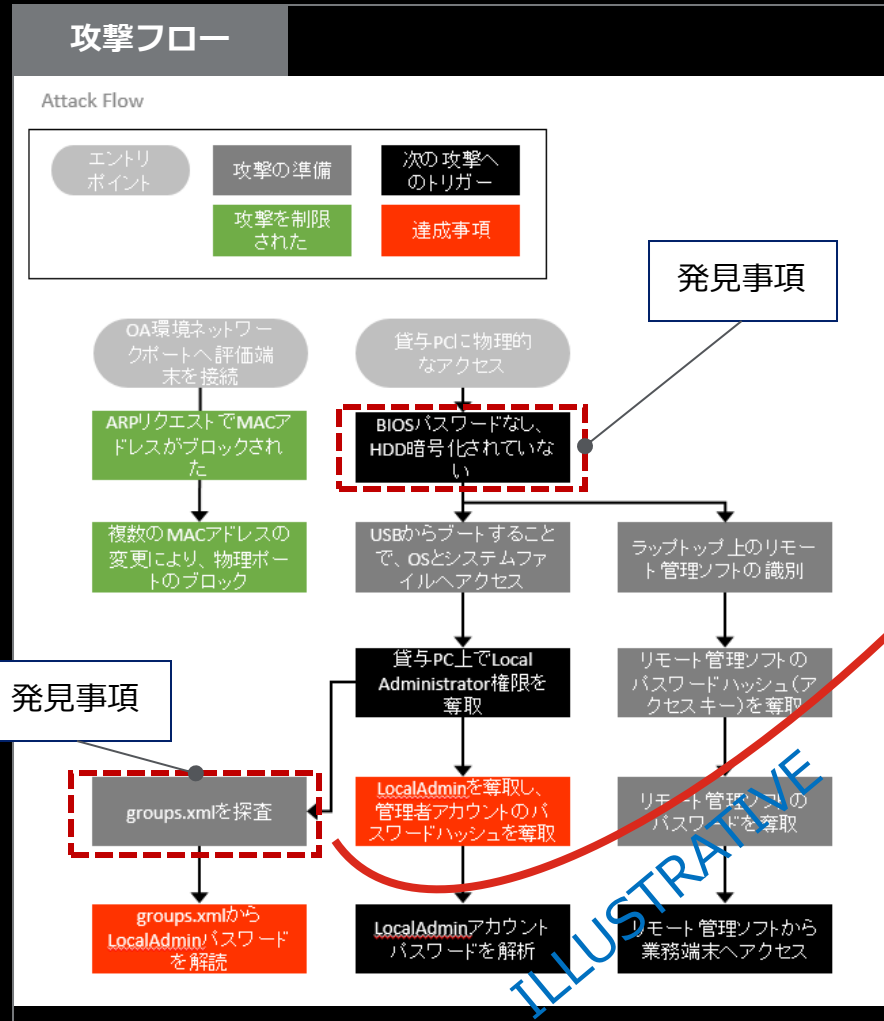
内部ネットワークへ侵入後、Crown Jewelの達成を試みる

- ・ 脆弱性を利用した権限昇格等によるシステムの停止
- ・ アクセス権限設定不備の利用による重要情報の窃取 等

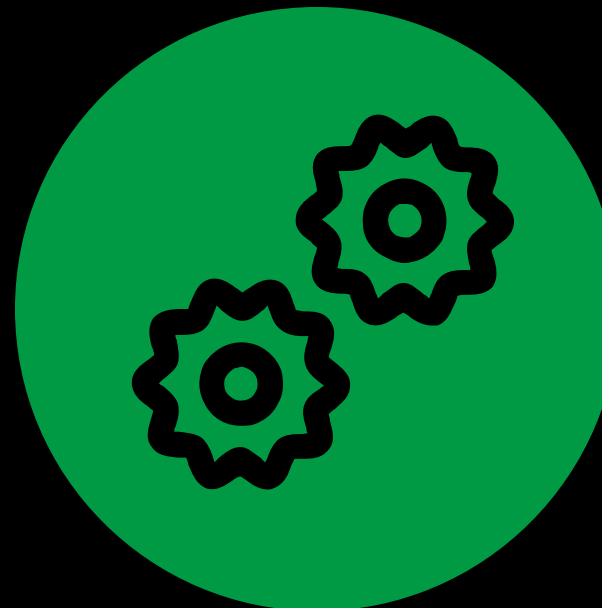


# 攻撃フローに基づき結果を分析することで対策の実効性向上につながります

## 評価結果 (イメージ)



## 今後重要性が増すサイバー対策 (3) Threats Monitoring



# 起きている状況を把握することが重要です

Radarがなければ、指令室で敵からの攻撃を把握することはできません。

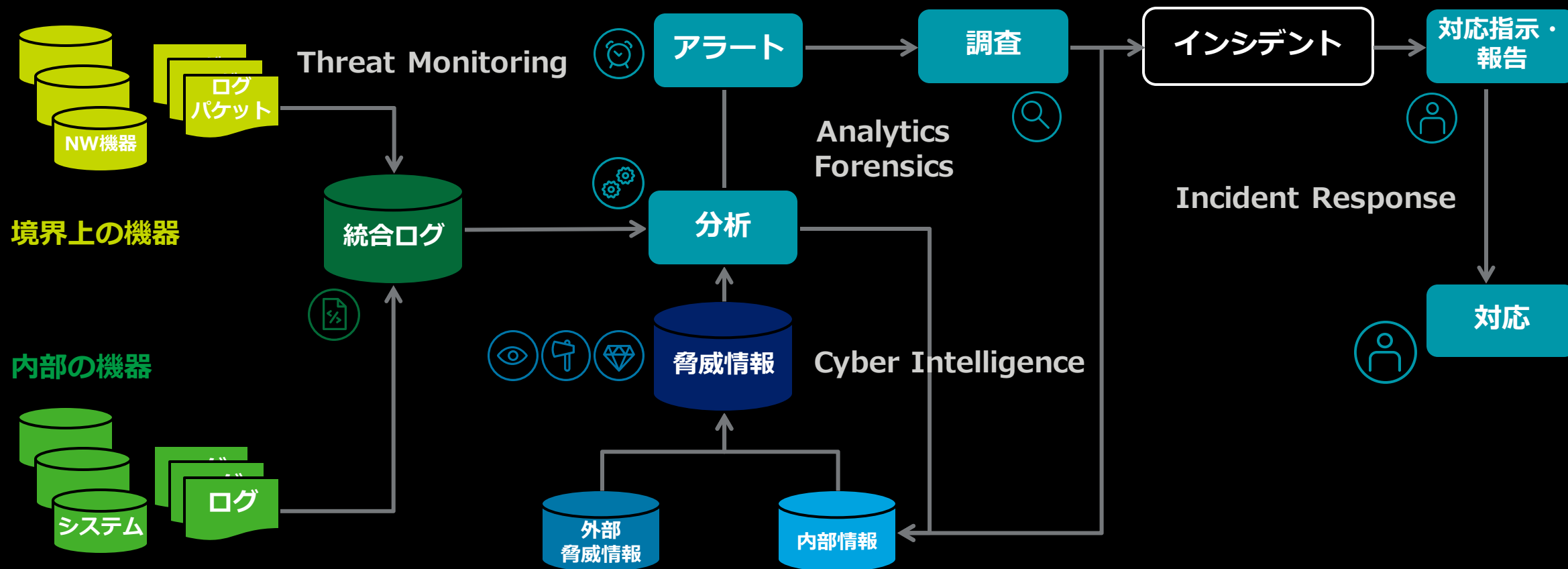


インターネットとの境界にあるファイアーウォール（FW）や侵入検知・防御システム（IPS/IDS）FWの監視は最低限必要です。

しかし、いったん侵入され内部に入られてしまえば、内部の行動を監視しなければ、被害を防止することはできません。

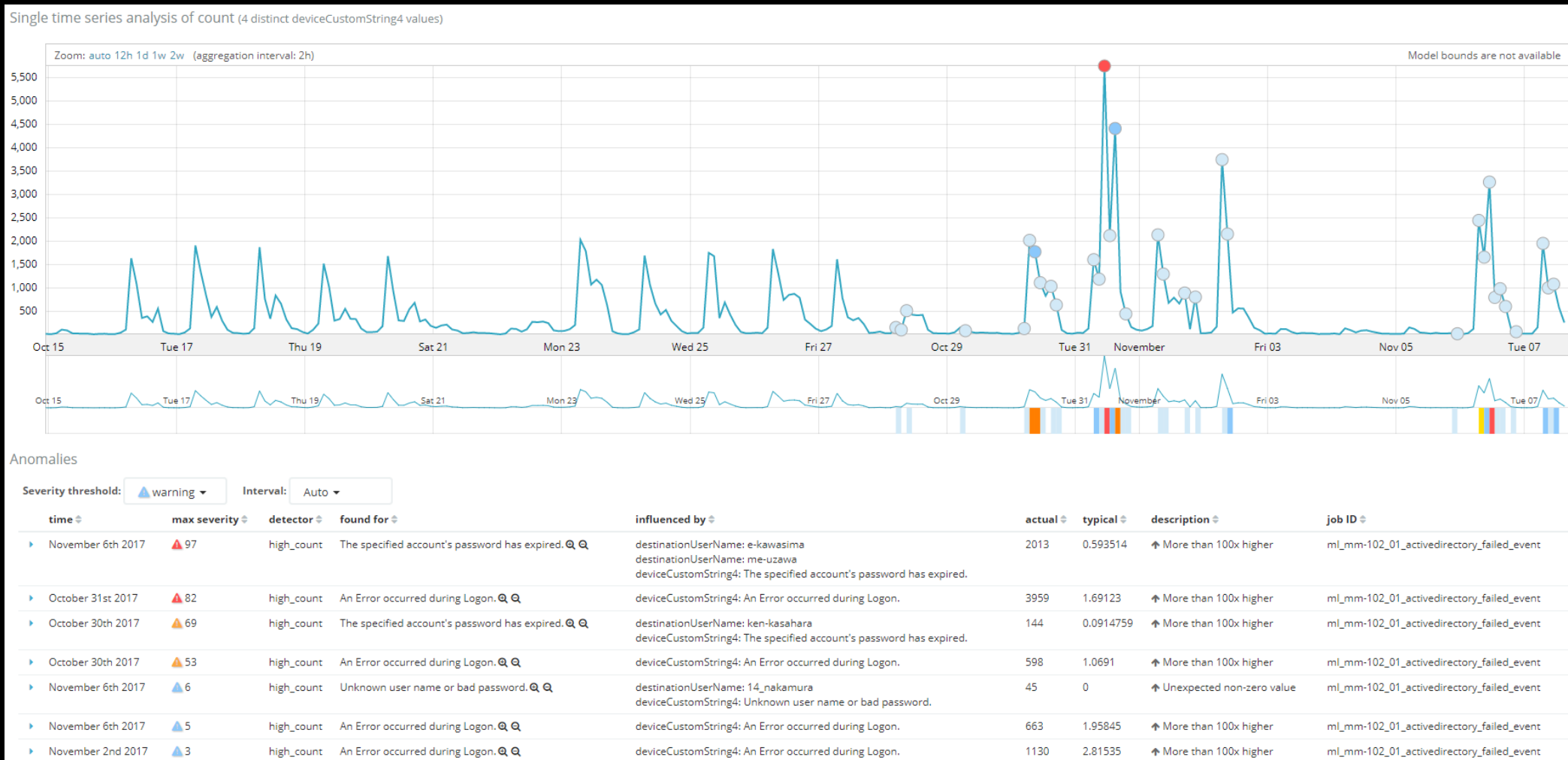
また、通常のログやトラフィックの中から不正なログやトラフィックを見つけ出す作業は、専門家による高度な分析が求められるようになってきています。

# 攻撃の発見から対応まで一貫して対応することが重要となります



# 【参考】欧米ではログ監視にディープラーニングは普通に使われています

## マシンラーニングを活用した異常検知



CISOの役割について考えましょう



# CISOのOはOfficerである。Officerとは何なのか？

## 株式会社を例に構造から考える

株式会社の特徴は、所有と経営の分離

株主は会社を所有するが経営は行ないません。

株主の資本的多数決により株主の立場に立って経営を監督する人（取締役）を選任します。

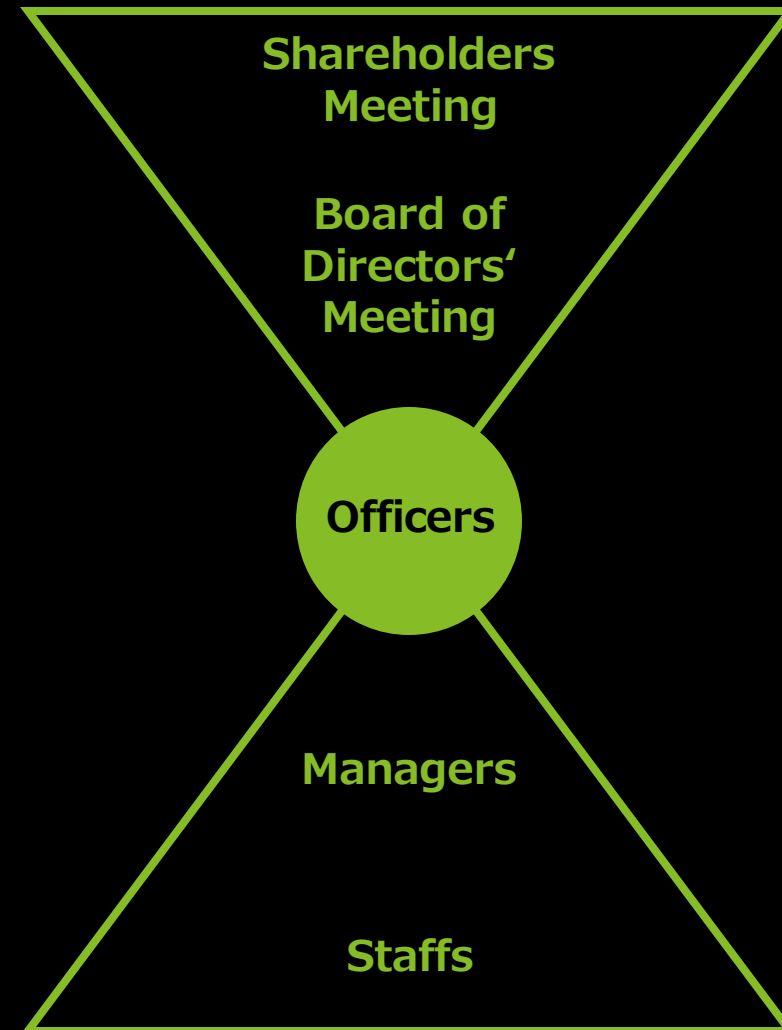
取締役の合議（取締役会）により経営を行う人（執行役）を選任します。

執行役が経営を行います。

執行役は

- ・ 業務の有効性・効率性を高め
- ・ 法令等を遵守し
- ・ 業務に関する説明責任を果たし、

株主の期待にこたえる必要があります。



# Officerの仕事の全体像

セキュリティは経営課題のひとつです





# CISOというポジションが必要かどうかは業務量等に依存します

業務内容が重要で、業務量が多ければCISOとして独立させて任命する必要性があります。

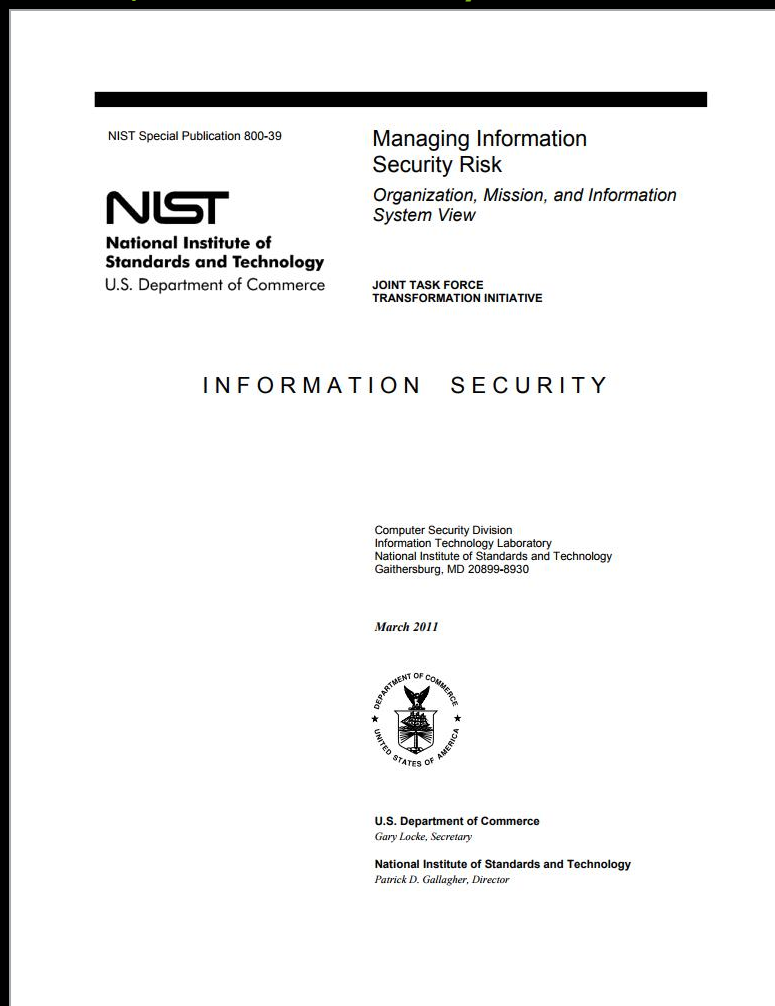


# (参考) 情報セキュリティマネジメントの内容

## NIST SP800-39

### Managing Information Security Risk

#### Organization, Mission, and Information System View



## CHAPTER ONE INTRODUCTION

- 1.1 PURPOSE AND APPLICABILITY
- 1.2 TARGET AUDIENCE
- 1.3 RELATED PUBLICATIONS
- 1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION

## CHAPTER TWO THE FUNDAMENTALS

- 2.1 COMPONENTS OF RISK MANAGEMENT
- 2.2 MULTITIERED RISK MANAGEMENT
- 2.3 TIER ONE—ORGANIZATION VIEW
- 2.4 TIER TWO—MISSION/BUSINESS PROCESS VIEW
- 2.5 TIER THREE—INFORMATION SYSTEMS VIEW
- 2.6 TRUST AND TRUSTWORTHINESS
- 2.7 ORGANIZATIONAL CULTURE
- 2.8 RELATIONSHIP AMONG KEY RISK CONCEPTS

## CHAPTER THREE THE PROCESS

- 3.1 FRAMING RISK
- 3.2 ASSESSING RISK
- 3.3 RESPONDING TO RISK
- 3.4 MONITORING RISK

## APPENDIX

A. REFERENCES

B. GLOSSARY

C. ACRONYMS

**D. ROLES AND RESPONSIBILITIES**

E. RISK MANAGEMENT PROCESSTASKS

F. GOVERNANCE MODELS

G. TRUST MODELS

H. RISK RESPONSE STRATEGIES

D.1 HEAD OF AGENCY (CHIEF EXECUTIVE OFFICER)

D.2 RISK EXECUTIVE (FUNCTION)

D.3 CHIEF INFORMATION OFFICER

D.4 INFORMATION OWNER/STEWARD

**D.5 SENIOR INFORMATION SECURITY OFFICER**

D.6 AUTHORIZING OFFICIAL

D.7 AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE

D.8 COMMON CONTROL PROVIDER

D.9 INFORMATION SYSTEM OWNER

D.10 INFORMATION SYSTEM SECURITY OFFICER

D.11 INFORMATION SECURITY ARCHITECT

D.12 INFORMATION SYSTEM SECURITY ENGINEER

D.13 SECURITY CONTROL ASSESSOR

## D.5 SENIOR INFORMATION SECURITY OFFICER

The senior information security officer is an organizational official responsible for:

- (i) carrying out the chief information officer security responsibilities under FISMA; and
- (ii) serving as the primary liaison for the chief information officer to the organization's authorizing officials, information system owners, common control providers, and information system security officers.

The senior information security officer:

- (i) possesses professional qualifications, including training and experience, required to administer the information security program functions;
- (ii) maintains information security duties as a primary responsibility; and
- (iii) heads an office with the mission and resources to assist the organization in achieving more secure information and information systems in accordance with the requirements in FISMA.

The senior information security officer (or supporting staff members) may also serve as authorizing official designated representatives or security control assessors.

The role of senior information security officer has inherent U.S. Government authority and is assigned to government personnel only.

FISMAというルールの中での話ですが

- (i) CIOの下でセキュリティに関する責任を果たす
- (ii) CIOと組織の承認者、情報システムオーナー、総務部門、情報システムセキュリティ担当者との主な連携役となる

CISOは

- (i) セキュリティプログラムを管理するために必要な専門的能力を有する
- (ii) セキュリティに関する責務を第一の責任として維持する
- (iii) 情報、情報システムをより安全になるように組織を支援するための使命と資源を有するチームを指揮する

# セキュリティに関する責任

## 整備と運用

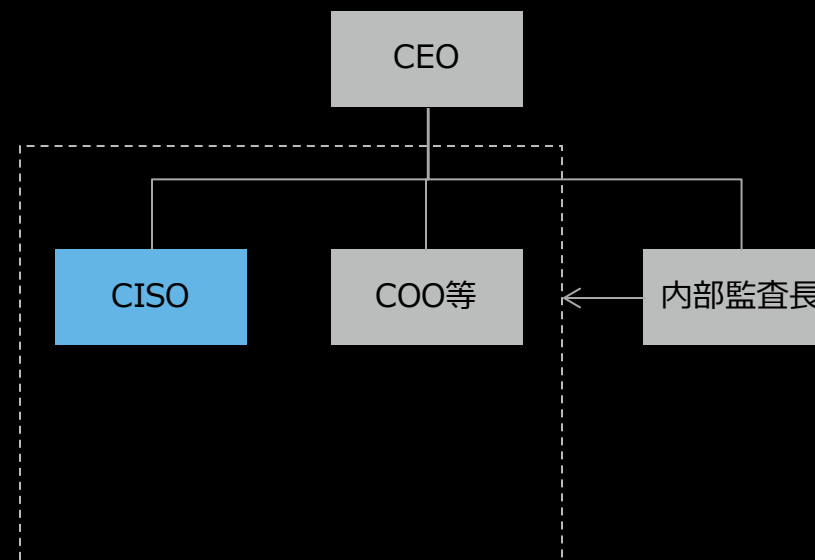
### 一般企業の場合

セキュリティに関するルールを整備するのはセキュリティ担当の責任です。

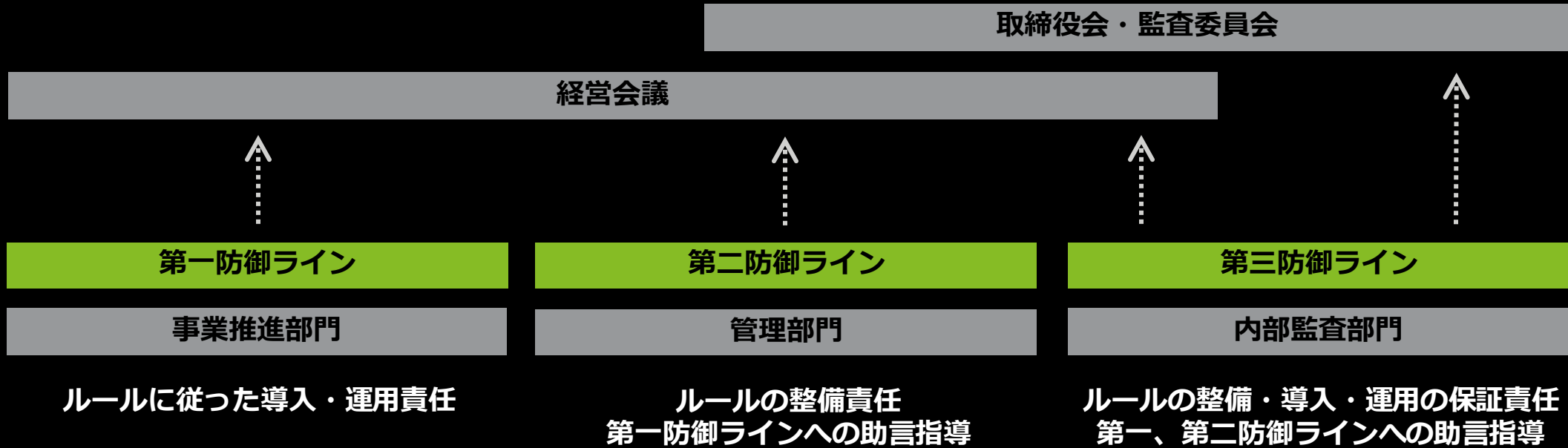
整備されたルールに従って運用するのは、各事業部門の責任です。

運用の支援（Consultation）をするのはセキュリティ担当の責任です。

実施結果の保証は内部監査部門の責任です。



# CISOの機能をCIOの一部とする場合の課題



CIO配下の情報システム部門が第一防御ラインになり、CIO配下のCISOが第二防御ラインとなることが想定されるため、第一防御ラインと第二防御ラインの牽制機能が有効とはなりません。CIOが責任をもってバランスをとることになるが、CIOは第一防御ラインの責任が重いために、第二防御ラインの機能がおろそかになる可能性があり、セキュリティ対策が全社的に進まなくなる可能性が高まる。

# セキュリティの危機対応時のCISOの責任

## 専門家として危機対応に当たる

最終決定はCEO等が行うとしても、専門知識と経験を踏まえて、適切な意思決定を支援します。

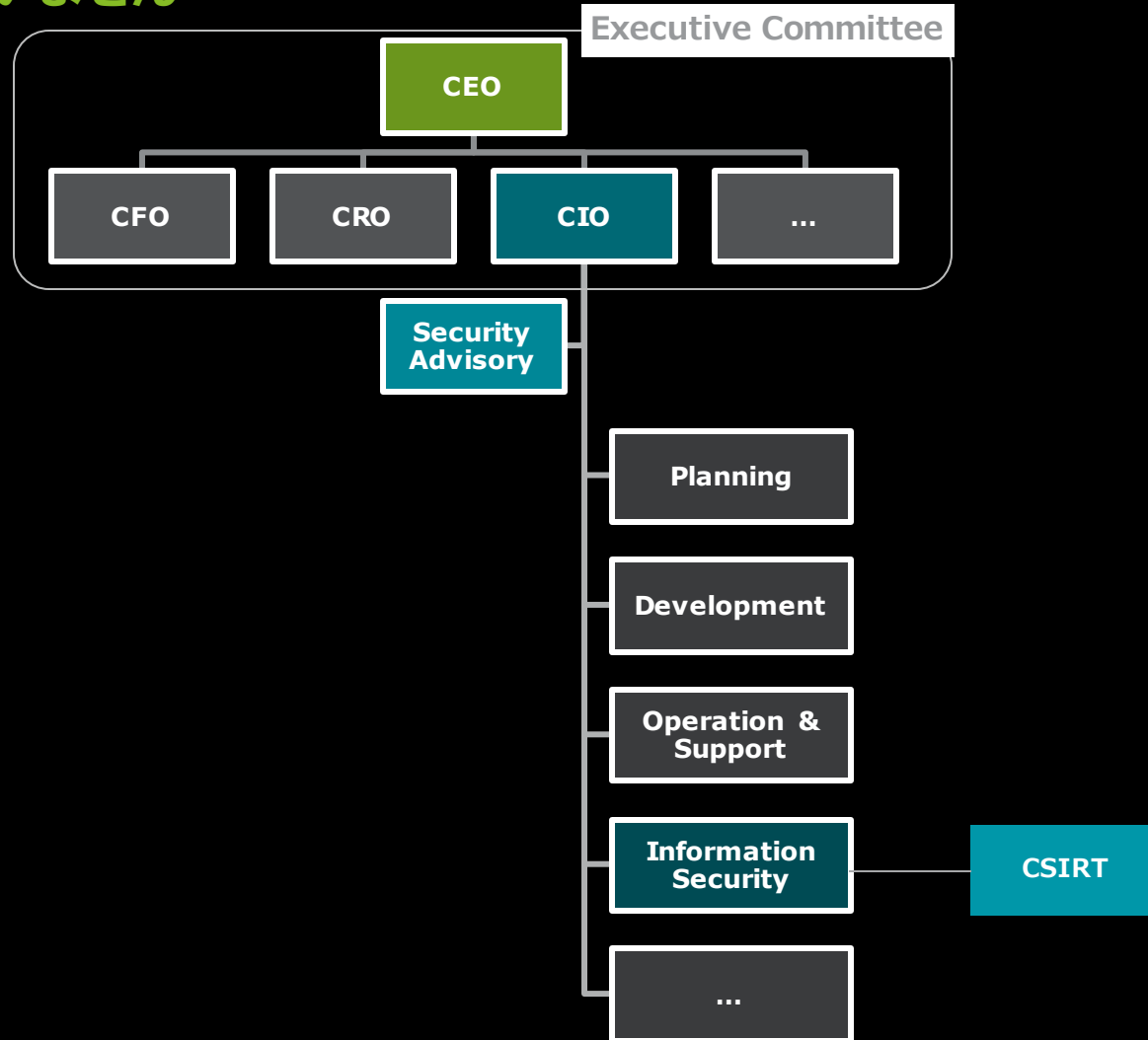
事実上は、権限の委譲を受けて取り仕切ることになりません。

マルウェアに感染し機密情報が漏洩していることが想定されることがわかったときに、情報システムの状況も知らない、マルウェアが何をするかも理解していない状態で、経営者に適切な意思決定ができるのでしょうか？



# 参考 A社（12,000名）では

## CISOはいません



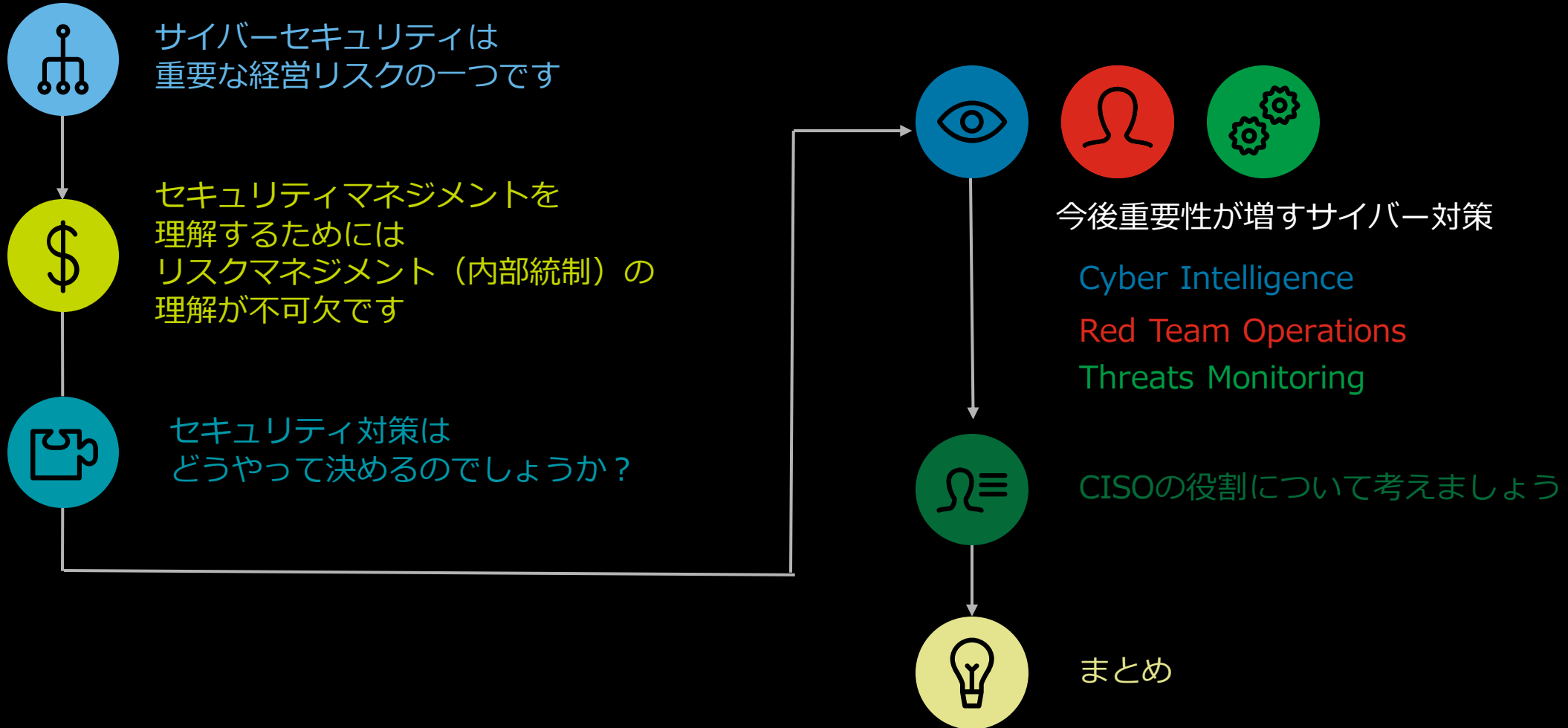


# まとめ



# まとめ

## 企業の危機管理担当者が把握すべきサイバーセキュリティ最前線



デロイト トーマツ グループは日本におけるデロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）のメンバーファームであるデロイト トーマツ 合同会社およびそのグループ法人（有限責任監査法人 トーマツ、デロイト トーマツ コンサルティング 合同会社、デロイト トーマツ ファイナンシャル アドバイザリー 合同会社、デロイト トーマツ 税理士 法人、DT 弁護士 法人およびデロイト トーマツ コーポレート ソリューション 合同会社を含む）の総称です。デロイト トーマツ グループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザー、コンサルティング、ファイナンシャルアドバイザー、税務、法務等を提供しています。また、国内約40都市に約11,000名の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト（[www.deloitte.com/jp](http://www.deloitte.com/jp)）をご覧ください。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザーサービス、リスクアドバイザー、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを Fortune Global 500® の8割の企業に提供しています。“Making an impact that matters”を自らの使命とするデロイトの約245,000名の専門家については、[Facebook](#)、[LinkedIn](#)、[Twitter](#)もご覧ください。

Deloitte（デロイト）とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド（“DTTL”）ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数を指します。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL（または“Deloitte Global”）はクライアントへのサービス提供を行いません。Deloitteのメンバーファームによるグローバルネットワークの詳細は [www.deloitte.com/jp/about](http://www.deloitte.com/jp/about) をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

