事例から考える、IT内部不正の現状と対応

白濱 直哉

2015年5月22日

サイバーリスクに関する豊富な経験があります

自己紹介

監査法人系 リスクコンサルティング会社 シニアマネジャー
東京電機大学 国際化サイバーセキュリティ学特別コース　外部講師

大手情報セキュリティ会社を経て、監査法人系のリスクコンサルティング会社に入社。
大学を卒業して17年間、一貫してサイバーセキュリティ関連のコンサルティング業務に携わる。
現在は、様々な業種に対して、技術的なセキュリティ対策支援やインシデント対応、組織の事業継続やレギュレーション対応という観点からのサイバーリスク対応支援を行っている。

■ 内部不正関連の業務経験

- 不正アクセスや情報漏洩調査
- eDiscovery支援
- 不正会計、インサイダー、反社取引（データ保全や分析等、IT調査の支援）

本資料および講演内容の意見に関する部分は私見であり、所属する法人の公式見解ではありません。

アジェンダ

- はじめに
- 内部不正とは
- 不正の事例と対策
- 対策のまとめ
- 不正発生時の対応（少しだけ）

はじめに

不正が発生する会社ってどんなんなんでしょう

本日お話したいこと

1. 公開されている内部不正は氷山の一角
2. 誰もが不正行為者になりうる
   しかし、簡単に防げる内部不正はごまんとある
3. 本気の内部不正に対する対策は非常に困難
   発見する仕組みが重要

内部不正は対岸の火事か

内部不正対策を阻害する組織の認識

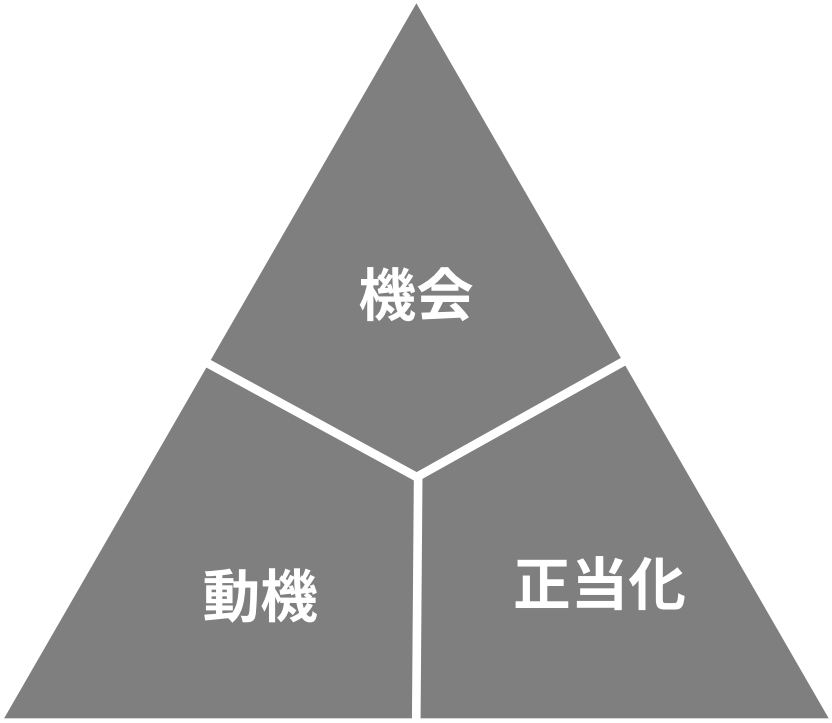
不正を行う職員はいない	不正が発生した組織でさえ、「みなショックを受け心を痛めている。同様のことを起こなさないと全員から一筆もらったので大丈夫」との認識。
漏洩して困る情報はない	組織として活動をしているのであれば、必ず何かしらの価値ある情報があるはずです。また、組織に対する活動妨害を目的に不正を行う可能性もあります。
対策は万全である	内部不正対策はその特徴から、標的型攻撃よりも対策も発見も困難と言えます。実効性のある対策が行われているか、内部に攻撃者がいるという前提で確認することが重要です。

このような認識の組織が多いのが現実

内部不正とは

なぜ、不正が発生するのか

不正発生の要因となる３要素



不正のトライアングル

機会

不正が可能な環境
- 内部統制の不備、形骸化
- 権限管理の不備
- システムの脆弱性、未監視

動機

不正を働くきっかけ
- 個人的な経済問題
- プレッシャー
- 待遇への不満

正当化

不正を正当化する理由
- 会社が悪い
- みんなやってる
- バレない、お金は返す

「内部不正」の「内部」の定義はさまざまあります・・

内部の定義

内部

- ■ 物理セキュリティの内側へ立ち入る、テンポラリでない権限を有する人
- ■ 一般公開していない情報システムにIPリーチャブルな、テンポラリでない権限を有する人

→
- ✓ 役職員
- ✓ 常駐しているシステム開発や運用等の人
- ✓ 派遣社員 等

その他

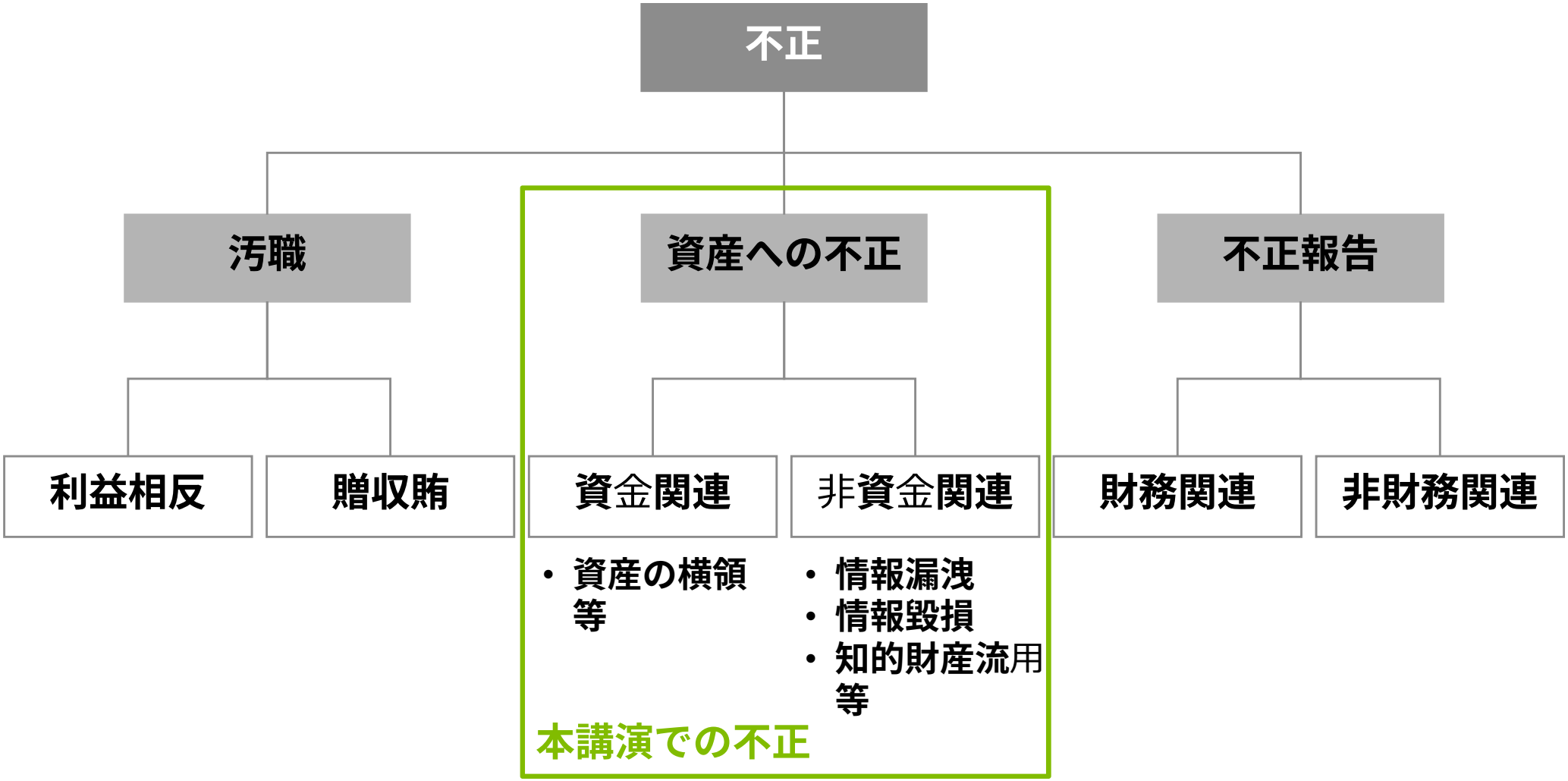
- ■ 上記以外

→
- ✓ 組織と契約関係のない、第三者
- ✓ テンポラリで入室する業者
- ✓ 過去に契約があった者（退職者等） 等

特定のシステムや情報へのアクセス権は無関係

不正といってもいろいろあります・・

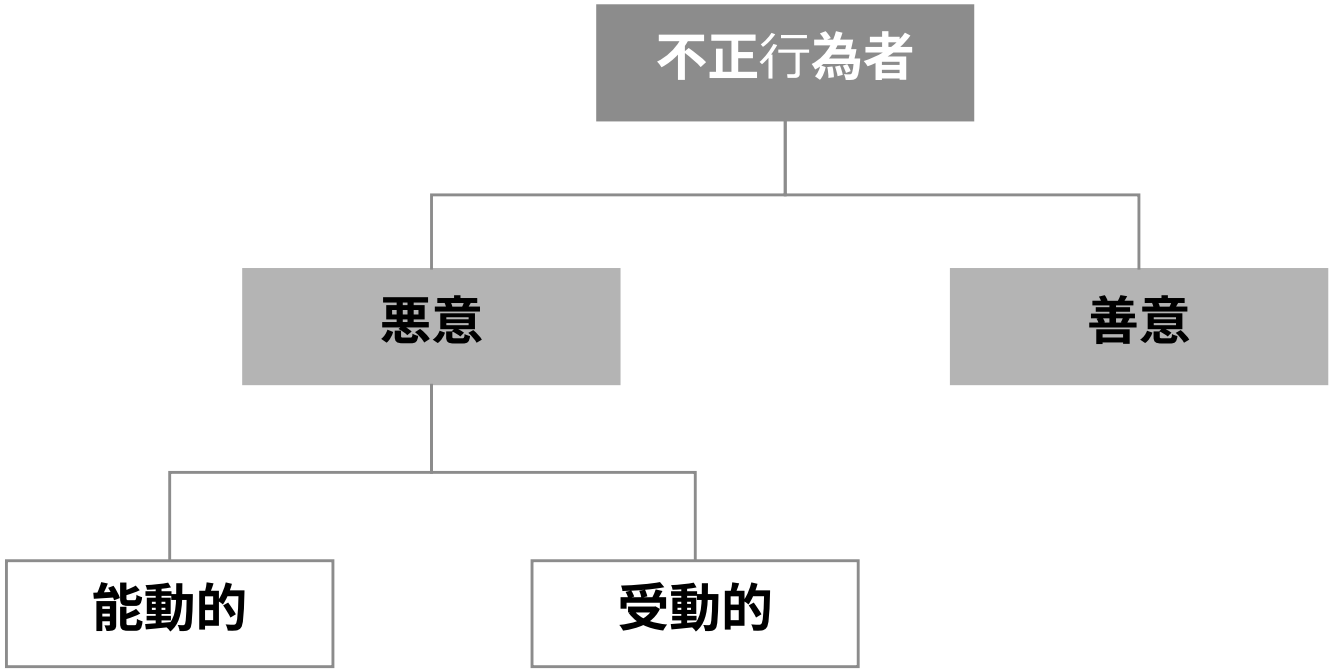
不正の分類



参考：日本公認会計士協会「不正調査ガイドライン」
ACFE 「2012年度版　職業上の不正と濫用に関する国民への報告書」 職業上の不正と濫用　不正の体系図

不正を行う人もいろいろあります・・

不正行為者の分類（検討中）



本講演では、

IT内部不正の定義

- ✓ 組織内の情報システムにIPリーチャブルな者が、
- ✓ 契約期間中に、
- ✓ 情報・情報システム資産に対して、
- ✓ 故意に、
- ✓ 法令・コンプライアンス違反を行う

こと。

タイプ別の事例と対策

根っからの悪者が犯す不正は全体の30%弱！？（白浜調べ）

タイプ別不正行為者の概要

	概要	割合
① 善意の不正行為者	■ 「悪いこと」「不正である」という認識がない状態で、不正を実行する者 ■ 「良いことをしている」と思っている人もいる	10%弱
② 悪意のある、受動的不正行為者	■ 「機会」を認識したがために、「動機」や「正当性」が生まれ、不正を実行する者 ■ 「悪いこと」「不正である」という認識はある	60%強
③ 悪意のある、能動的不正行為者	■ 「動機」を満たすために、積極的に「機会」を探し、不正を実行する者 ■ 「正当性」による歯止めは利かない	30%弱

不正の認識がない行為でも内部不正に該当するケースがあります

① 善意の不正行為者の事例

出向職員による出向元への情報漏洩

■ 概要

親会社に出向した子会社職員が、親会社の営業秘密を子会社の上司にメールで送信していた。

過去何年にもわたって慣例的に行われていた行為であり、出向者は前任の担当者から引継ぎ、当たり前のこととして行っていた。

■ 発見の経緯

メールログの分析

機会	情報へのアクセスやメール送信が可能であり、監視も行われていない
動機	情報を送るものだと思っていた（指示されていた）
正当化	正当化の必要はない（契約違反の認識がない）

「悪意がなければ問題がない」と思い実行するケースがあります

① 善意の不正行為者の事例

自宅に送信したクライアントの情報が漏洩

■ 概要

システム開発を請け負う会社の職員が、自宅で作業をするため、クライアントから受領した情報等を自宅に送信し、送信した情報が漏洩した。

■ 発見の経緯

クライアントがプロジェクト名でWeb検索

機会	情報へのアクセスやメール送信が可能であり、監視も行われていない
動機	自宅で仕事がしたかった （高評価がもらいたかった）
正当化	人一倍ガンバっているのだから、問題ではない

いますぐ出来る対策で、内部不正が10%減るかもしれません

① 善意の不正行為者の対策

機会	情報へのアクセスやメール送信が可能であり、監視も行われていない	■ 適切な内部統制の構築 （リスク分析等を行い、どこにどのようなリスクが潜在し、どのような影響可能性があるか認識し、対策する）
動機	■ 情報を送るものだと思っていた ■ 自宅で仕事がしたかった	■ 情報取扱ルールや契約、コンプライアンスの再確認・教育 ■ 事例等による教育
正当化	■ 正当化の必要はない ■ 人一倍ガンバっているのだから、問題ではない	■ 倫理教育

悪意のない不正行為者には、教育が効果的

内部統制の不備が不正の動機の引き金になるケースは多いです

② 受動的な不正行為者の事例

残業データを変更し、自身の給与を増額

■ 概要

人事部給与担当者が、毎月集計される残業時間数が入った残業データファイルを書き換え、残業手当を横領した。

業務手続およびシステム権限管理（内部統制）の不備であり、本人は結婚を控えており、内部統制に不備がなければ一生このようなことはしなかった可能性もある。

■ 発見の経緯

給与計算をしている委託先の直感

機会	残業データにアクセスができ、誰もチェックしていないことを知っていた
動機	お金が欲しかった
正当化	オレだってガンバってのに、みなの方がもらってる。 絶対バレないし！

適切な内部統制の構築および風通しのよい環境で内部不正の大半はなくなるかもしれません

② 受動的な不正行為者の対策

機会	残業データにアクセスができ、誰もチェックしていないことを知っていた	■ 適切な内部統制の構築 （リスク分析等を行い、どこにどのようなリスクが潜在し、どのような影響可能性があるか認識し、対策する）
動機	お金が欲しかった	■ 情報取扱ルールや契約、コンプライアンスの再確認・教育 ■ 事例等による教育
正当化	オレだってガンバってのに、みなの方がもらってる。 絶対バレないし！	■ 倫理教育

内部不正による情報漏洩も同じです

自己中心的で善悪の区別もつかない人も、世の中にはいます

③ 能動的な不正行為者の事例

退職後に会社のシステムが動かなくなるよう細工

■ 概要

長年システム管理者を兼務していたが、会社でいやなことがあり、退職を決意。

自身が退職後にシステムに不都合が起きるようタイマーを仕込み退職。

■ 発見の経緯

システム障害

機会	会社にITがわかる人がいなくて、自身に権限が集中
動機	憂さ晴らし（仕返し）
正当化	これくらい当然の酬い

悪意をもって能動的に不正を実行する者の対策は困難です

③ 能動的な不正行為者の対策

機会	会社にITがわかる人がいなくて、自身に権限が集中	■ 適切な内部統制の構築 （個人に権限を集中させない。BCPの観点からも、バックアップ体制は必要）
動機	憂さ晴らし（仕返し）	■ 透明性のある人事評価 等 ■ コンプライアンス教育 ■ 社内コミュニケーションの充実
正当化	これくらい当然の酬い	■ 倫理（人間）教育

防げなくても、発見できる仕組みは必須です

対策のまとめ

画期的な対策などないと考え、地道に対応する必要がある

対策のまとめ

1. 教育（主にコンプライアンス系）
2. 内部統制の構築
3. 発見的コントロール

全社員から守る、くらいのつもりで対応する必要がある

守るべき情報資産を明確にし、周辺のリスクを洗い出す

内部統制の構築

APT対策の考え方に似ている

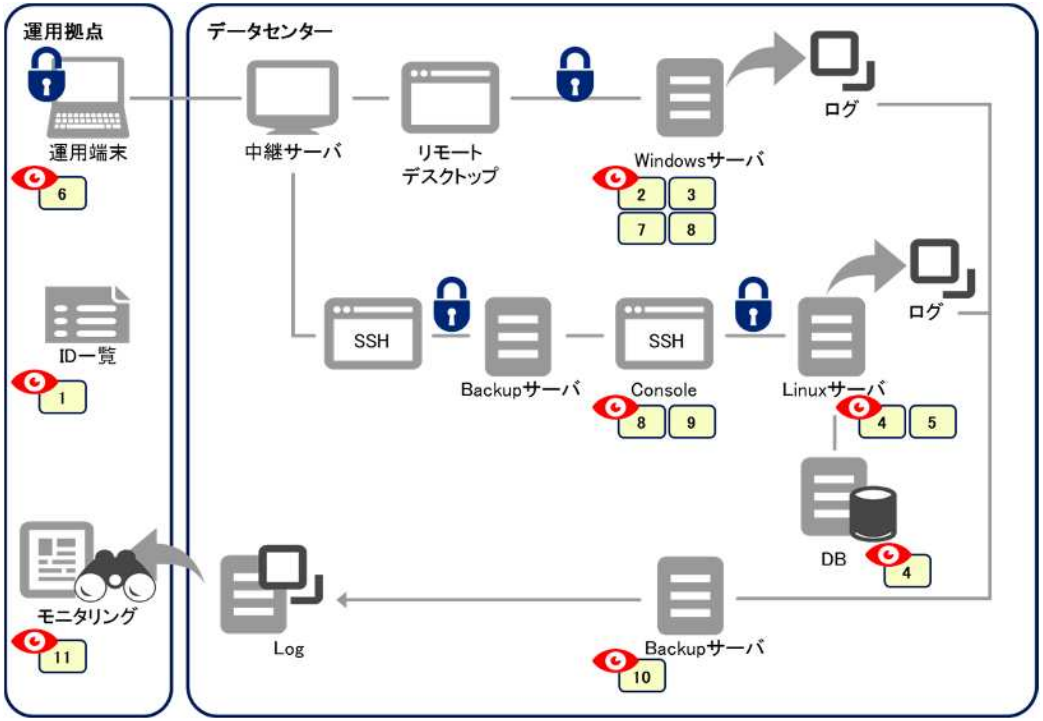
■ 情報漏洩対策

情報のライフサイクルを詳細に分析し、どこにどのようなリスクが潜在するか把握し、対応する。

■ システムの不正利用

システムを把握し、厳格な権限管理を実施する。

システム上のリスクポイント例



発見されることがわかっていて、不正を行う人がどれほどいるか

次世代型モニタリング？の導入

高度な不正アクセスの発見手法と似ている

■ 発見的コントロール

業務アプリケーションのログや電子メールも含めたモニタリングを行うことで、セキュリティインシデントだけではなく業務上の不正等の発見も行う。

参考）内部不正対策状況のチェックリスト

定義と責任の明確化

- ☑ 1. 重要情報の定義及びアクセス権限者が明確化され、管理に関するルールがあるか。
- ☑ 2. 情報の責任者を明確にし、責任者はその責任を認識しているか。

重要情報の所在を明確にし、アクセス権限者を限定

- ☑ 3. 情報のライフサイクルや業務フロー、データフローが管理され、どこにどのような情報が残るのか把握しているか（システムが利用するテンポラリ等を含む）。
- ☑ 4. 重要情報が保存されたサーバ等へのアクセスが、許可されたもの以外から拒否されることを確認しているか。
- ☑ 5. 重要情報へのアクセスを、改竄ができない仕組みで記録し、トレースが可能な状態か。
- ☑ 6. 退職者による不正を想定した退職プロセスが定義され、厳格に運用されているか。

情報の出口を押さえる

- ☑ 7. USBデバイス等、情報システムと物理的・論理的に接続できるものを把握し、媒体・情報の持ち出しを管理しているか。
- ☑ 8. 重要情報が保存されたシステムが物理的に保護されているか。
- ☑ 9. 相互監視やログ確認等により、牽制機能が働く環境になっているか。
- ☑ 10. 「動機」「正当化」を低減させるための教育等の施策を実施しているか。

既存の安全管理措置に対して、実証的検証を含めた再確認が必要

さいごに
（不正発生時の対応の考え方について少し・・）

全員がクライシスと呼ぶなら、それはクライシスです

FOR DISCUSSION DRAFT PURPOSES ONLY

－モーガン・ダウニー、ラサールグローバル

インシデントとクライシス

どのような対応を行うかで、組織のレピュテーションは大きく変わる

- **決断力のある指揮**
  - 行動する－行動しないこともひとつの決断
  - コントロール可能なことに集中し、コントロール不能なことを受け入れる
  - インシデントは現場で管理し、クライシスは組織全体で管理する
- **継続的なクライシスの把握**
  - 日々再評価する－計画に執着してはならない
  - インシデントに気を取られ、クライシスを見失ってはならない
- **活発なコミュニケーション**
  - 自ら語る。メディアに語らせてはならない
  - 一貫したメッセージを内外に伝える

：

：

クライシスは物理的な災害を超えます

FOR DISCUSSION DRAFT PURPOSES ONLY

デロイトによるクライシスの定義

クライシスは、事業の存続を脅かす単独若しくは複合的な事象です

企業
政府組織
労働組合
政治団体

マーケットシェアと市場価値
信用力および財務リソース
現物の設備等の資産
知的財産

信頼性
ブランド

収益性
支払能力/財政状態

…組織の戦略目標、レピュテーション、その組織の存在をも著しく毀損させる大規模な、もしくは複合的な事象を指します。

サイバー攻撃、悪意、不正行為、金融犯罪、対立、テクノロジーおよび産業に対する脅威、財政難、倒産、自然災害や人為的災害等の大惨事、
これらはすべて財政的なクライシスのきっかけとなる可能性があります。

ご清聴ありがとうございます。