電通総研

DX時代のサイバー危機は、システム障害ではなく「経営リスク」

サイバー事故を「技術復旧」で終わらせない事業継続と顧客信頼を守るCC360

株式会社電通総研

会社概要：共同提案体制

電通総研

- システムインテグレーション
- コンサルティング
- シンクタンク

電通PRコンサルティング

広報・PR領域の専門会社として、
危機管理広報やレピュテーション・
マネジメントを支援

2社が連携して
「技術＋広報＋経営」を全方位で支援

講演者紹介

赤澤 卓真

株式会社電通総研 営業第二本部
エンタープライズソリューション
営業6部部長

2019年に電通総研へ入社。
顧客課題に向き合った営業経験を活かし、
現在はセキュリティ及びクラウドインフラ領域
を統括

企業価値向上の観点から、全社的な
サイバーリスク対策を支援

広報・経営・情シスの連携を強化する
「CC360」の推進を通じ、緊急時における
迅速かつ適切な体制構築を支援している

攻撃されるのは「もしも」ではなく「いつか」の話

情報セキュリティ10大脅威2026（組織向け）

1位　ランサム攻撃による被害

2位　サプライチェーンや委託先を狙った攻撃

3位　AIの利用をめぐるサイバーリスク

4位　システムの脆弱性を悪用した攻撃

5位　機密情報を狙った標的型攻撃

サプライチェーン全体を巻き込み、
ある日突然、業務がすべてストップする
事態が急増しています。

最新AIによる脅威

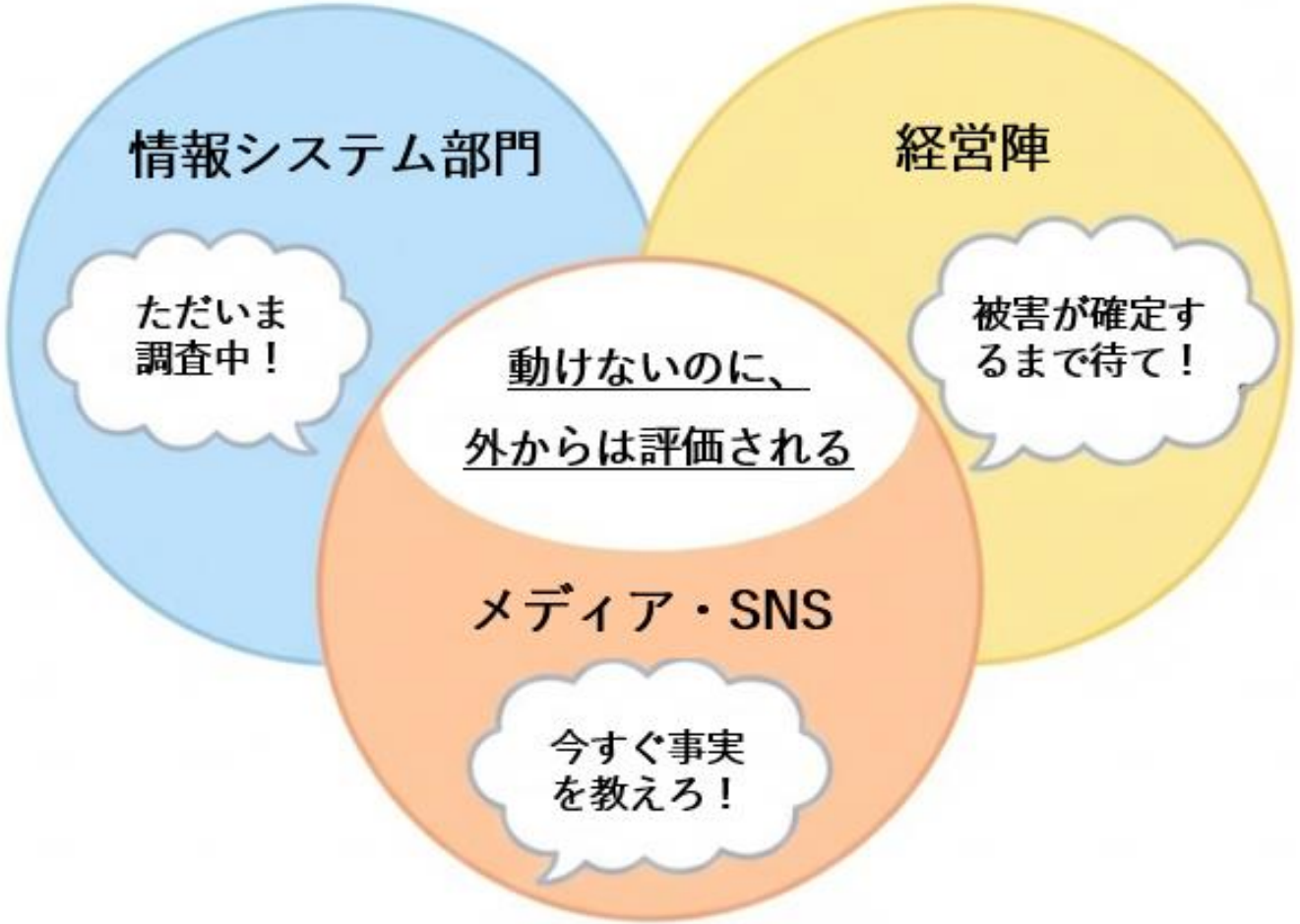
最新AI（例 Claude Mythos）の
登場により攻撃の高度化・
高速化リスクが高まっています。
国も緊急対策を急ぐ、
今そこにある危機です。

事実確認が終わる前に、社会の不安が先行してしまう「今そこにある危機」です。

国が求める「逃げないコミュニケーション」

※経済産業省「サイバーセキュリティ経営ガイドライン（第3版）」の「経営者が認識すべき3原則」より引用

インシデント時に起きる「部門間の情報断絶」



それぞれの部門が正義を持って動いているにも関わらず、
全体として連携が崩壊（サイロ化）する構造的弱点が存在します

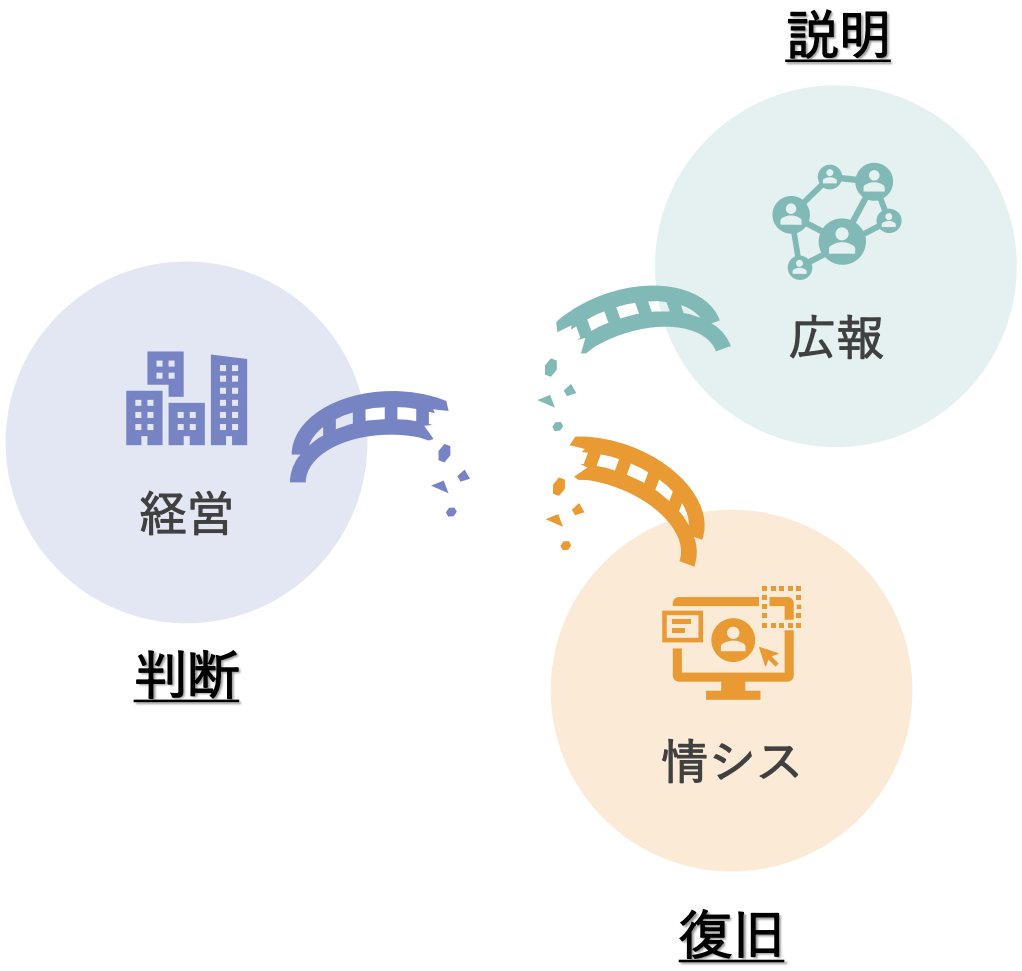
緊急時、担当部門だけでは動けない

「情報がない。方針が決まらない。でも、

電話は鳴りやまない。」

現場の対外対応チームを襲う「板挟み」のリアル。
社内と社外との「時間差」と「情報差」が現場をパニックに陥れます。

復旧・判断・説明が同時に走る難しさ



- サイバー危機において、「復旧が完了してから」→「経営が判断し」→「顧客へ説明する」という順番（直列）では間に合いません。
- 問題はどこか一部門が悪い訳ではなく、この3つが「同時に動く設計」になっていないことです。
- 情報を持つ部門、判断する部門、説明する部門がスムーズにつながるパイプラインが不可欠です。

シミュレーション：もし明日、自社のサーバーが人質にとられたら？

Alert

【シナリオ】

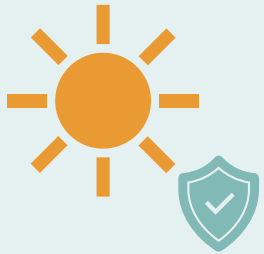
ある朝、自社のサーバーがランサムウェアで暗号化れ、全業務がストップ。

SNS上で、「システム止まっている？」「情報漏洩か？」と炎上の気配が拡大

2つの運命が分岐

準備ゼロルート（CC360なし）

準備万全ルート（CC360あり）



この瞬間、誰とつながり、
どう判断しますか？

【失敗例】業務復旧、顧客説明、経営判断がバラバラになる

準備ゼロの「本番が初見プレイ」状態。

社内連携のルールがなく、情報シス部門からの技術的な情報もおりてこない。
経営は判断材料を待つしかなく、憶測だけでメディアや顧客対応を迫られるパニック状態に。

【失敗結果】後手後手の対応で、ブランドが大炎上

- 情報がないまま会見に
  引きずりだされ、推測で回答。
- 「隠ぺい体質だ！」「対応が遅い！」とメディアに叩かれる。
- 結果的に、企業の長年の信頼は地に落ちてしまいます。

【成功例① 技術対応】専門チームが最速で「事実」をパスする

裏側で支える高度なセキュリティ監視・専門調査チームが即座に動きます。

「ファストフォレンジック」にて最速で「感染拡大の鎮静化」や「業務再開の判断」を実施

何が盗まれ、何が無事なのか。確かな「事実」だけを、迷わず広報へと届けます。

【成功例② 準備対応】迷わず動ける「緊急コールセンター」

事前準備の成果

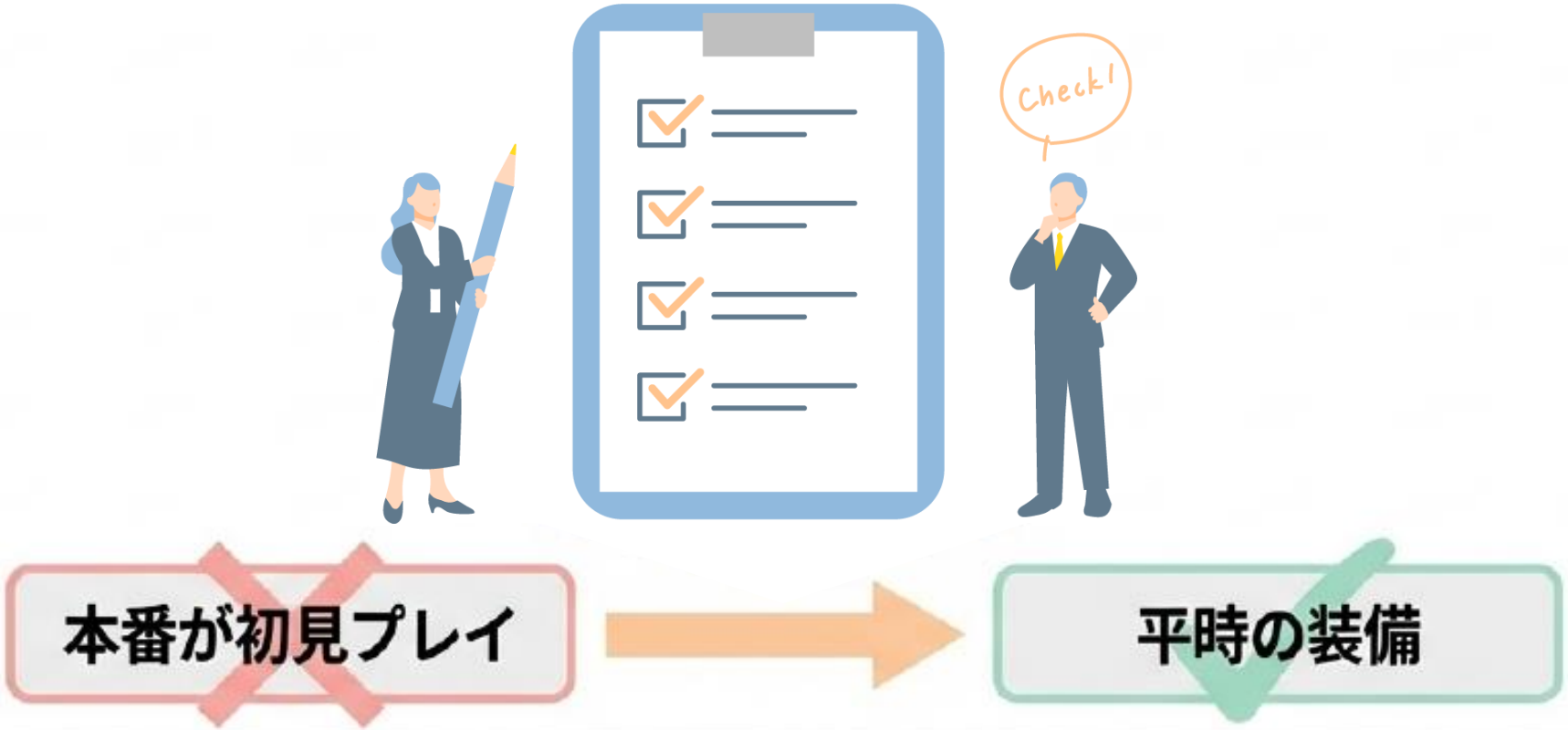
- 緊急コールセンターを即日立ち上げ
- 準備済みの「Q＆Aリスト」の展開
- 経営陣との迅速な方針合意

技術チームからの「事実」を受け、経営陣と広報は事前に決めていたルールに従って、迷わず即座に行動を開始します。

【成功結果】準備していた「盾」でブランドを守り抜く

- 誠実で透明性の高い記者会見を実施。
- 事実ベースの回答により、無用な憶測や炎上を未然に防止。
- 逆に「危機管理がしっかりしている企業」として、ピンチを乗り越え信頼を守り抜く。

広報を救った最大の武器。それは「平時のマニュアル」です



<u>シミュレーションで広報が落ち着いて対応できたタネあかし。</u>

それは、何もない平時のうちに「危機管理広報マニュアル」を作りこんでいたから。

サイバー危機は、起きてから準備するのでは絶対に間に合いません。

「誰が・何を・どの基準で」を明文化する

ルールの策定

迷わず動けるよう、インシデント発生時の公表基準を事前に決定します。

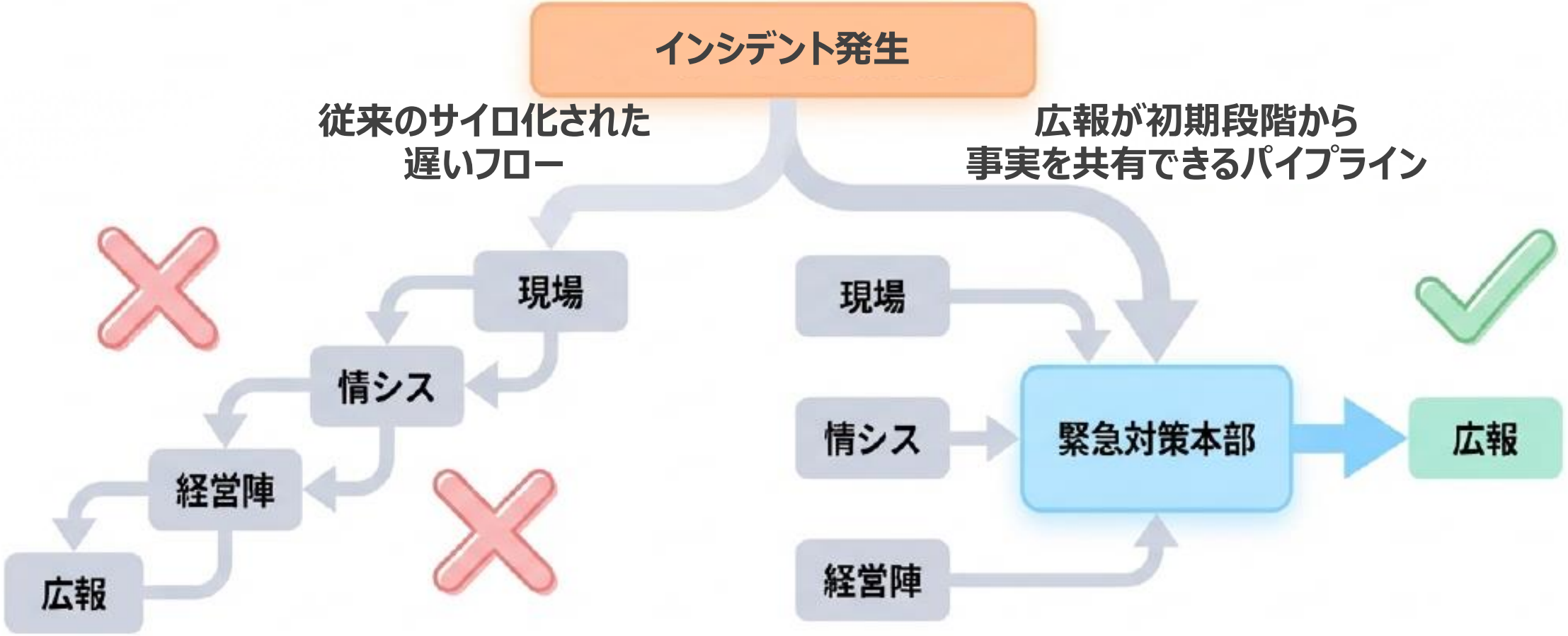
役割の明確化

「誰が最終判断を下すか」「誰がメディアの矢面に立つか」を平時に合意。

想定問答（QA）の準備

技術面で難しい内容も、広報が理解して説明できる言葉に翻訳しておきます。

初期フローの構築：マイナス情報を最速で広報へ

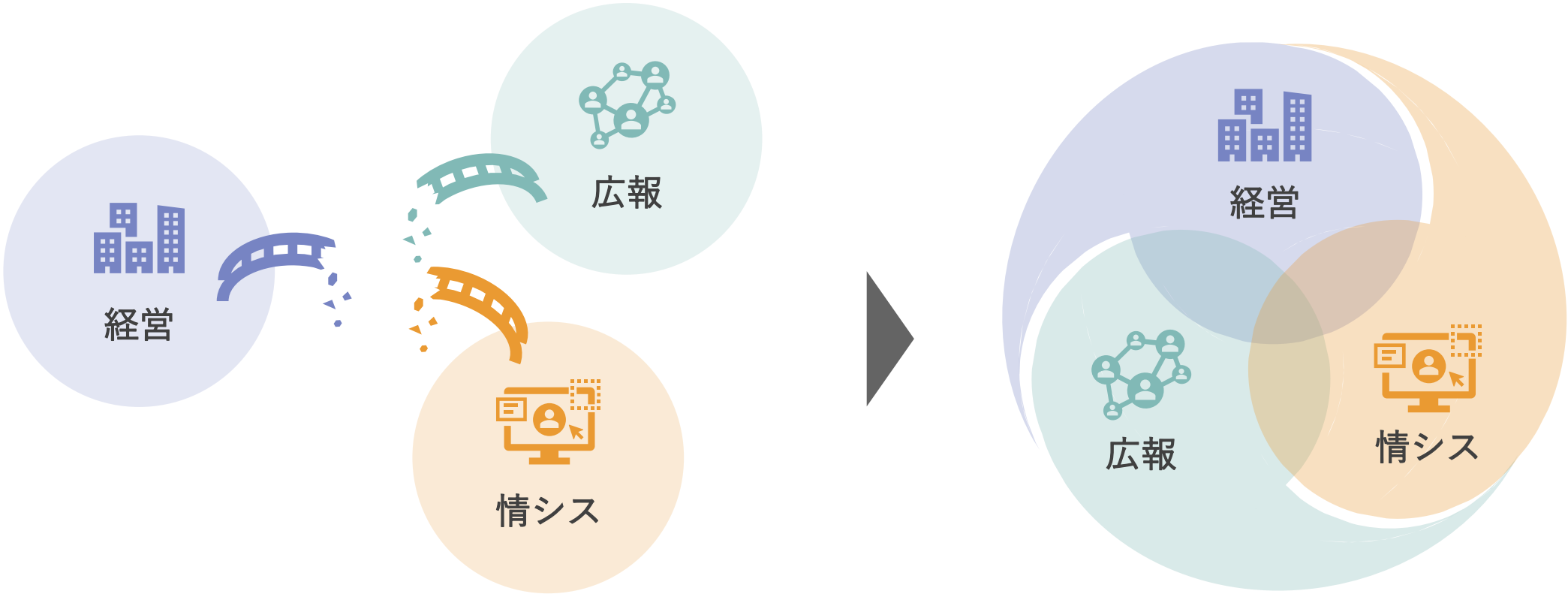


マイナス情報が「一番最後」ではなく
「一番最初」に広報へ届く仕組みを作ります。

マニュアルは「筋肉」と同じ。鍛えなければ使えない

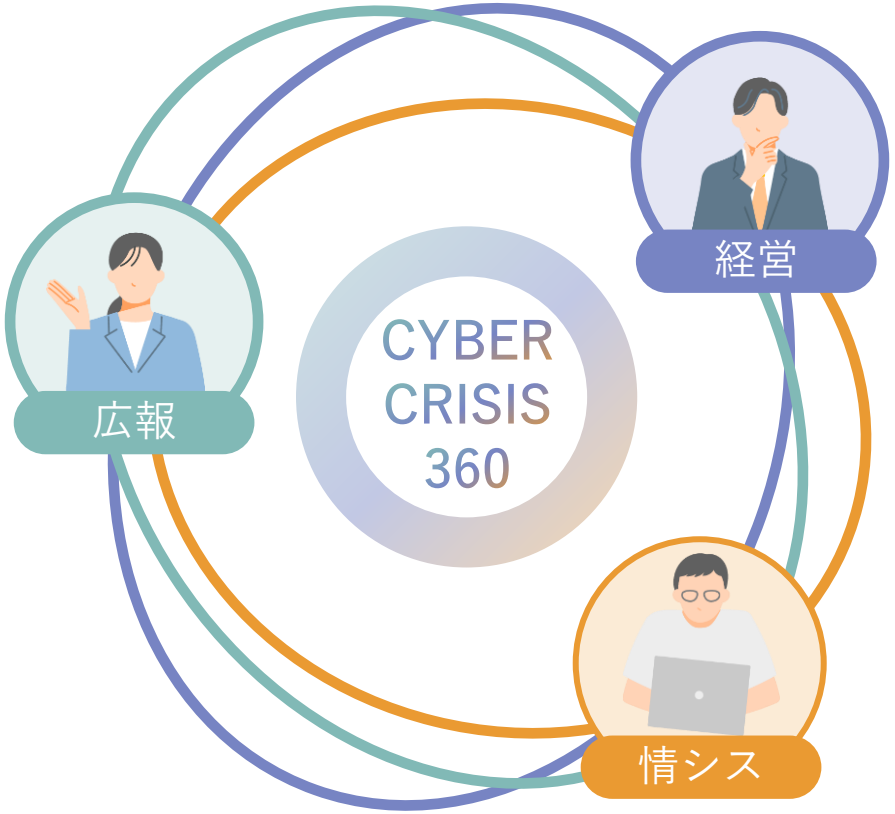
- 紙のルールを作っただけでは、いざという時に声が出ません。
- 本番さながらの「緊急記者会見トレーニング（模擬演習）」を
  セットで実施する事で、対応力は劇的に跳ね上がります。
- 厳しい質問にも動じない「組織の筋肉」を平時から育てましょう。

サイバー危機で失敗する本当の理由



企業が炎上する原因は、システムの問題（技術的）だけではありません。
「経営・広報・情シス」の連携崩壊（サイロ化）こそが最大の弱点です。
この3つをバラバラに支援するのではなく、すべてをワンストップで伴走パートナーが必要です

電通グループの最適解「CyberCrisis360 (CC360)」



技術的調査、メディア対応、経営判断を360度すべてサポートする独自の体制を作りました。
冷たいシステムツールではなく、広報に寄り添い、共に矢面に立つ「人」のチームです

「3つの盾」で企業を全方位から守る

経営判断の支援

- 経営層向け教育・シナリオ訓練
- レピュテーションリスク評価
- 緊急時の意思決定支援

メディア・SNS対応

- メディア・社外対応支援
- SNS炎上リスク管理
- プレスリリース文章案レビュー

高度な技術調査

- セキュリティ強化・技術支援
- フォレンジック対応（最速の事実確認と一次業務復旧支援）

※対応メニューの一部です。詳細はお問い合わせください

平時の準備から、いざという時の盾まで。途切れない安心

平時の準備

- マニュアル構築
- 模擬演習
- リスク評価

緊急時の伴走

- 緊急コールセンター
- 技術調査
- 記者会見支援

ブランド回復

- 再発防止策
- ブランド回復状況
- モニタリング及び施策検討

CC360ワンストップサポート

担当者が分かることなく、同じチームが伴走します

本日のまとめ：ブランドを守る最強の盾

サイバー攻撃は「システムの危機」ではありません。

「ブランドの危機」です。

関連部門が平時から繋がり、自信をもって動ける体制こそが、企業を守る最強の盾となります。

まずは、貴社の「現状の備え」についてお話しませんか？

平時・緊急時を問わず、自社の体制や予算に応じた柔軟な支援をご提供します。

【お問い合わせ窓口】

株式会社 電通総研
営業第二本部
セキュリティソリューション担当
https://security.dentsusoken.com/contact/

電通総研