ITで実現するガバナンスとセキュリティ

齊藤愼仁

自己紹介

齊藤 慎仁 さいとう しんじ

株式会社クラウドネイティブ
代表取締役社長

文部科学省 最高情報セキュリティアドバイザー

取得経験のある認証

- ISO:20000 ITSMS
- ISO:27001 ISMS
- ISO:27017 クラウドセキュリティ
- PCIDSS レベル1 継続監査
- SOC2 セキュリティ及び可用性
- AWS独自監査
- 取引先及び当局からの監査
- 上場前監査におけるITアプローチ
- エンタープライズJSOX監査
- プライバシーマーク

目次

ITで実現するガバナンスとセキュリティ

1. 最近のセキュリティ情勢について

なくならない内部不正と止まらない攻撃

ＮＴＴ西日本子会社の個人情報流出、元派遣社員の６０代男を逮捕

https://www.yomiuri.co.jp/national/20240131-OYT1T50082/

900万件の個人情報/59組織/一部クレジットカード情報を含む。10年近い期間。買取業者から1,000万円を超える金銭授受の疑い。

バンナムHD、6億円着服の元社員を提訴　スマホ転売で

https://www.nikkei.com/article/DGXZQOUC1891F0Y3A110C2000000/

子会社が保有するタブレット端末やスマートフォンなどのモバイル端末を、都内の中古端末販売店などに持ち込み、6億円の売却益を得ていた。

名古屋港システム停止、脆弱なＶＰＮ狙われたか

https://www.yomiuri.co.jp/national/20230727-OYT1T50215/

復旧を急ぐあまり、証拠保全ができなかったため原因不明。VPN機器の脆弱性を悪用したと考えられている。ロシアのハッカー集団が関わっているとみられている。

大手外資系保険会社から20万件の個人情報の流出

https://www.zurich.co.jp/customerdata/
https://www.aflac.co.jp/news_pdf/2023011001.pdf

業務委託先の両社の顧客情報の保存されていたサーバーを「適切なセキュリティ対策を講じない状態」で設置したことで、不正アクセスを許したと公表されている。

短縮URLサービスに悪質な広告が表示される

https://piyolog.hatenadiary.jp/entry/2023/02/27/014257

企業や大学の配布物に掲載された短縮URLのリンク先に、悪質なサイトへ誘導する広告が配信される。

-
-
-

目次

ITで実現するガバナンスとセキュリティ

2.ゼロトラストによるセキュリティの取組

インシデントはなぜ起こるのか？

事故の発生

脅威 ✖ **脆弱性**

脅威は外部にあるため
コントロールできず、抑制は難しい。
ゼロにすることはできない。(抑止)

脆弱性は組織の内部にあるため
コントロール可能。

セキュリティ対策

脆弱性をコントロールすることを
セキュリティと呼ぶ（防止）

コスト

セキュリティ対策にはコストが発生するため、
費用対効果を考慮する必要がある。

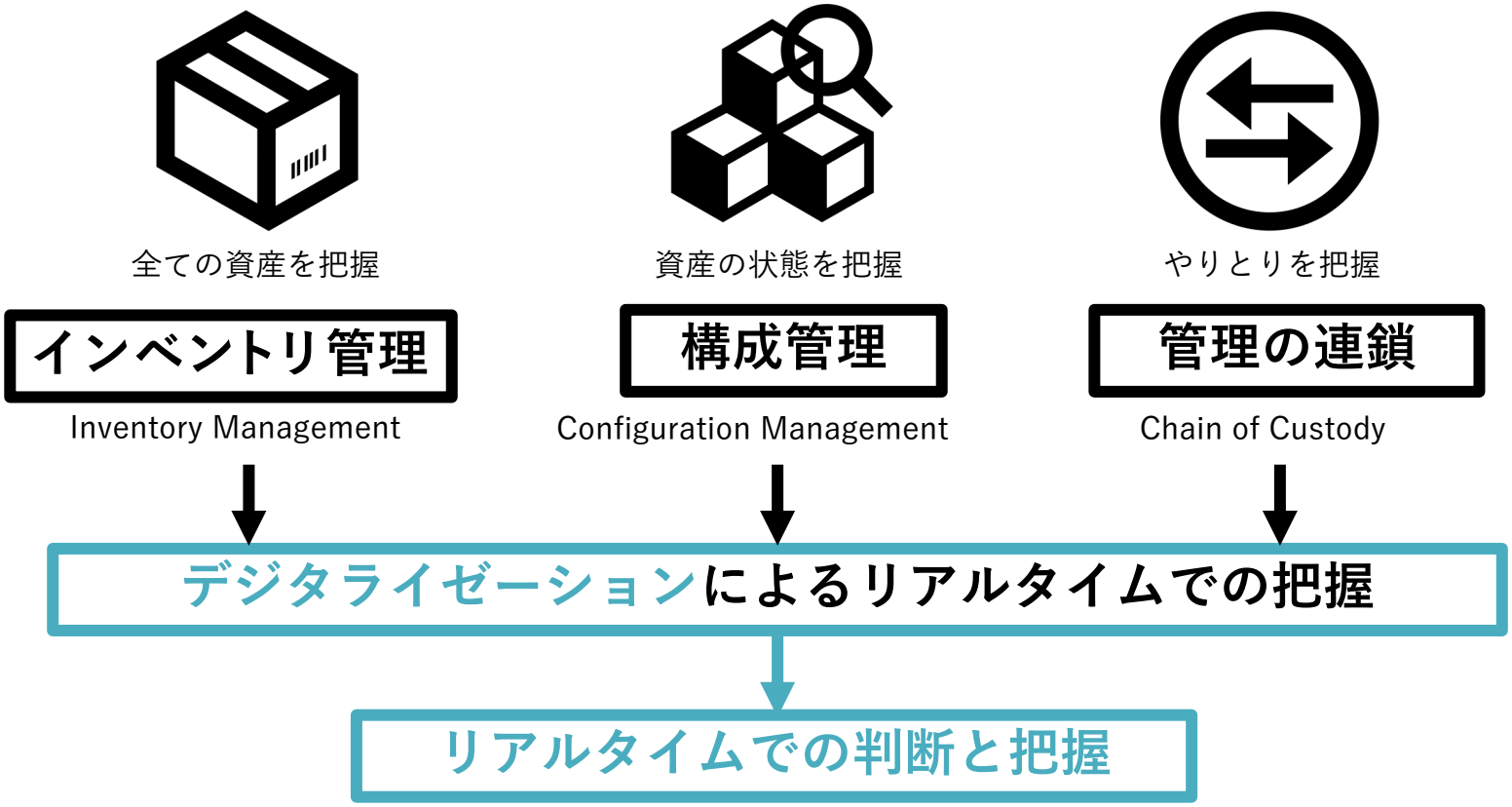
いつでも脆弱性のない状態を作る

サイバーハイジーン

資産をすべて管理し
その状態を把握することで
期待された状態を維持する

2.ゼロトラストによるセキュリティの取組

サイバーハイジーンの維持にはすべての資産の把握が必要



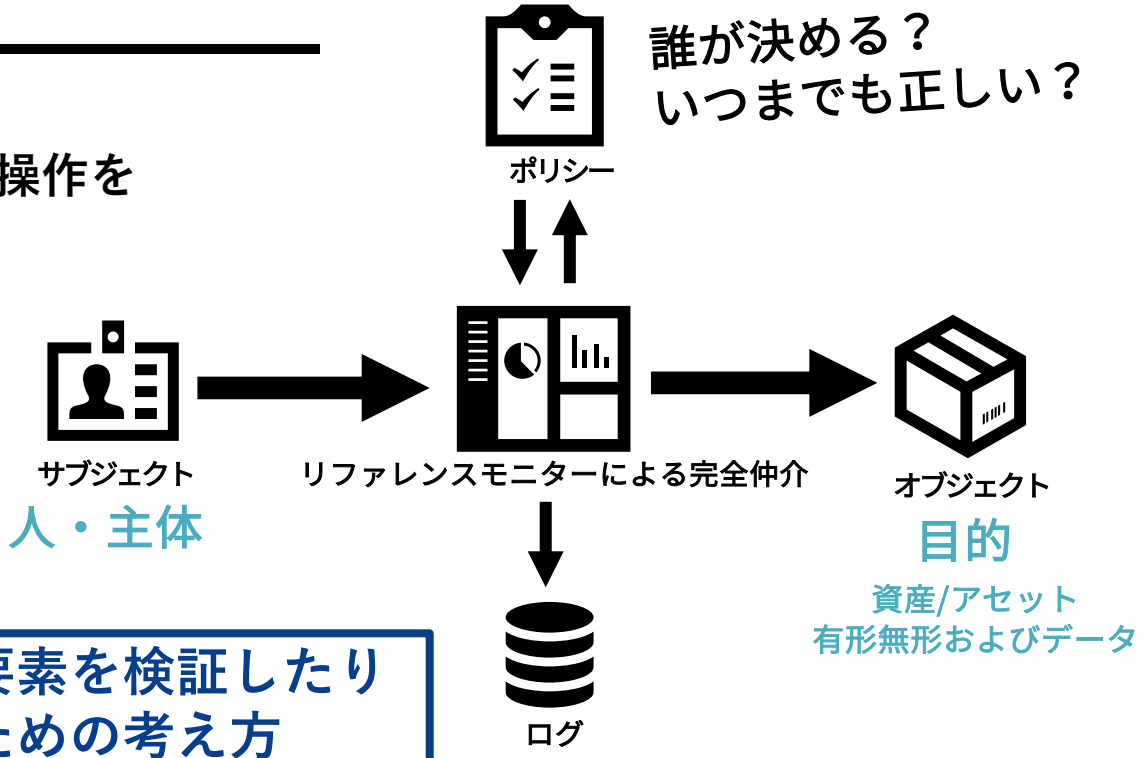
2.ゼロトラストによるセキュリティの取組

すべての通信をポリシーによって判断する

ポリシーとは？

誰かがなにかをするときに、させる/させないを
決めるルール/規定。やりたいこと。

すべての資産を把握・維持し
その資産への通信/アクセス/操作を
認可（判断）するポリシーを
適切に保つことが必要。



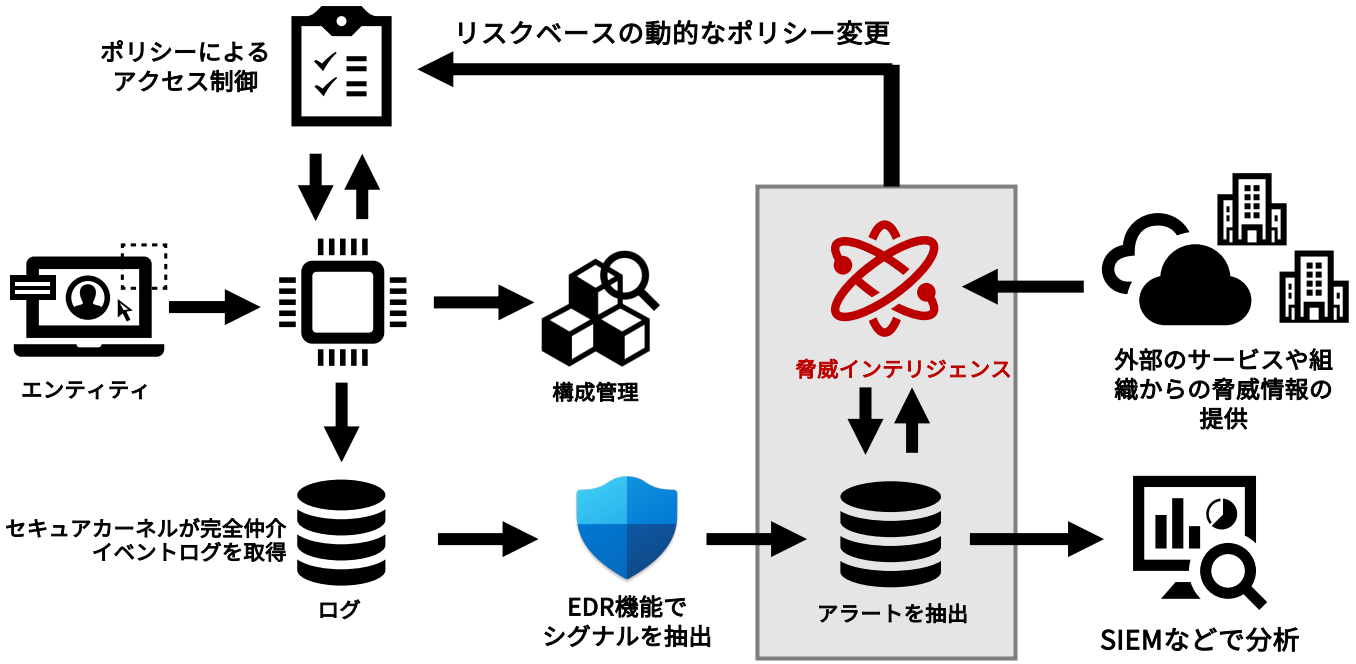
**ゼロトラストはこれら各要素を検証したり
適切に変更して信頼するための考え方**

2.ゼロトラストによるセキュリティの取組

ITで実態の把握と適切な判断を仕組み化する

実リスクに応じてリアルタイムにポリシーを変更する仕組み（例）

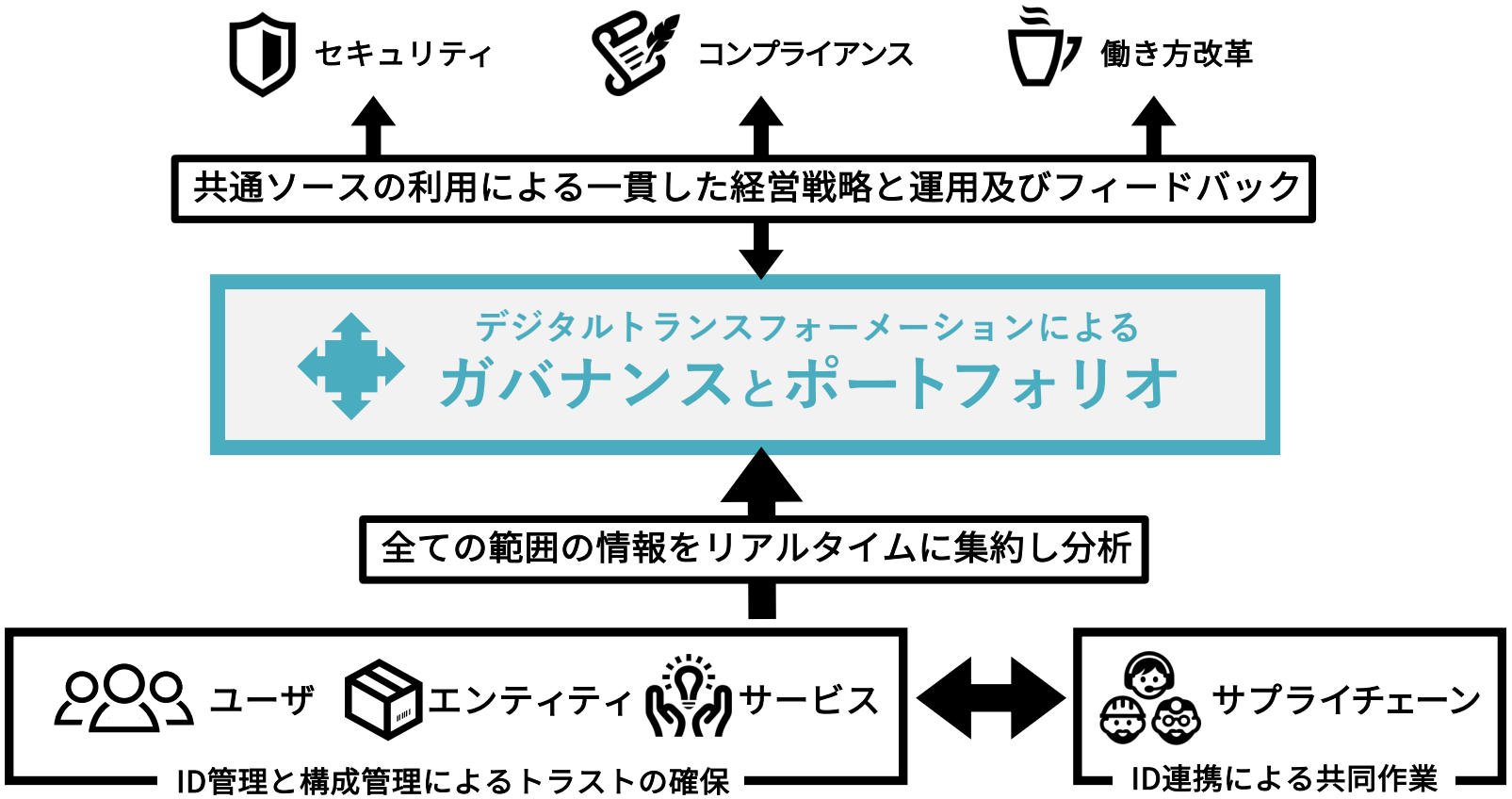
「今」世界中で起こっているインシデントの実態を収集し
どのようなポリシーにすべきかを適切に判断できる仕組み



Dynamic Policy Enforcement

2.ゼロトラストによるセキュリティの取組

組織運営の実態に即した情報を集め適切な経営判断をす

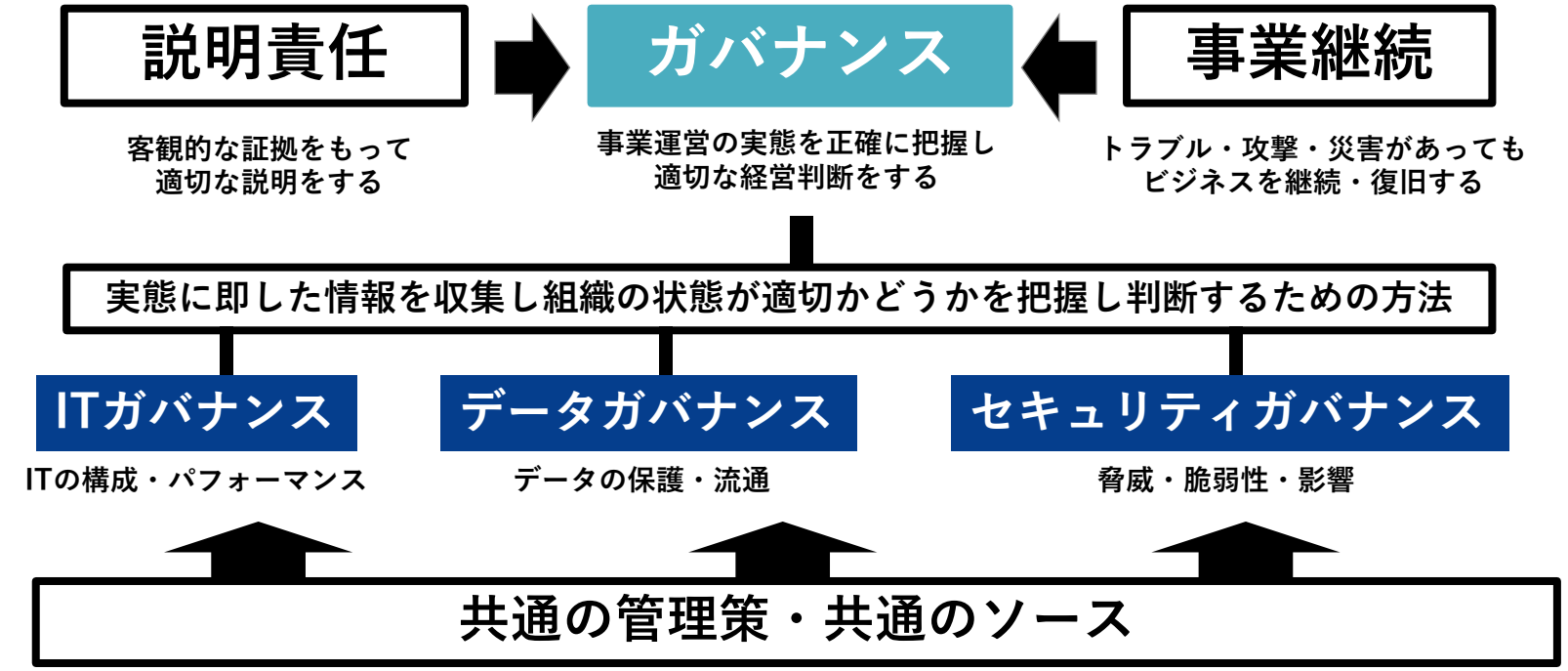


目次

ITで実現するガバナンスとセキュリティ

3. ガバナンスとセキュリティ監査の関係

ガバナンスのために必要なのは実態を把握する方法

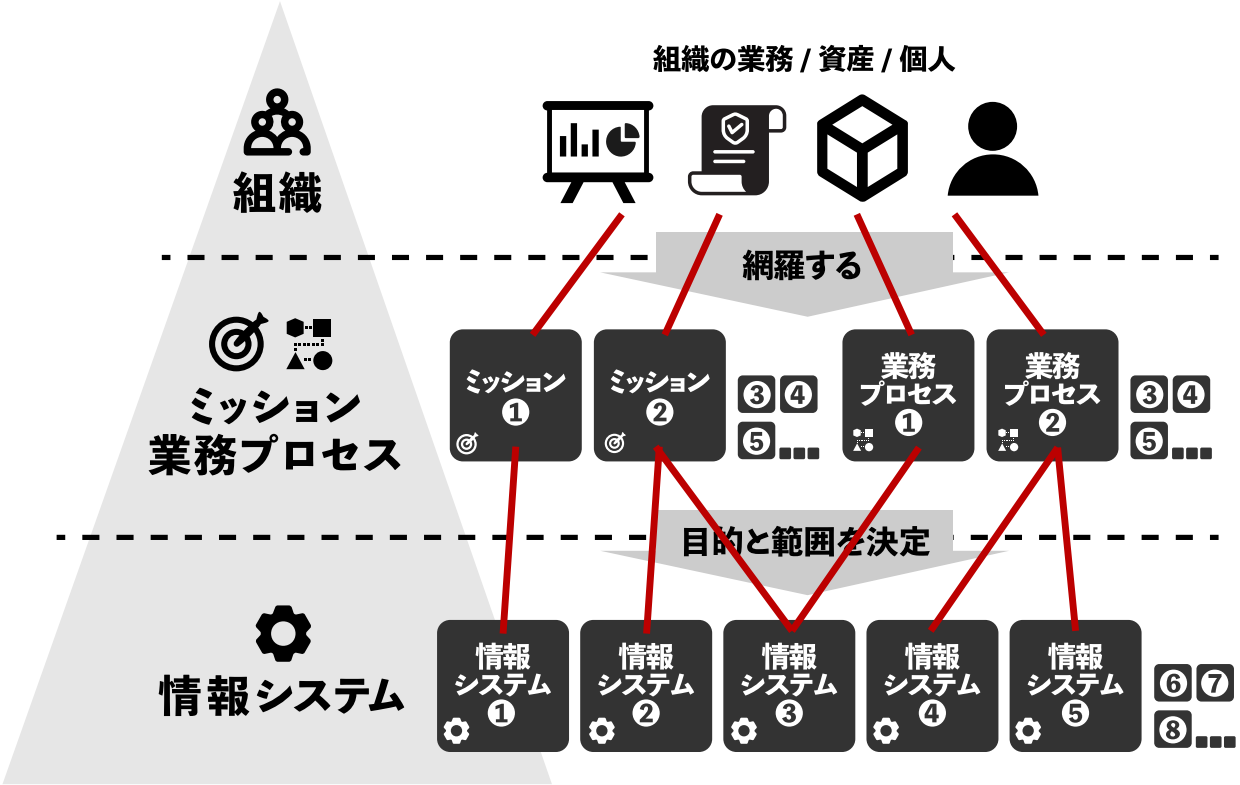


終わらない攻撃や社会環境の変化があったとしても、ガバナンスのために必要な情報を入手するためのIT環境

3. ガバナンスとセキュリティ監査の関係

組織の実態とそのリスクを把握し明らかにする

相互にかかわる見落としがちなリスク



引用： NIST Special Publication 800-30 Revision 1 リスクアセスメントの手引き

3. ガバナンスとセキュリティ監査の関係

その方法としてのセキュリティ監査

ただしインシデントの前か後かでなくどちらも準備は必要

3. ガバナンスとセキュリティ監査の関係

ペネトレーションテスト

テストで自組織のITインフラを把握する

自組織のシステムや資産を把握することからはじめる

① 内部/外部向けシステムの情報収集
② テストの計画・準備（範囲/環境）
③ テストの実行
④ レポート
⑤ 対応

テストの種類

- 侵入テスト
- Red/Blue/Purple Team テスト
- ネットワーク負荷テスト
- DDoS シミュレーションテスト
- フィッシングシミュレーションテスト
- マルウェアテスト など

システムを刷新することはすぐには難しい
まずは自組織のシステムの脆弱な箇所を知り
リスクを特定（把握）する

3. ガバナンスとセキュリティ監査の関係

説明責任とは？目指すべきポイント

経営者が株主や投資家に対して、企業の経営状態や財務内容を報告する義務

企業から他の利害関係者に状況を説明する責任

- ✓ ITインフラを自組織で把握している
- ✓ どのような仕組みでITガバナンスができているのかを説明できる
- ✓ 定期的な見直しとテスト/改善を行っている
- ✓ インシデントの詳細を調査/説明できる準備をしている
- ✓ ステークホルダーへ連絡・通知する手順がある
- ✓ 改善策を提示し実行できる

アカウンタビリティとは、会計Accountingと責任Responsibilityの合成語。経営者が株主などの出資者や債権者に対して、資金の使い途を説明する「会計説明責任」のこと。最近は会計だけでなく、企業（経営者）が負う説明責任全般を指すことが多い。

完