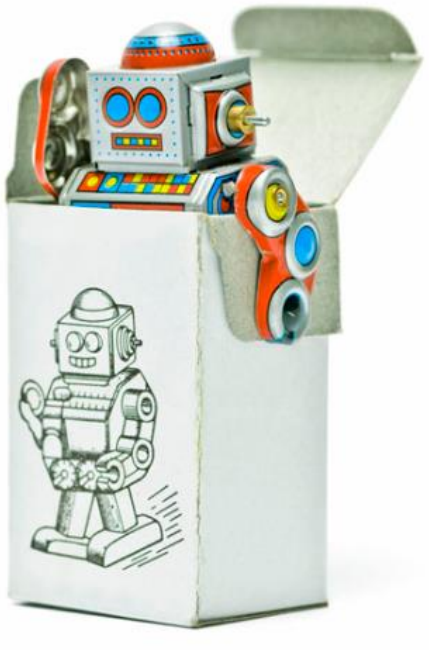
Deloitte.

内部不正

どう対応するか



2015年01月27日

デロイト トーマツ リスクサービス株式会社　代表取締役 社長
公認会計士 公認情報システム監査人 （CISA）
丸山　満彦

トーマツ.

アジェンダ

会計から学ぶ内部不正対策の基本

情報セキュリティ対策の基本

不正対策手法から学ぶ情報保護

どこまでするのかは経営判断

当該内容は発表者の私見であり、関係する団体の公式見解ではありません。

まずはじめに理解して欲しいこと

不正をなくすことはできるか？

死刑制度があっても殺人がなくならないように

どのような手段をとっても内部不正を100%なくすことはできない。

重要なことは**合理的な範囲に内部不正によるリスクを低減**するために

・**どのような方法**があるのか

・**どの程度**それを実施すればよいのか

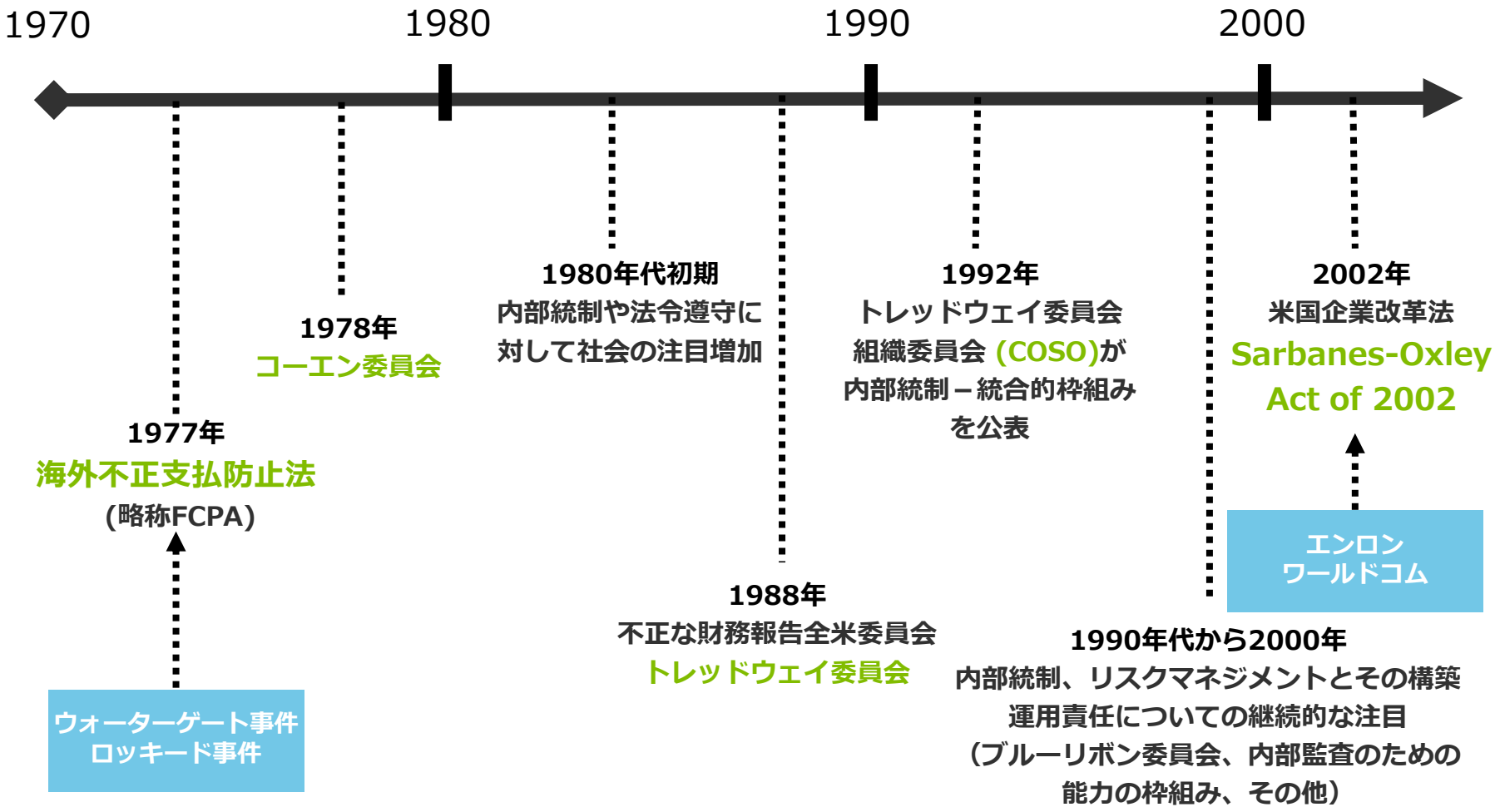
ということである。

内部統制の限界

会計から学ぶ内部犯行対策の基本

米国における不正との戦い

おもに経営者不正



公認会計士は常に不正と戦っている

財務報告に重要な影響を及ぼす不正

	経営者による不正	従業員による不正
財務報告の虚偽表示		
資産の流用		

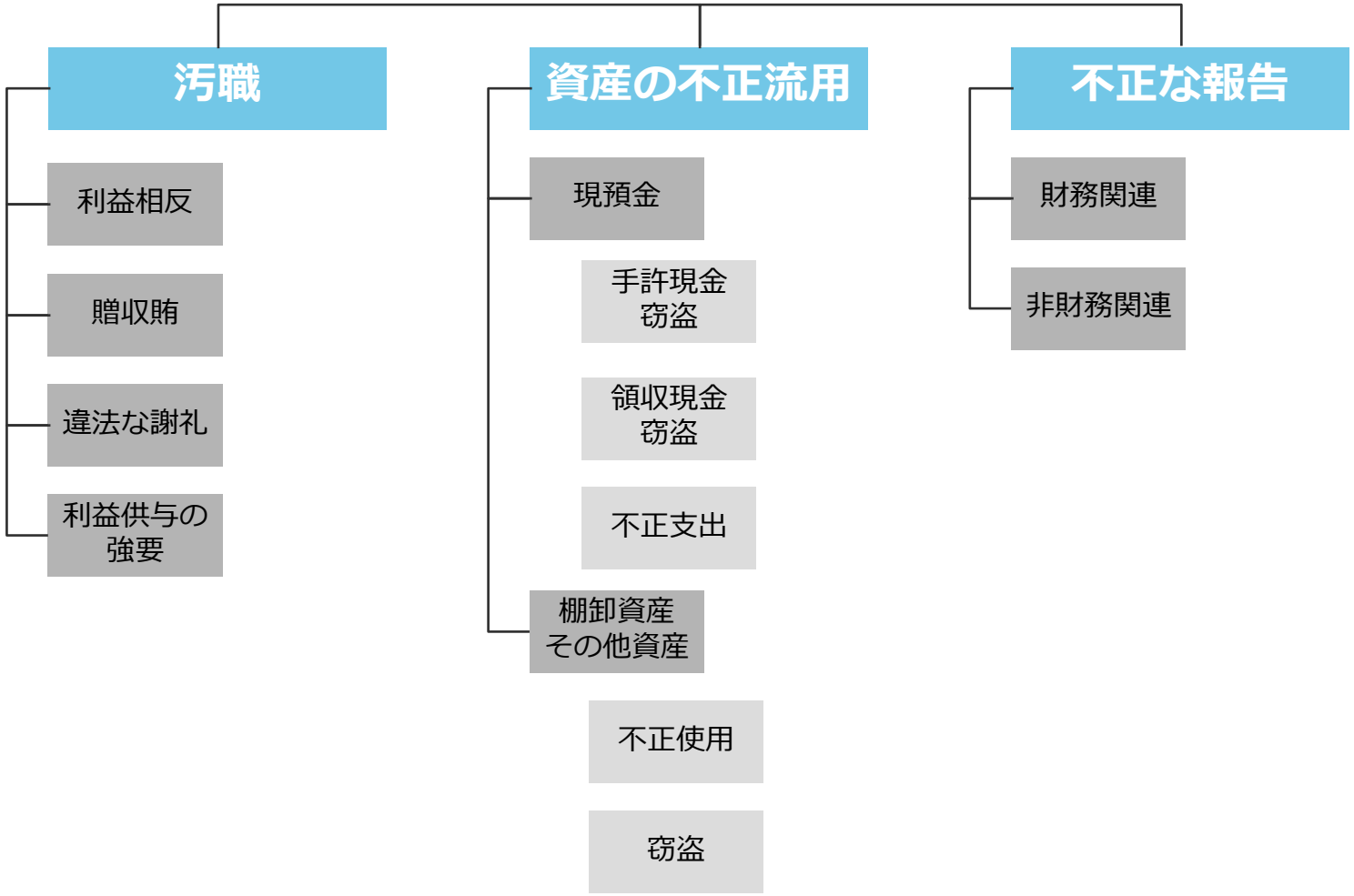
経営者は

1．内部統制を無効にできる立場にある

2．影響度の大きな不正を行いうる立場にある

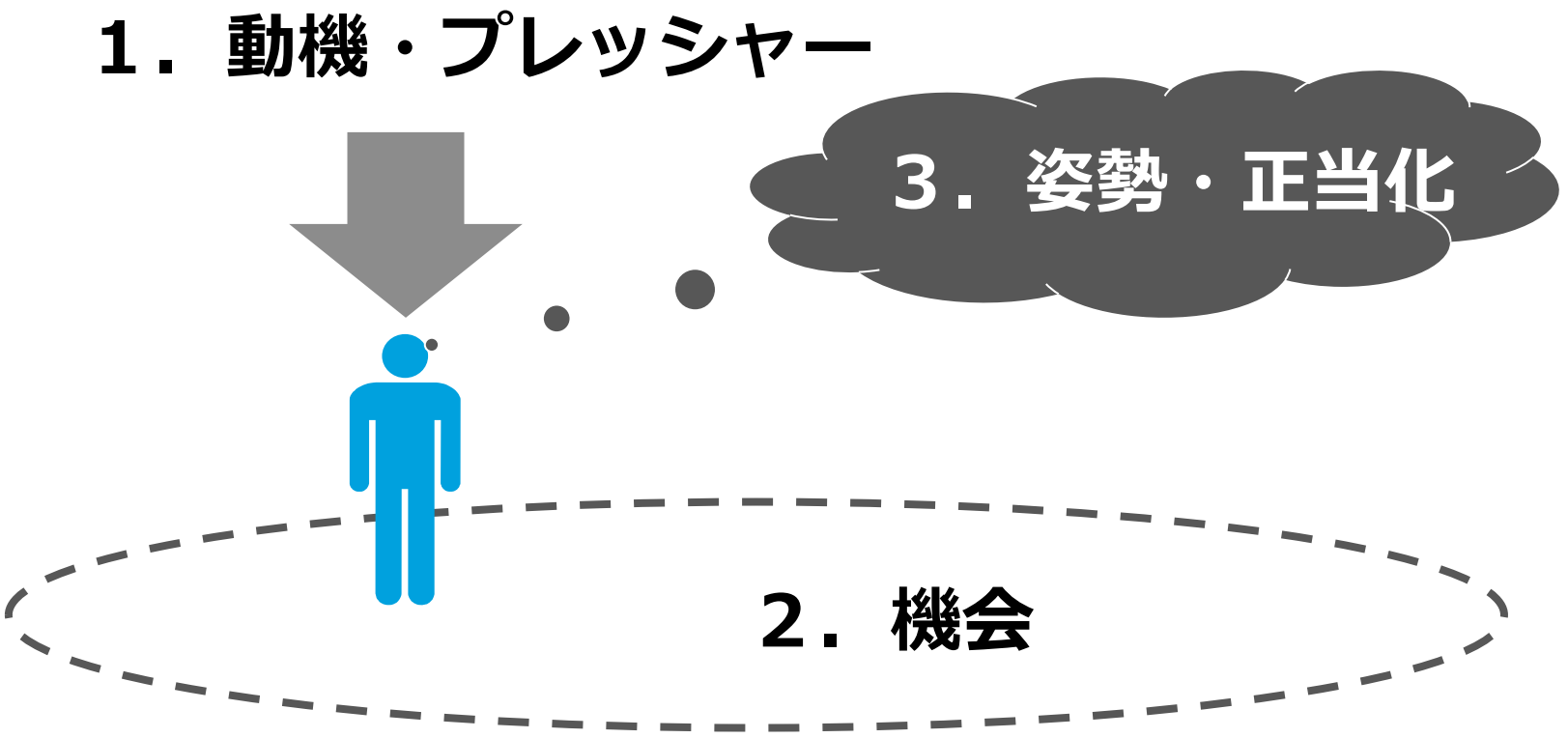
不正の分類（不正検査士協会）

不正の全体像を俯瞰してみる



内部犯行対策には不正のトライアングルの理解が重要です

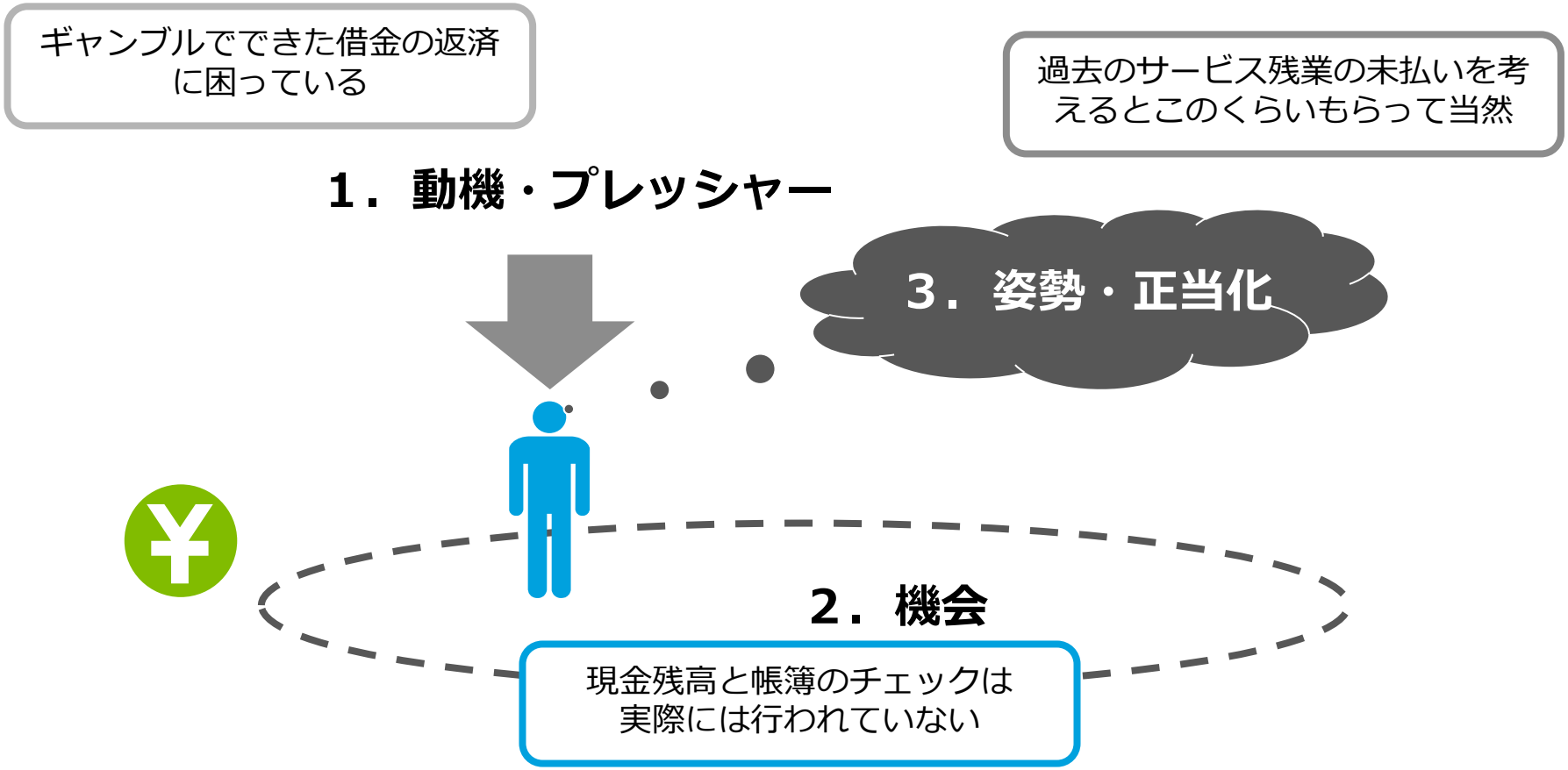
不正の要因を減少させる対策が必要です



3つの要素が重なると不正が起こるといわれています。

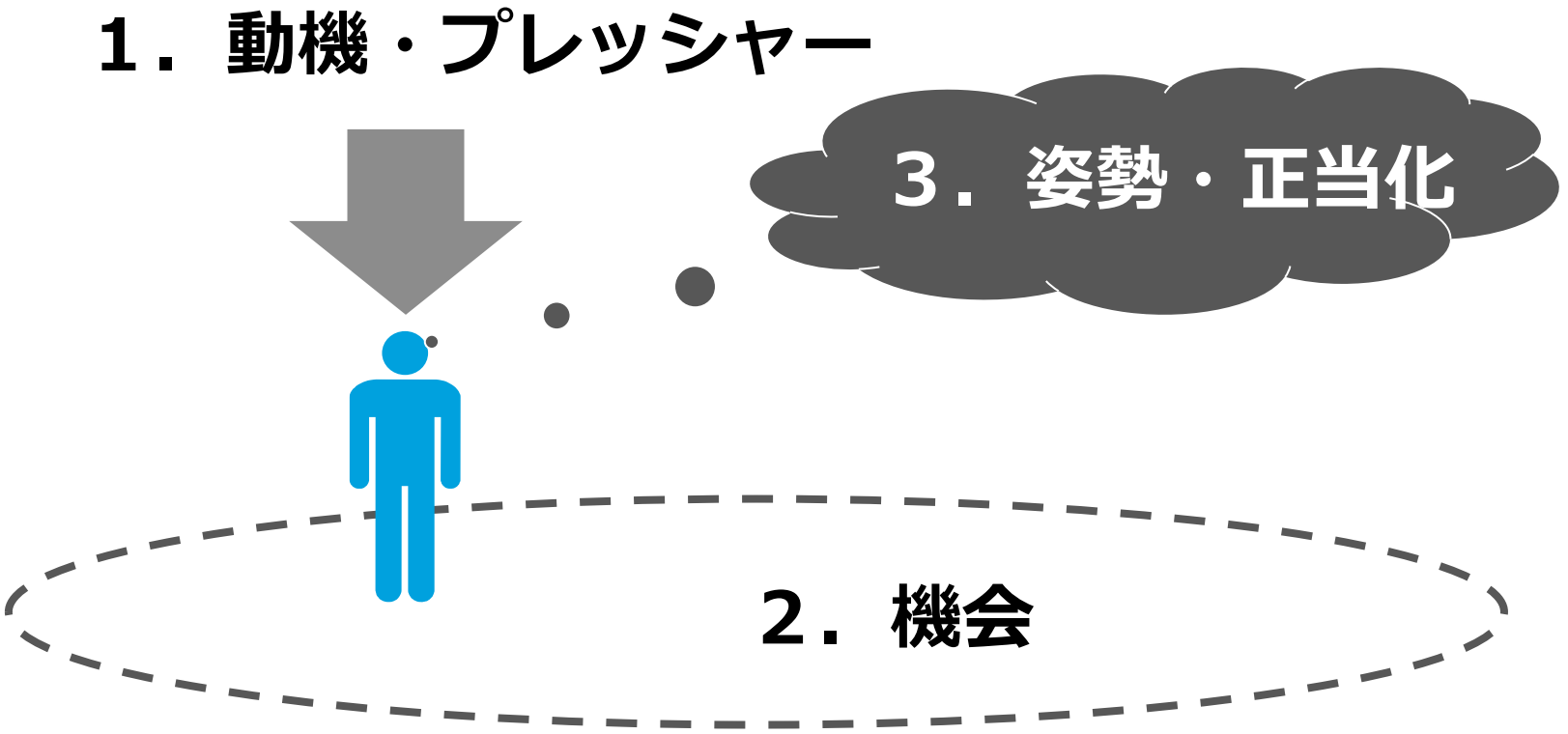
不正のトライアングルによる不正の説明

現金の着服（手許現金窃盗）



不正の要員を減少させる対策が必要です

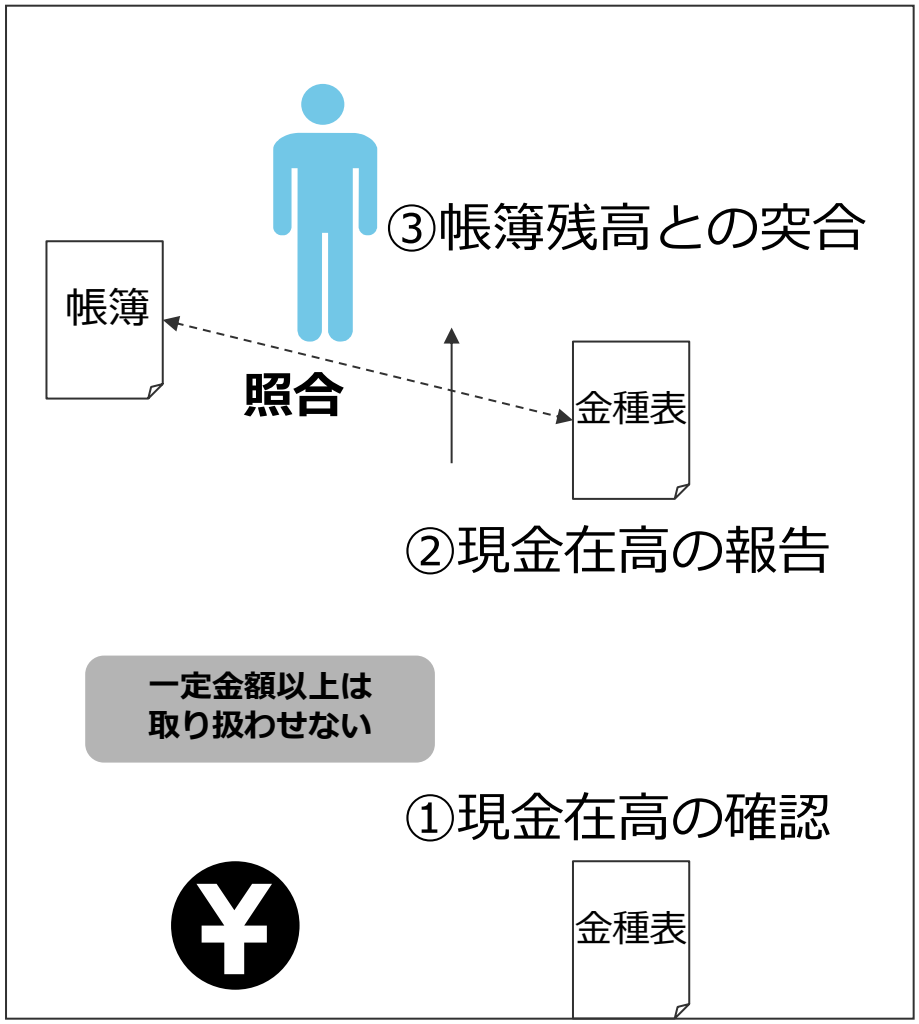
不正を行える「機会」をなくすことが重要です

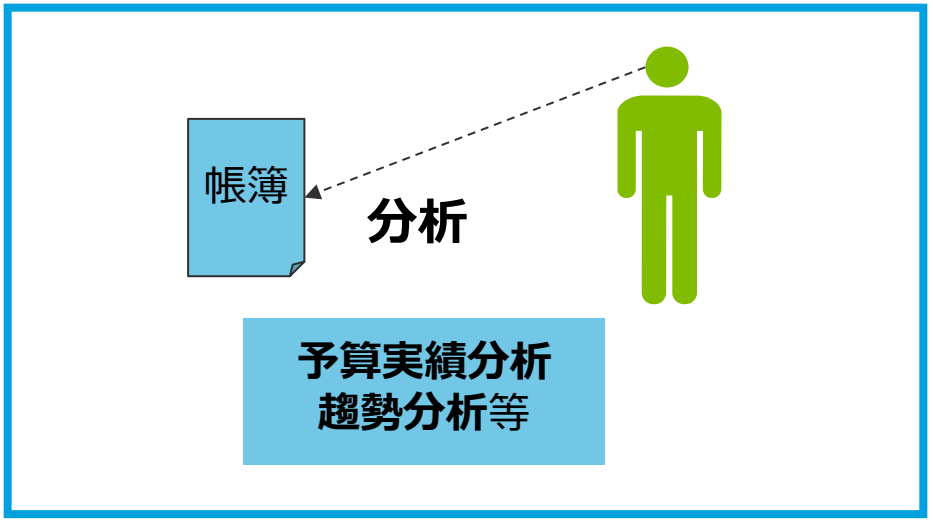


「機会」以外の要因を会社側で有効にコントロールすることは難しい

不正を防ぐための現金管理の仕組み（機会）

現金管理





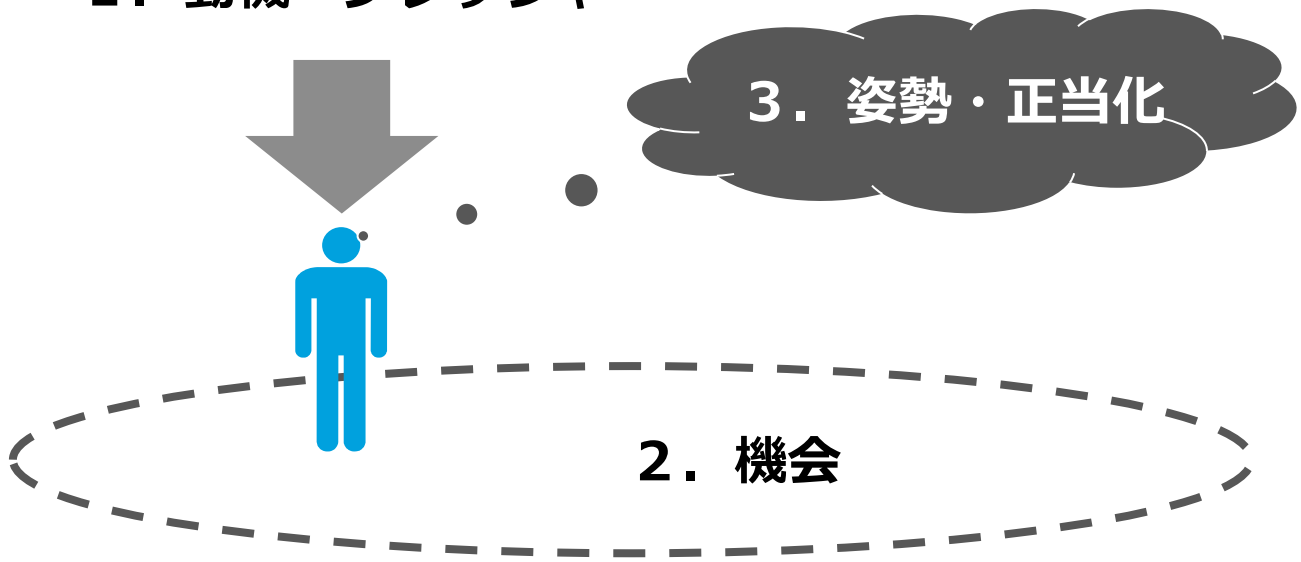
1. 現金の上限金額を定める
2. 現金出納と帳簿をつける人を分ける
3. 現金残高と帳簿残高の一致を上長が確認する
4. 残高の推移等をレビューする人を設置する
5. 内部監査等の第三者の確認をいれる

動機・プレッシャーと姿勢・正当化への対策

確実性は高くないですが、一定の効果はあります

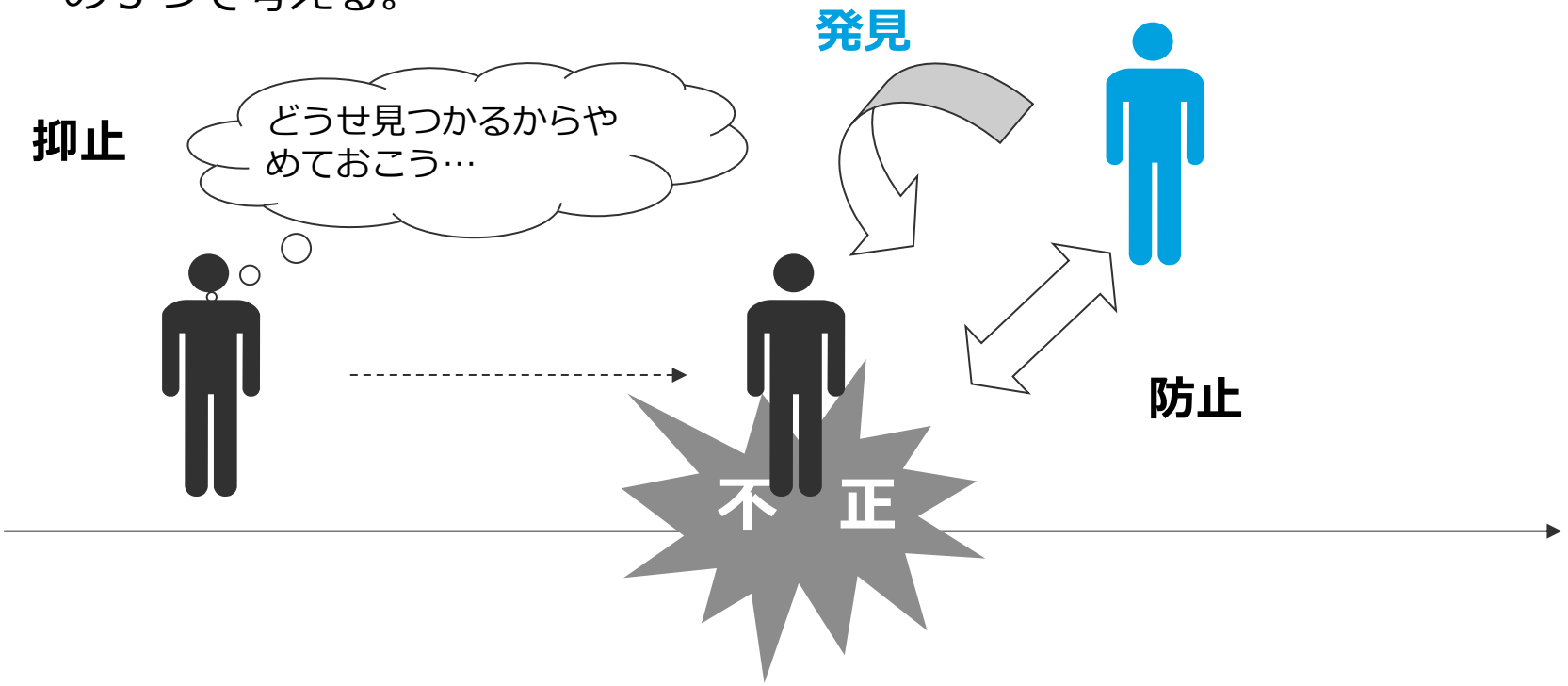
不正をしても発見され、
不利益を受けることを理解していれば
不正への抑止となる

倫理観高く、
誰も不正をしていない環境であれば
不正への抑止となる



する気にさせない、できない、みつける

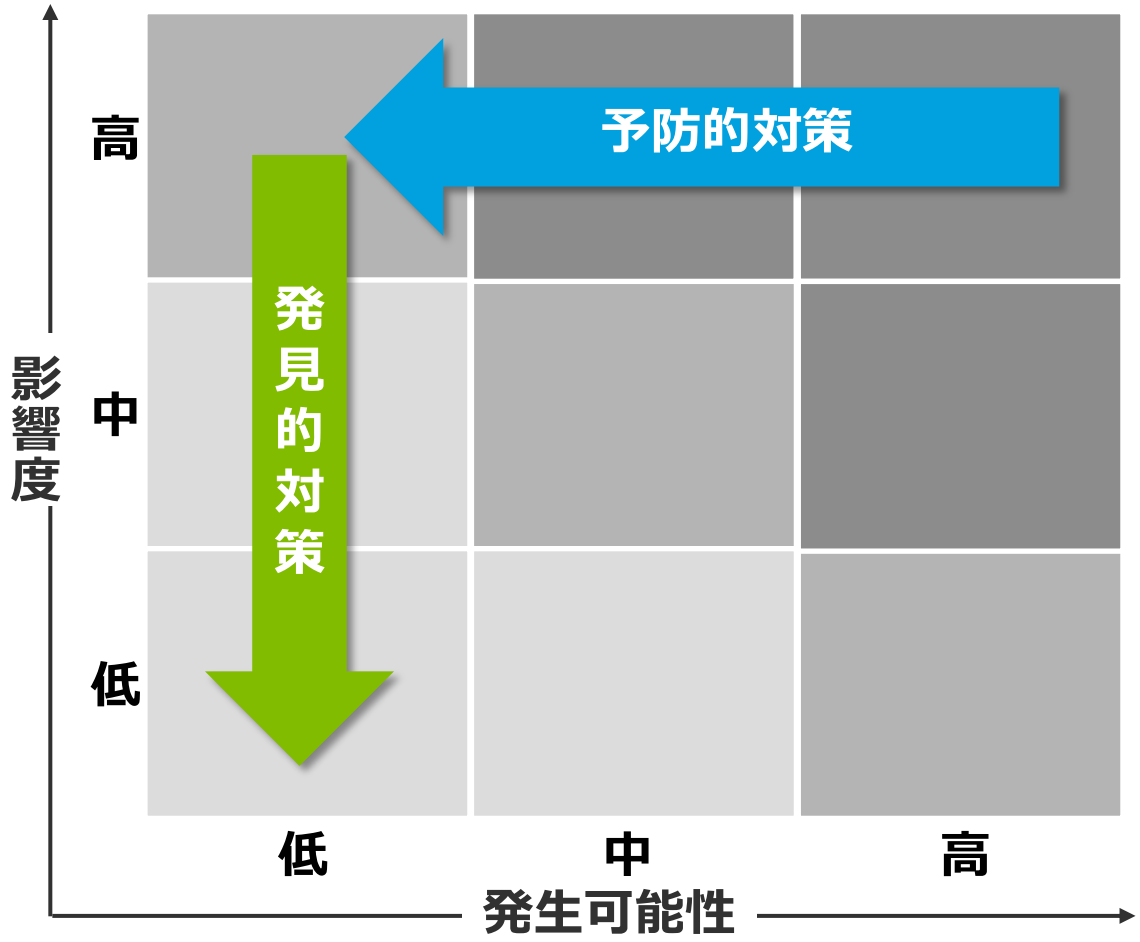
■ 抑止　（する気にさせない）
■ 防止　（できないようにする）
■ 発見　（不正を見つけ出す）
の３つで考える。



情報セキュリティ対策の基本

情報セキュリティ対策はリスク対策の一環です

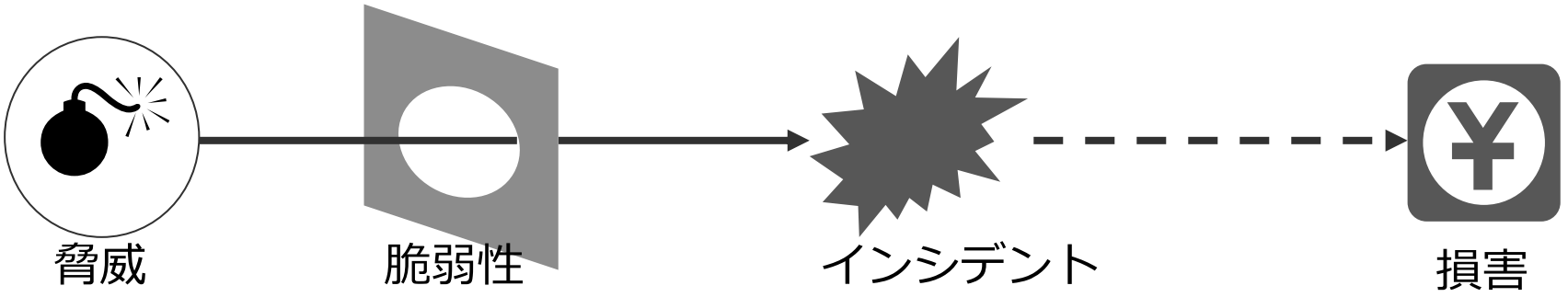
予防的対策と発見的対策を組み合わせなければなりません



予防的対策に加えて、発見的対策を強化することでリスクを低減する

情報セキュリティ対策の基本

損害をミニマムにすることが目的です



予防的対策　　**発見的対策**

対策

抑止	予防	検出	対応

主に**発生可能性**の低減　　**損害**の低減

損害のミニマム化

ITセキュリティ対策の基本は変わりません

アクセス管理が基本です

- Need to Know
- Least Privilege

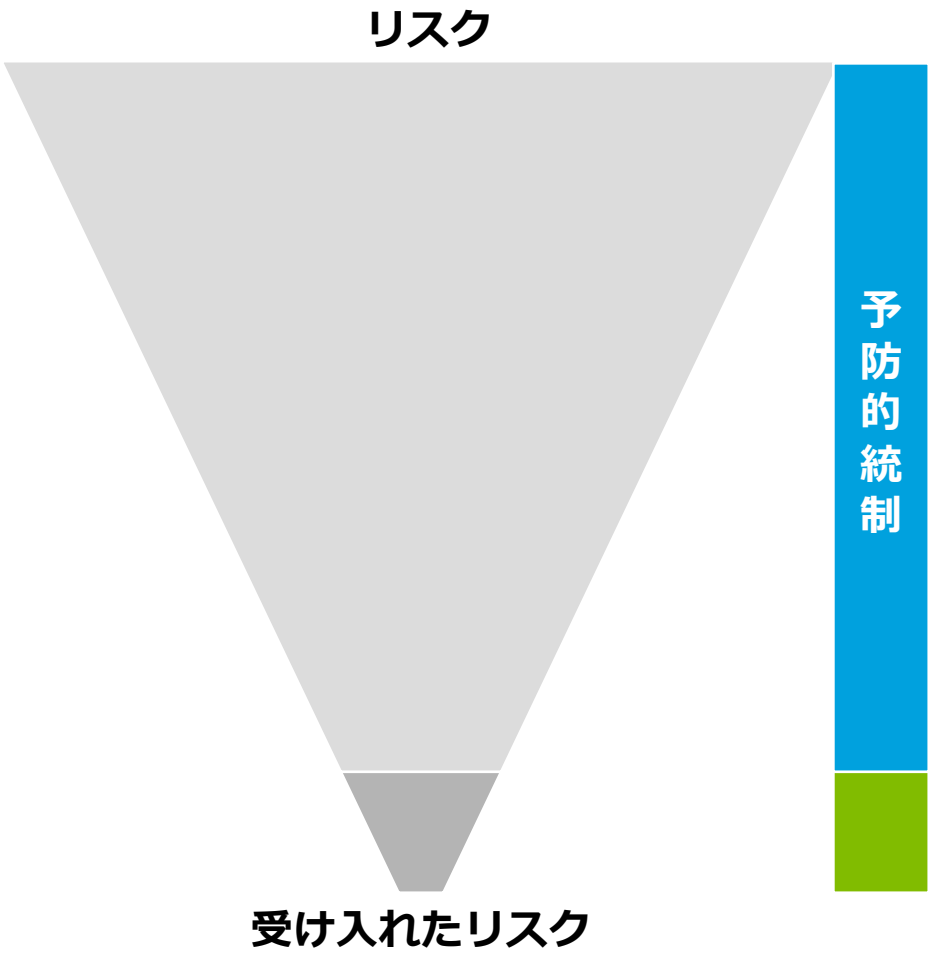
予防的対策　　発見的対策

アクセス管理で不正を行える機会を減らすことが重要です

Need to Know, Least Privilegeは厳格に適用できていますか？

セキュリティ対策の基本は予防的な対策です

アクセス管理、脆弱性管理、暗号化をまずは実施する。



できる限り泥棒にお金を盗まれないようにする

できる限りアクセス管理、暗号化等で対策を実施する

システム管理者	OSの特権	データベースの特権	アプリケーションの特権
OS 管理者A	○	×	×
データベース 管理者B	×	○	×
アプリケーション 管理者C	×	×	○
ネットワーク 管理者D	×	×	×

「万が一」盗まれても見つけて捕まえれるようにする

アクセス管理を十分に実施できなかった部分は検知対策を実施する

内部不正と標的型攻撃の対策は似ています

事後的な対策も重要となってきます

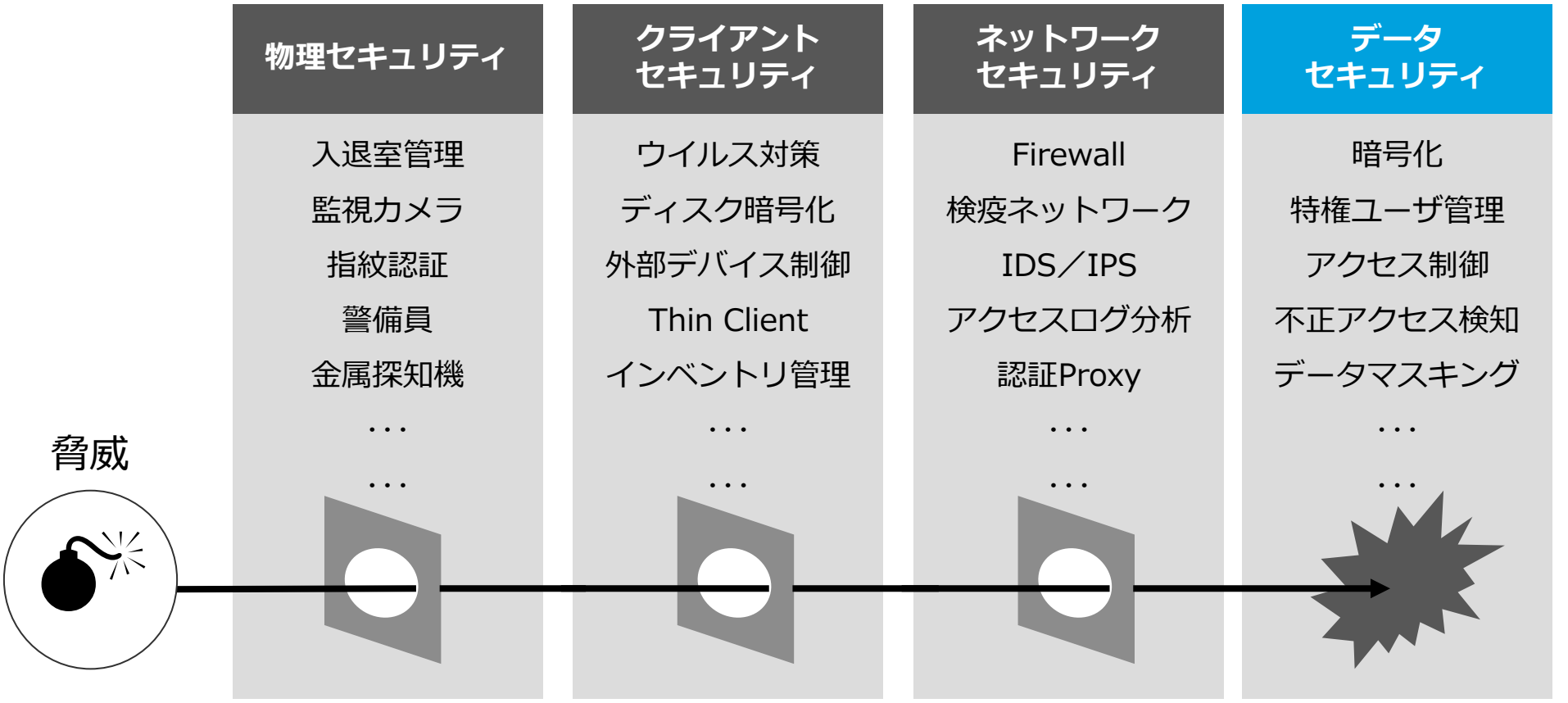
		抑止	予防	検出	対応
1	一般的なミス・不正	○	◎	○	△
2	受け入れたリスクで付与した 権限者による不正	○	△	○	△
3	(2で設計した特権を奪取する) 標的型攻撃	×	△	○	△

不必要な権限は与えないことが重要
権限がとられないようすることが重要

◎：効果的
○：効果あり
△：効果は限定的
×：効果はない

企業に求められるセキュリティ対策
～多層防御で特権を分散させる

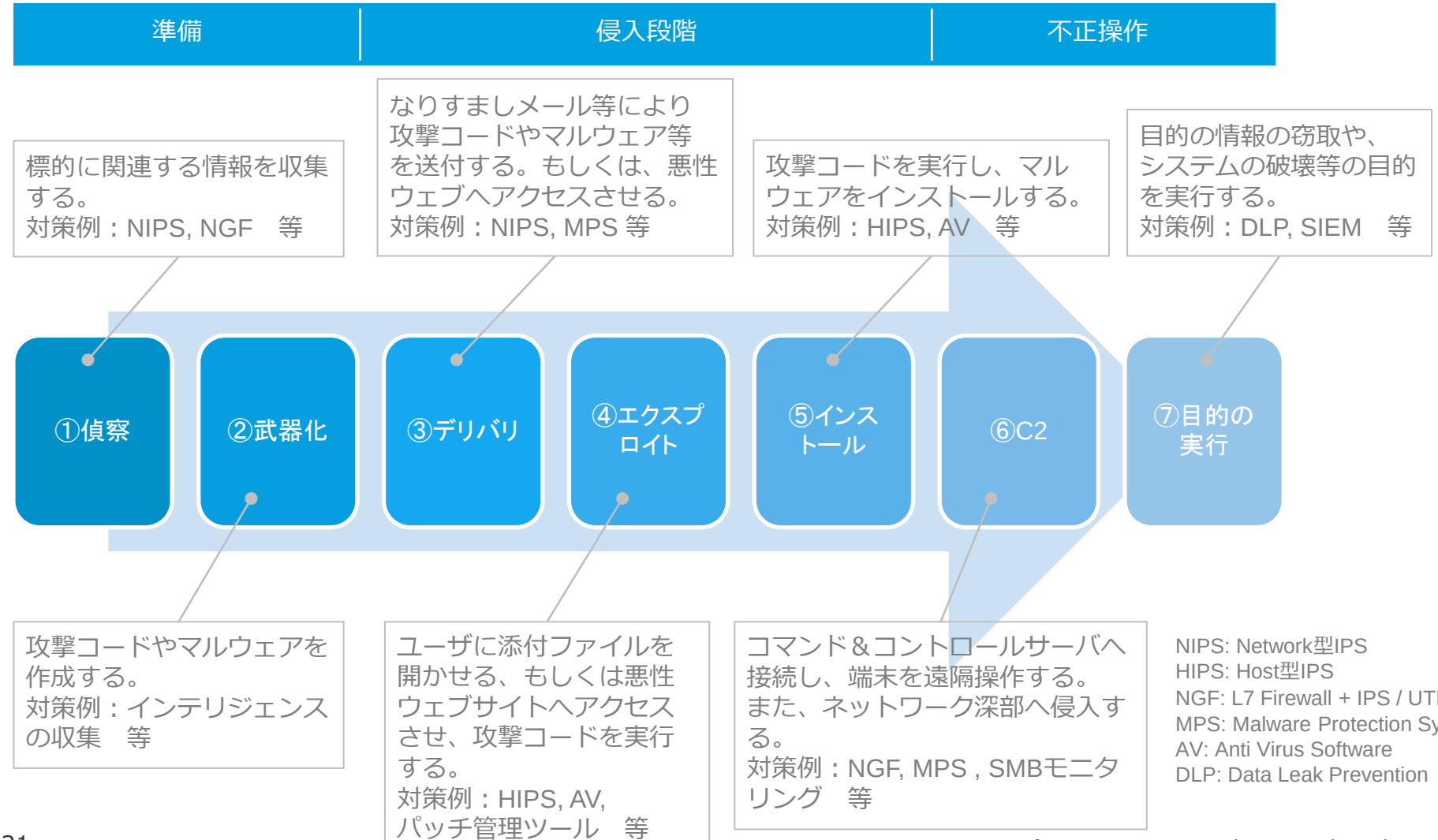
それぞれの対策での管理者を分離する



多層防御をしていても、
すべてのデバイスの特権ユーザが一人であれば内部不正は防げません

【参考】Cyber Kill Chain とは

Cyber Kill Chainとは攻撃者の一連の行動を、軍事行動に例えたもので、検知・拒否・中断・緩和・騙欺により、多層防御を実現し各ステップのいずれかで脅威を断ち切る考え方。



NIPS: Network型IPS
HIPS: Host型IPS
NGF: L7 Firewall + IPS / UTM
MPS: Malware Protection System
AV: Anti Virus Software
DLP: Data Leak Prevention

ログをとっているだけではログ管理になりません

ログの検査は最低限必要です

イベントソース

- PC
- Network Devices
- UNIX, Linux, Windows…
- AS/400 Mainframe
- Data Base
- Business Applications

参照情報

- 脆弱性管理DB
- Security Intelligence

【一元管理】

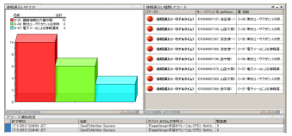
SIEM System

【分析とレポーティング】

①即時アラート

攻撃の疑いが検知された場合、その事実を直ちにメール等で通知する

②ダッシュボード



システム上で発生しているイベントのサマリ情報をダッシュボード形式でリアルタイムに確認する

③定期レポート

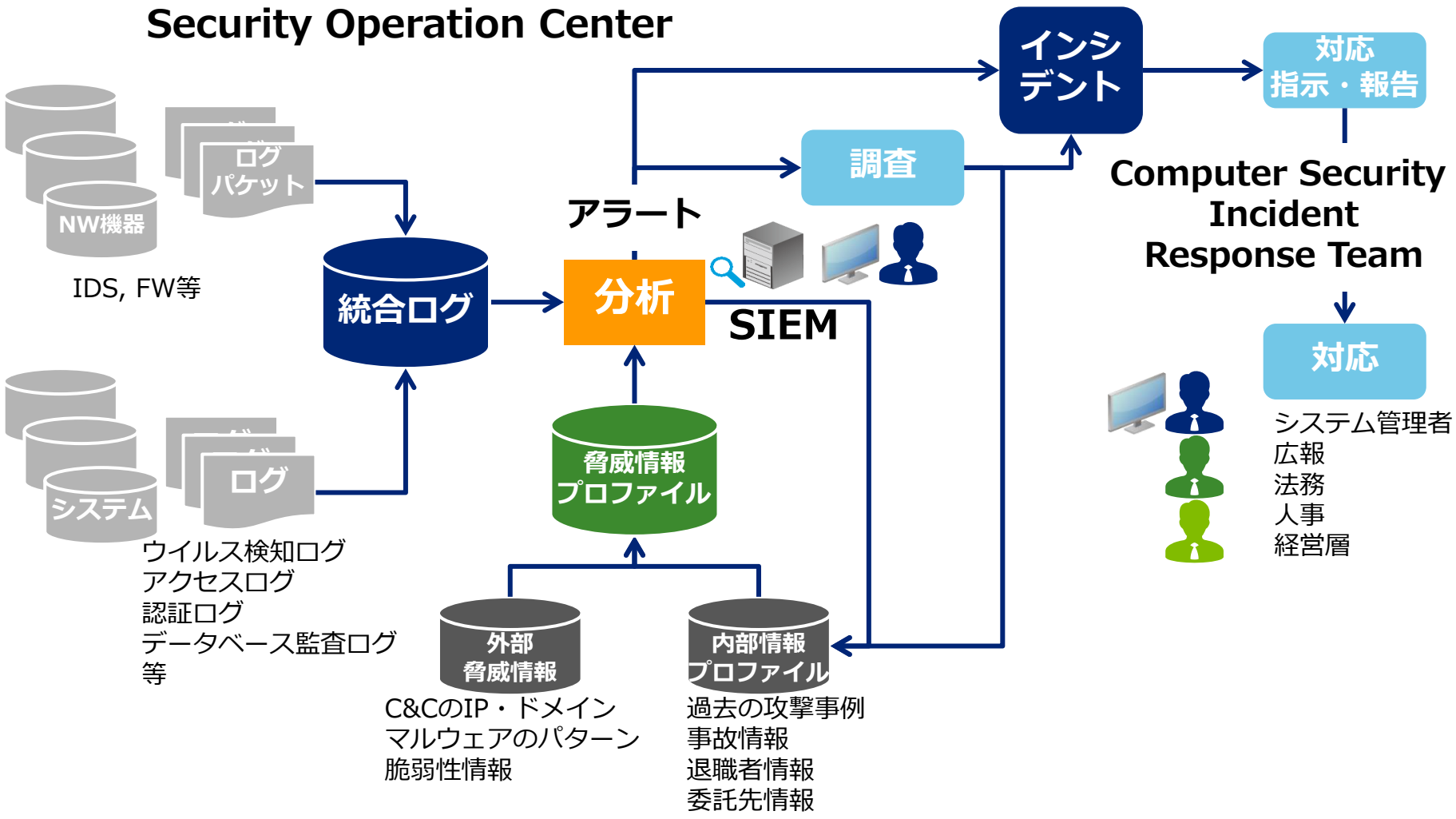
日次/週次/月次等の頻度で、攻撃の兆候や発生に係る定期レポートを出力する

【ステータス管理】

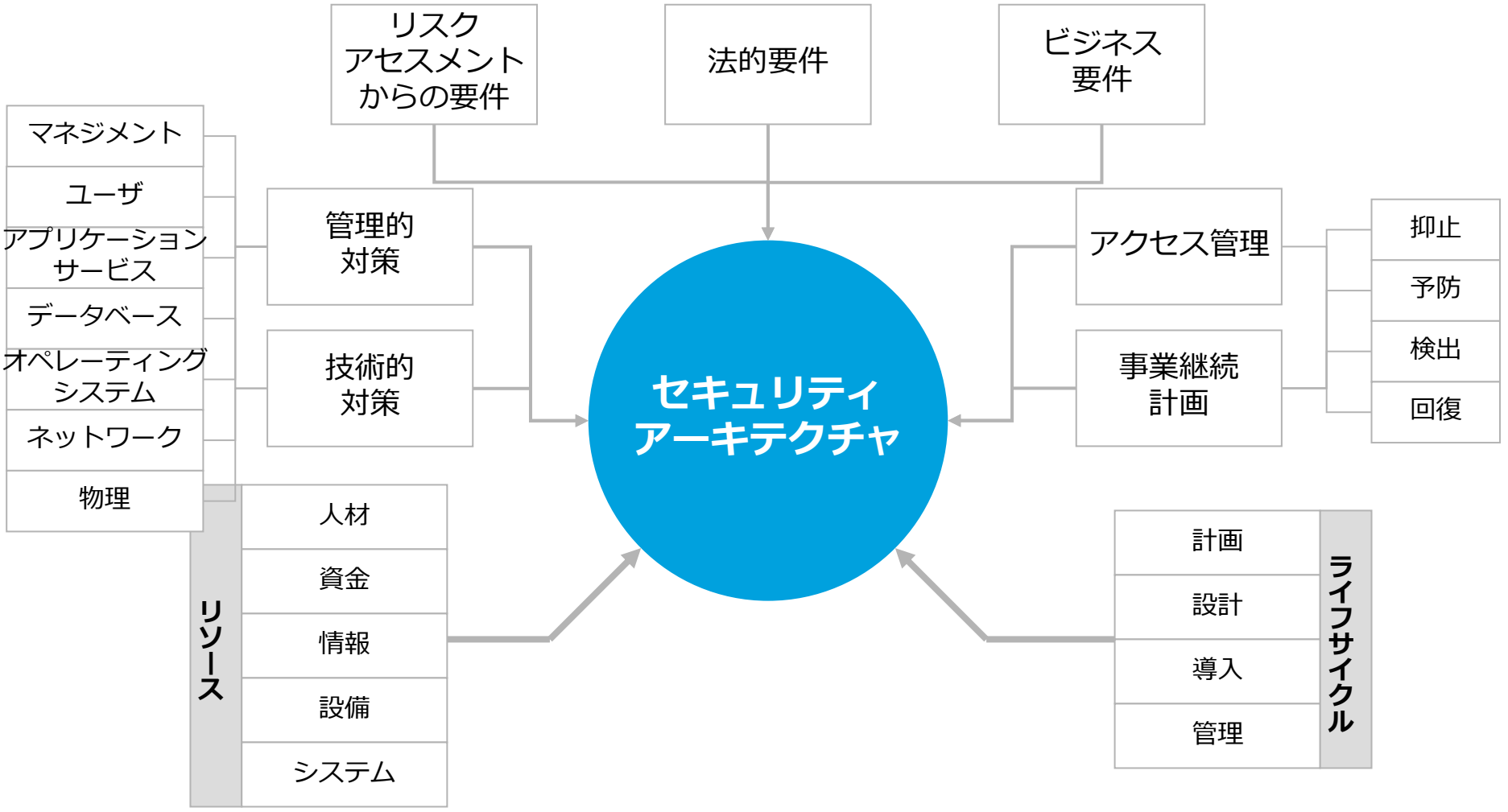
即時アラート、ダッシュボードまたは定期レポートで攻撃の疑いを検知した場合、関連部門と連携し、調査する

企業に求められるセキュリティ対策
～発見的対策と対応の強化

SOCとCSIRT

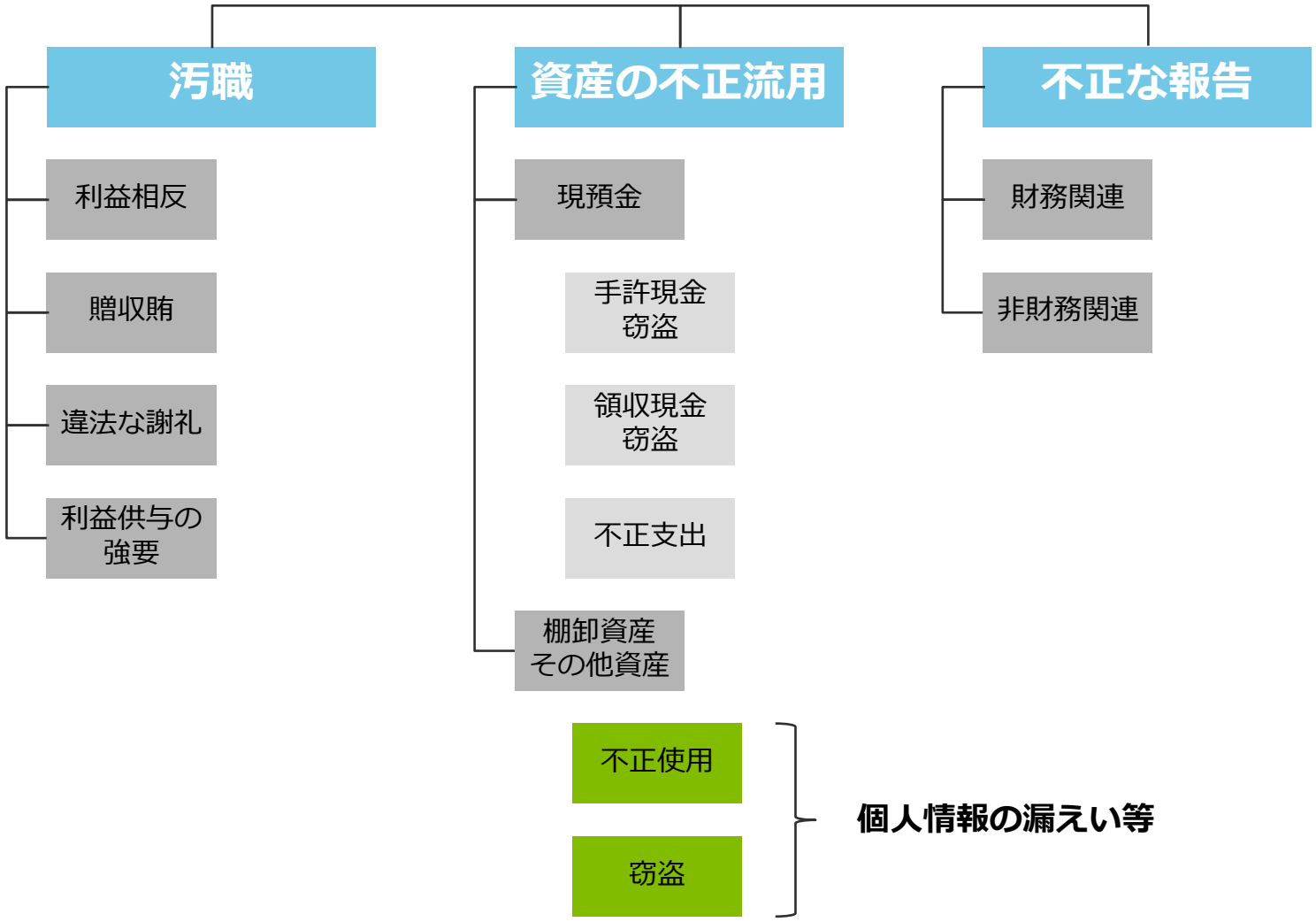


【参考】セキュリティ対策は単純ではありません



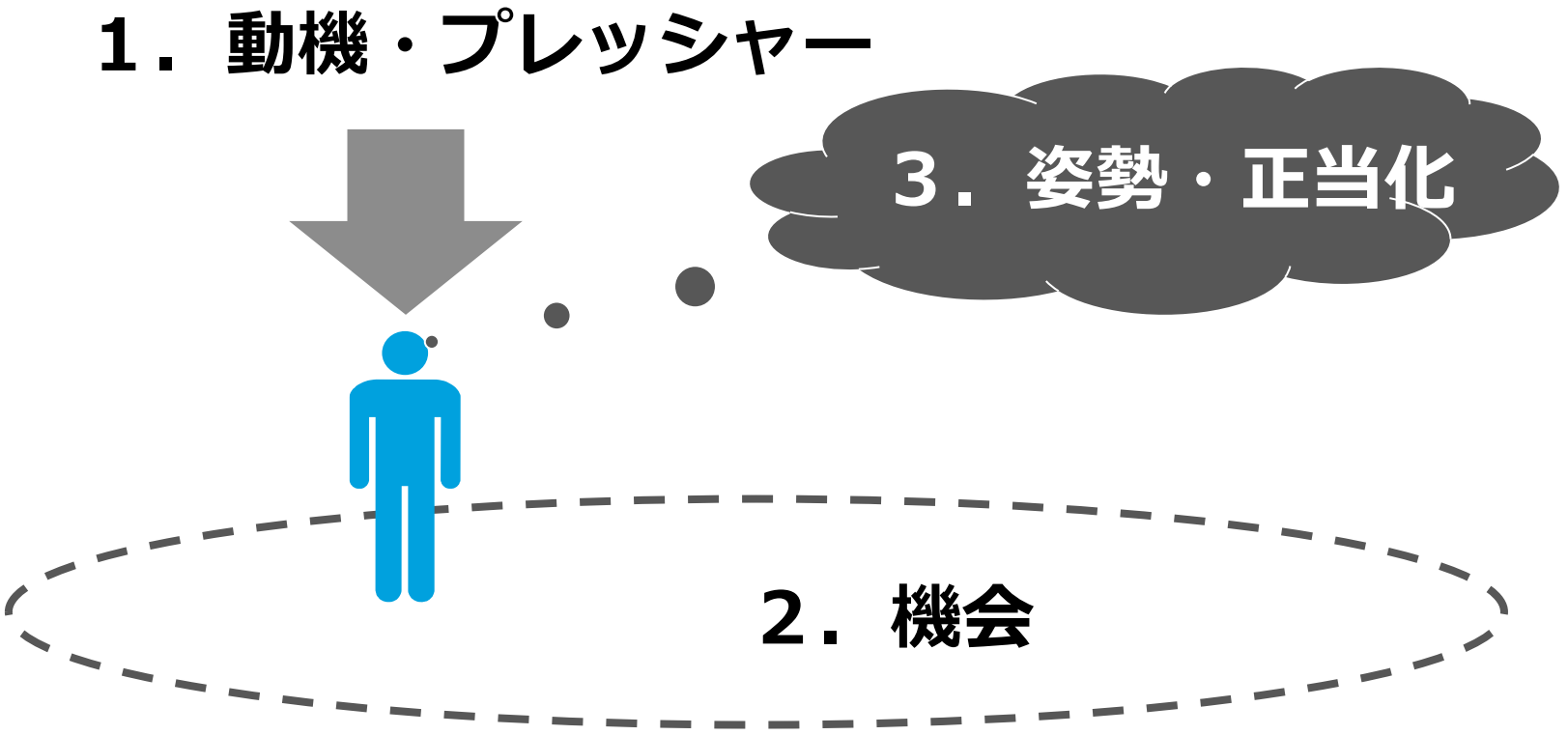
不正対策手法から学ぶ情報保護

個人情報の漏えいと不正の分類



内部犯行対策には不正のトライアングルの理解が重要です

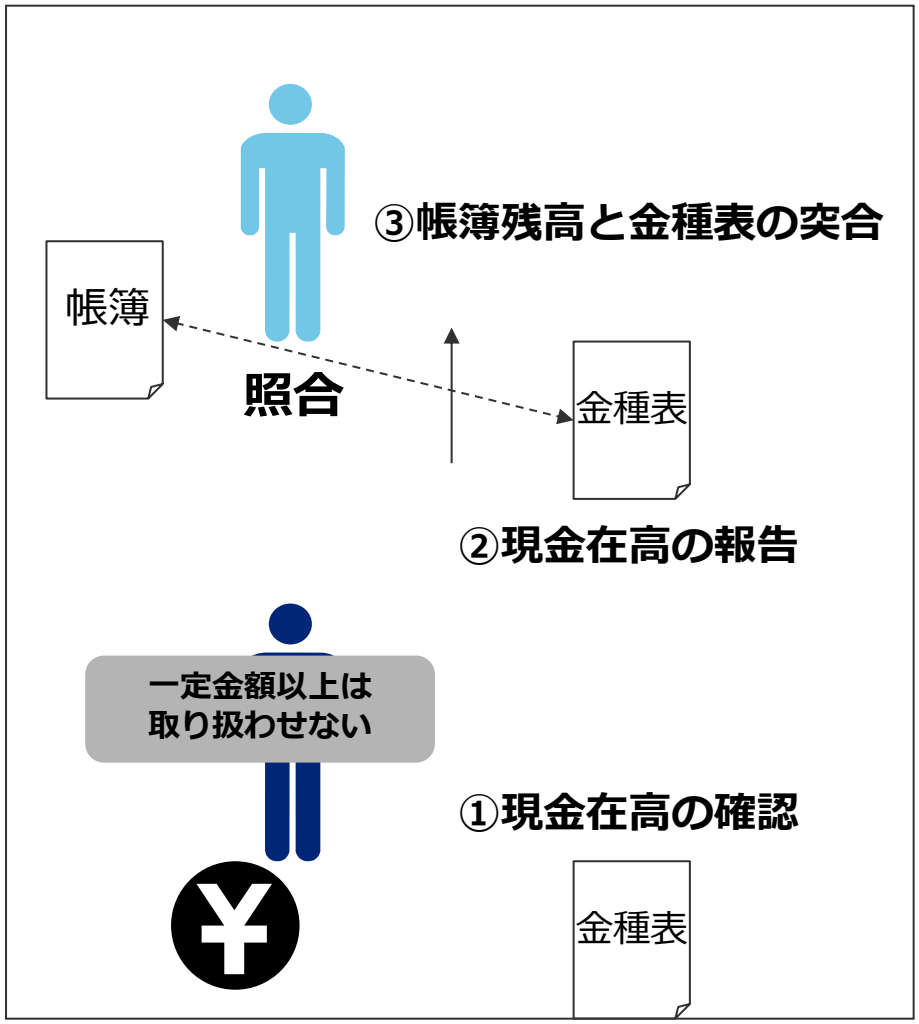
不正の要因を減少させる対策が必要です

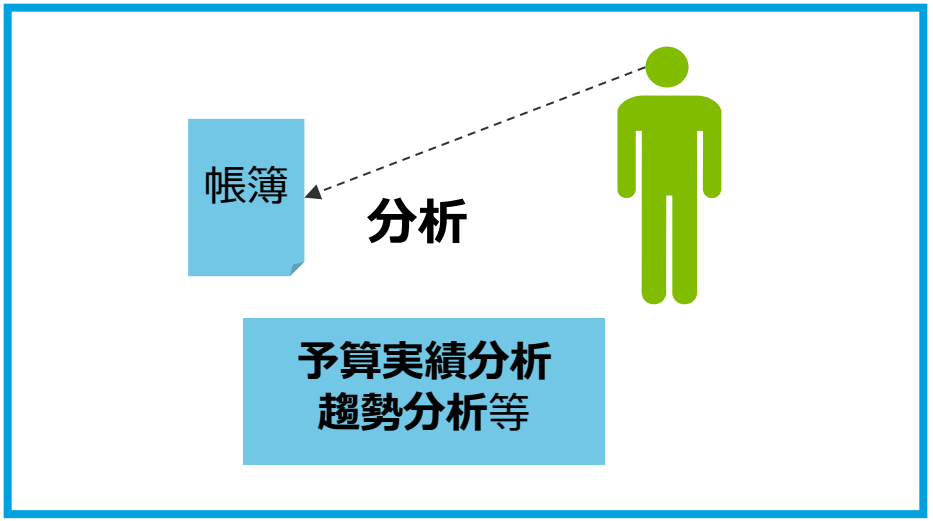


不正のトライアングルをよく理解しましょう

現金管理と同じ枠組みで情報管理を考えてみたらどうだろう

現金管理

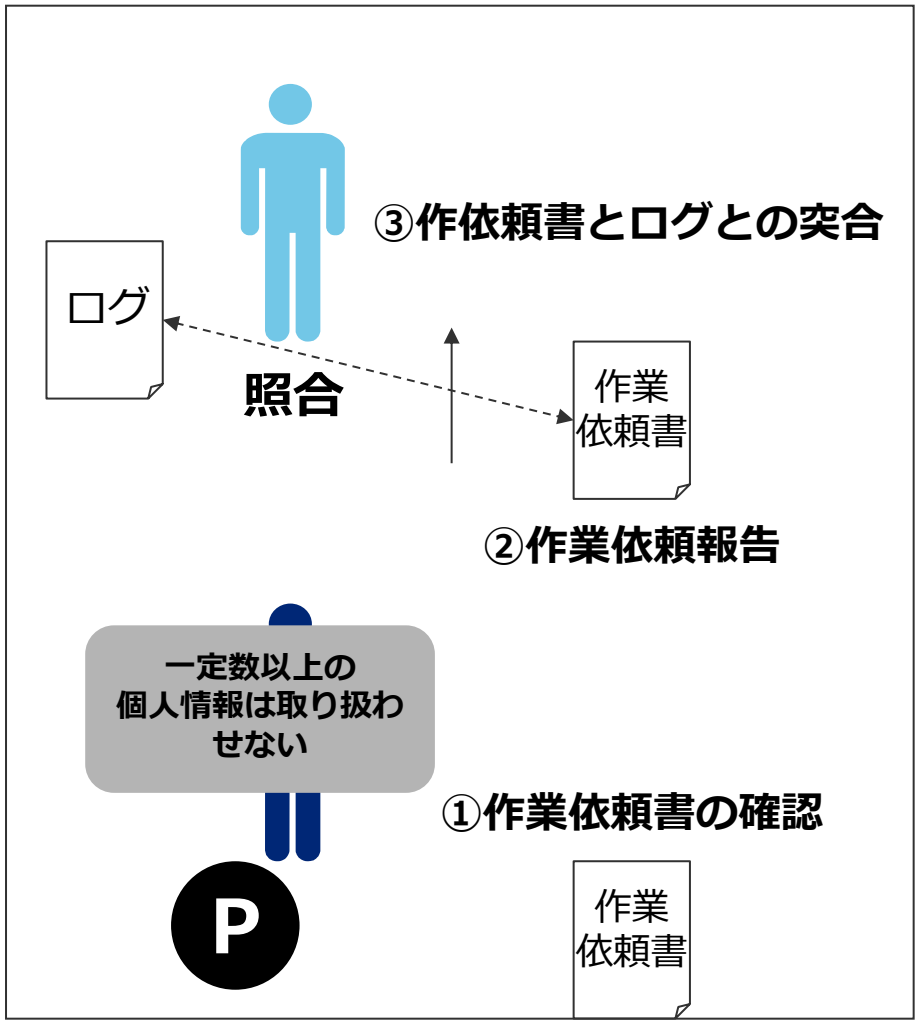


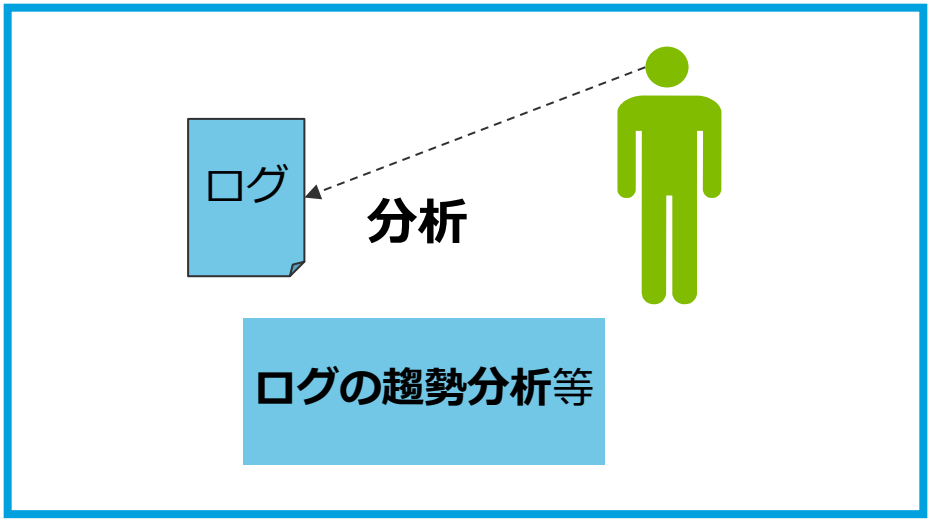


1. 現金の上限金額を定める
2. 現金出納と帳簿をつける人を分ける
3. 現金残高と帳簿残高の一致を上長が確認する
4. 残高の推移等をレビューする人を設置する
5. 内部監査等の第三者の確認をいれる

現金管理と同じ枠組みで情報管理を考えてみたらどうだろう

個人情報管理

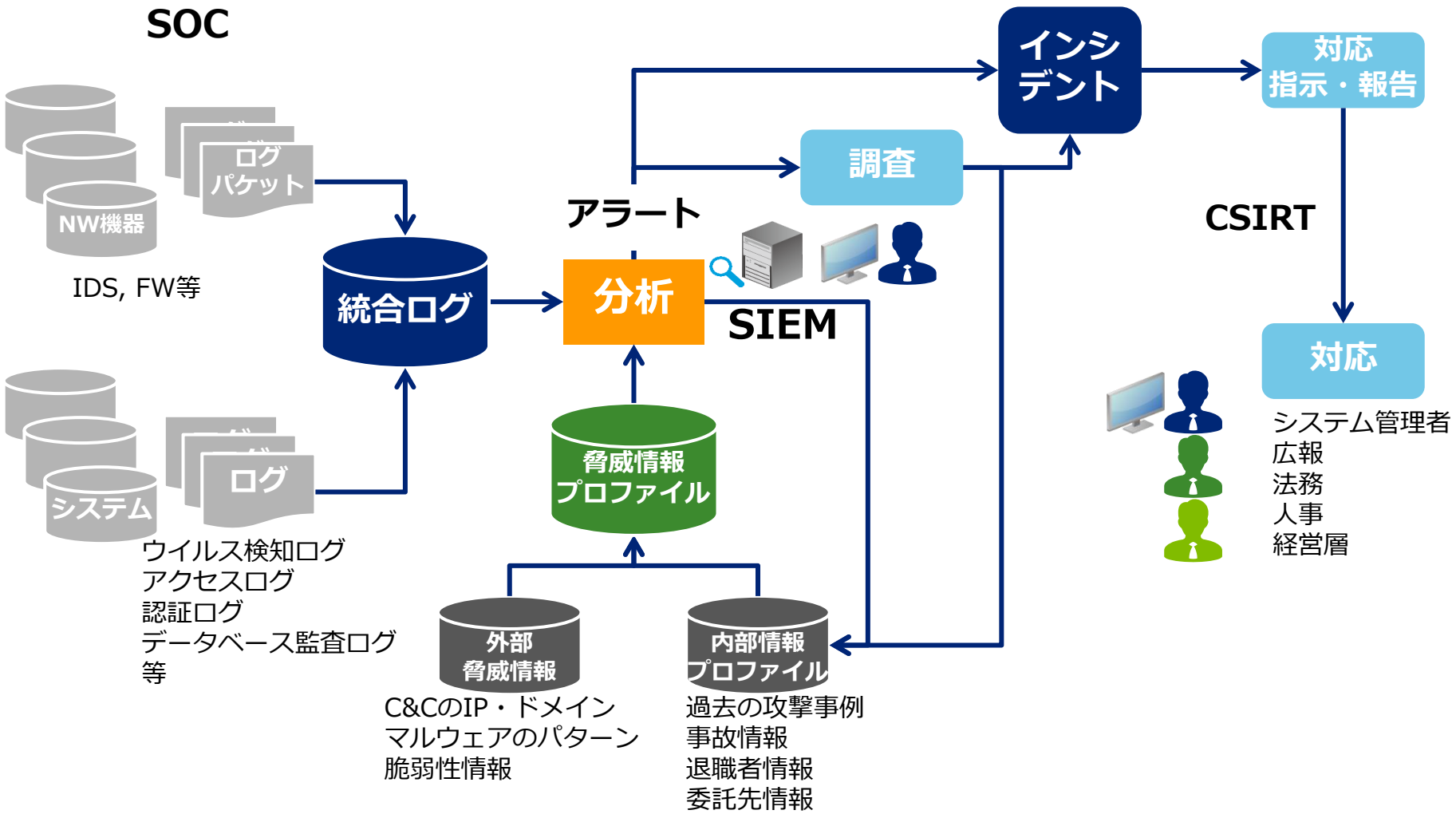




1. 取り扱える個人情報の上限数を定める
2. 個人情報を取り扱う者とログ管理者を分ける
3. 作業依頼書とログの一致を上長が確認する
4. ログをレビューする人を設置する
5. 内部監査等の第三者の確認をいれる

発見をして対応をすることが重要です

SOCとCSIRTの構築がポイントになります



正社員とそれ以外を分けるもの（抑止の観点から）

退職金が人質である説

社歴が長いほうが組織への帰属意識が高く、忠誠心が高まり、不正を働きにくいということは考えられる。

正社員は、つつがなく勤めていれば

- 後年になるほど給与が高くなる
- 最後には退職金（給与の後払い）が支払われる

であれば、少しの不正を働くよりも、まじめに勤めるほうが、経済的に得である。

忠誠心というような、不確かなものに依存することはできるのか？

退職金制度といったようなものが、抑止になっている可能性はある。

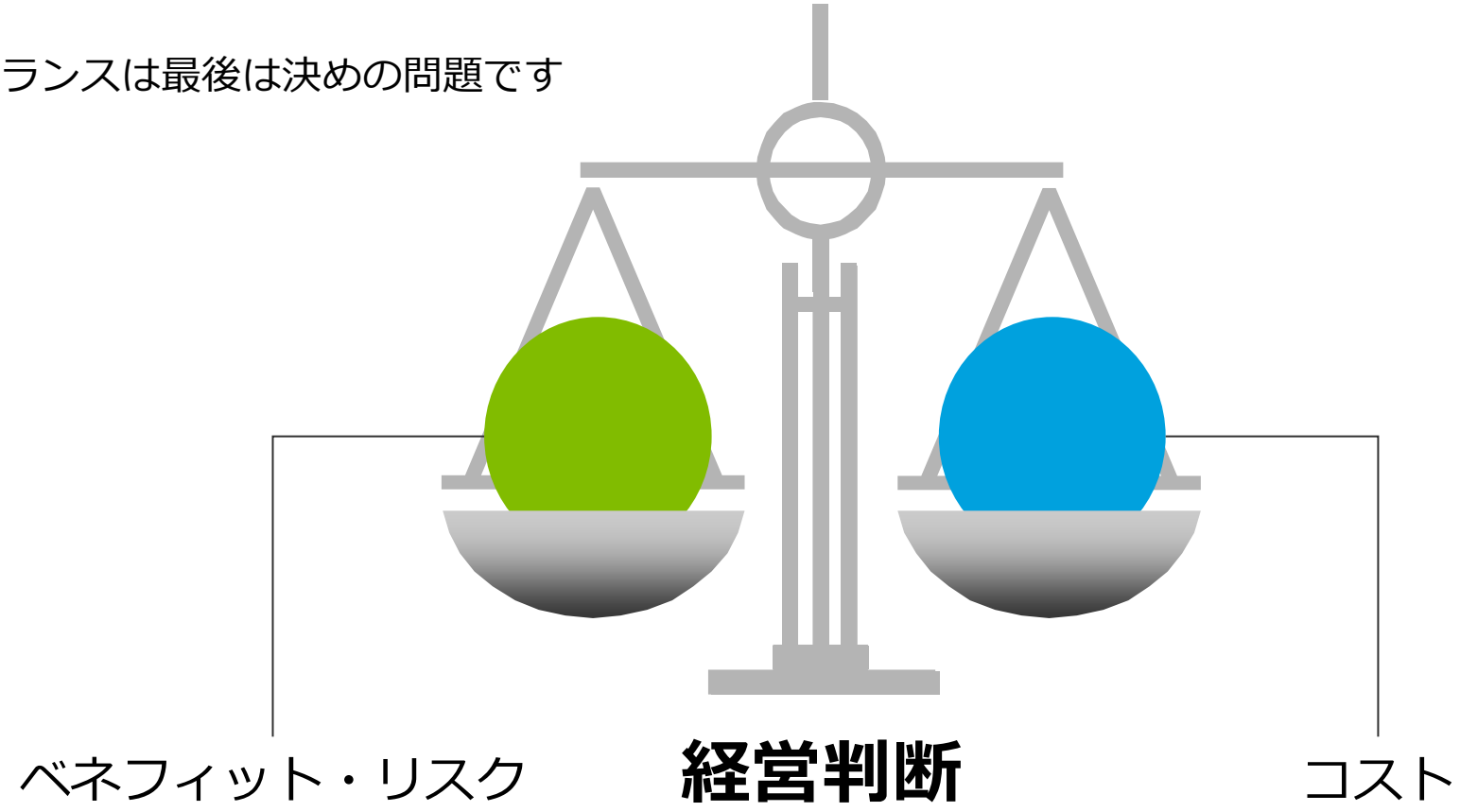
しかし、今の労働環境はどうであろうか？

論理的な思考で不正対策を考えることが重要である

どこまで不正対策をするかは
経営判断

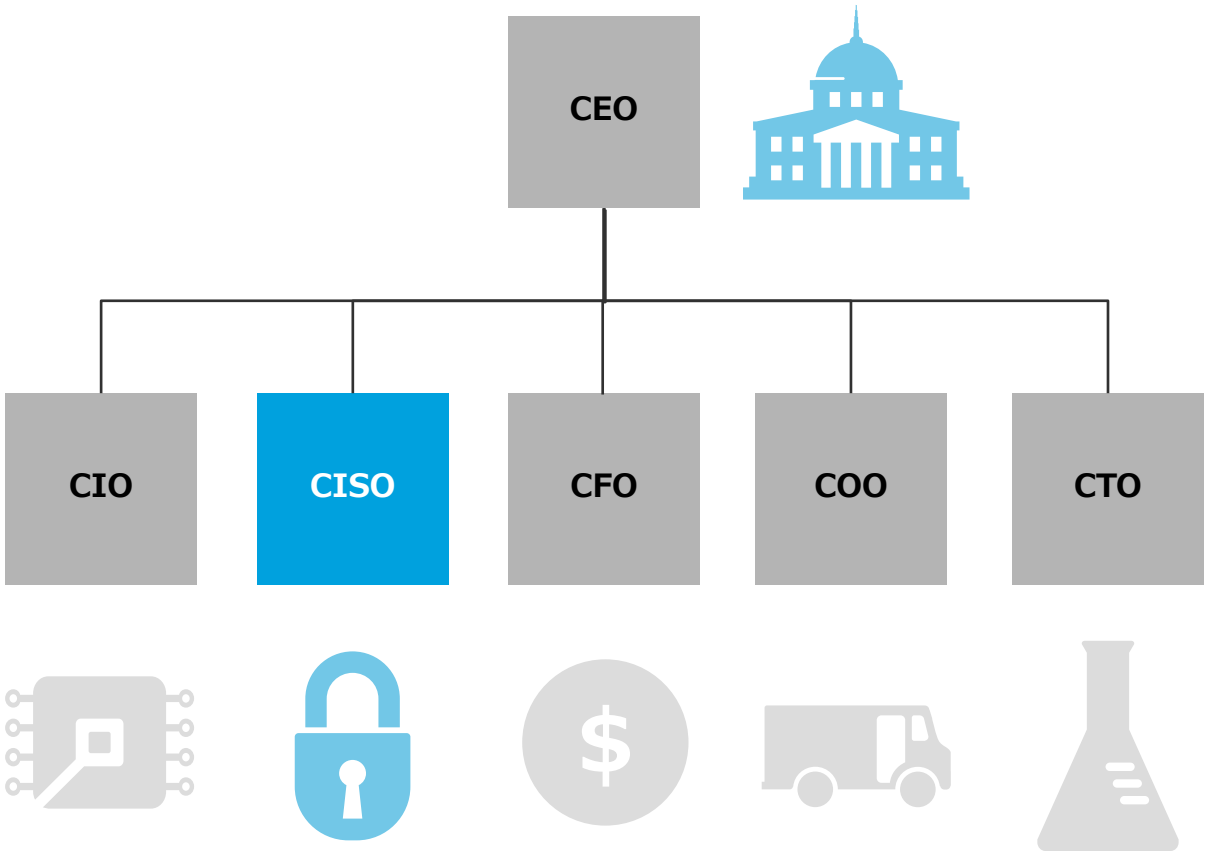
どこまでコストをかけてリスクを引き下げるかは経営判断です

バランスは最後は決めの問題です



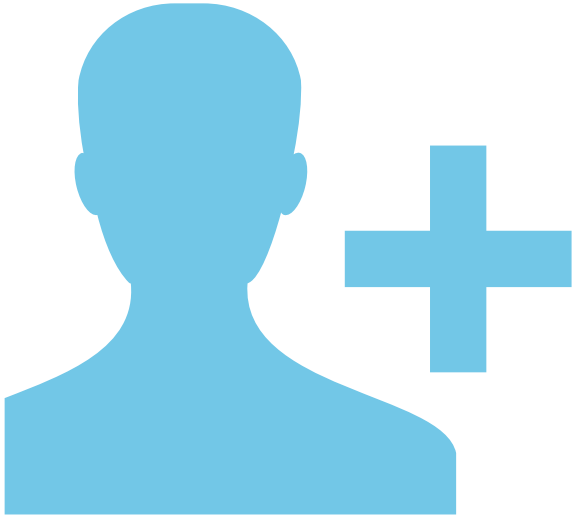
現場に任せても会社全体の最適解は導き出されません

経営者にセキュリティの判断ができる人（CISO）が必要です



問題はCISOをどのように育成するのか？

WHO?



Deloitte. トーマツ.

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およびそれらの関係会社（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング株式会社、デロイト トーマツ ファイナンシャルアドバイザリー株式会社および税理士法人トーマツを含む）の総称です。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、各社がそれぞれの適用法令に従い、監査、税務、コンサルティング、ファイナンシャルアドバイザリー等を提供しています。また、国内約40都市に約7,600名の専門家（公認会計士、税理士、コンサルタントなど）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。詳細はトーマツグループWebサイト（www.tohmatsu.com）をご覧ください。

Deloitte（デロイト）は監査、税務、コンサルティングおよびファイナンシャル アドバイザリーサービスをさまざまな業種にわたる上場・非上場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提供しています。デロイトの約200,000名を超える人材は、“standard of excellence”となることを目指しています。

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。DTTLおよびそのメンバーファームについての詳細は www.tohmatsu.com/deloitte/ をご覧ください。

Member of
Deloitte Touche Tohmatsu Limited