サイバーリスクへの対処

その対策は、どこまで有効なのか

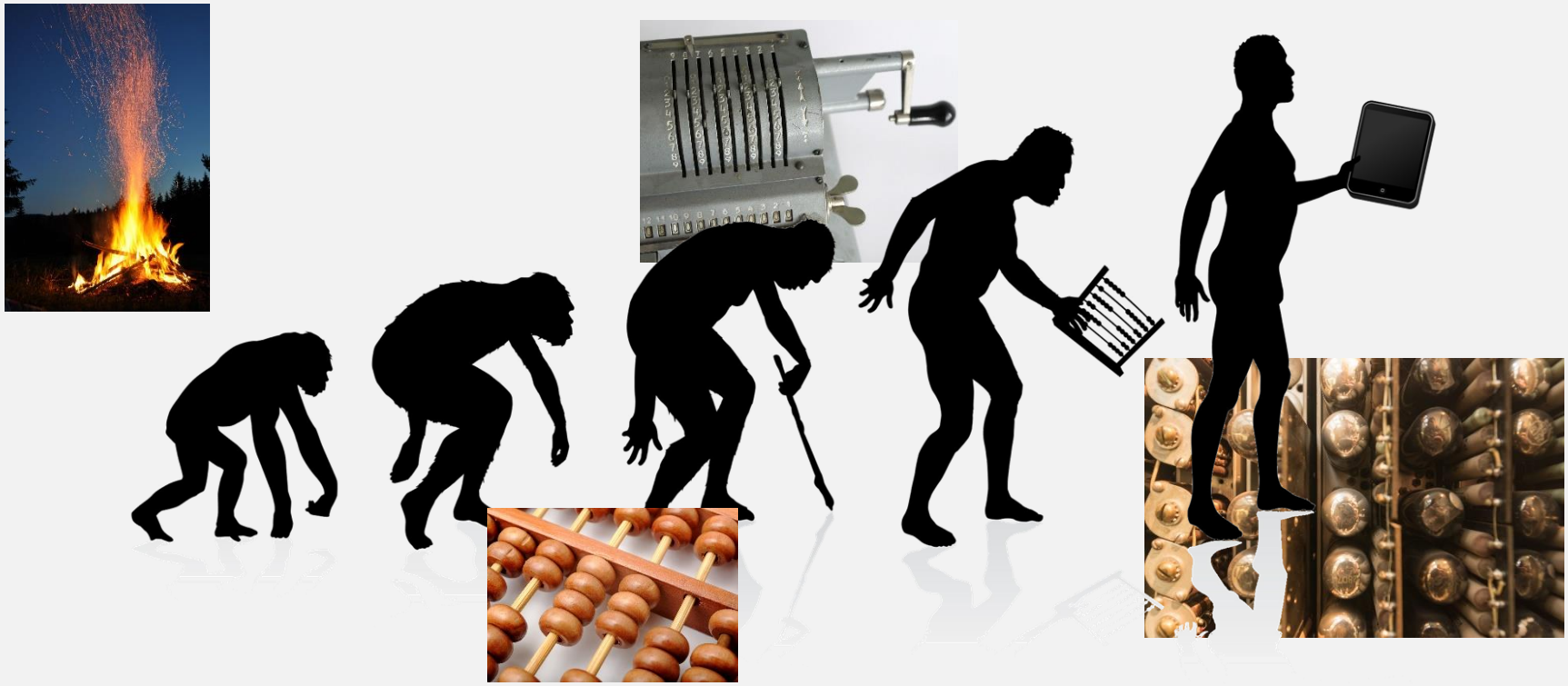
高　元伸
ヤフー株式会社　リスクマネジメント室

YAHOO! JAPAN

画像提供:Aflo

Before Cyberspace

計算機能の向上と計算機の普及



※投影資料を参照ください

画像提供:Aflo

江戸時代のサイバー犯罪

※投影資料を参照ください

Cybercrime

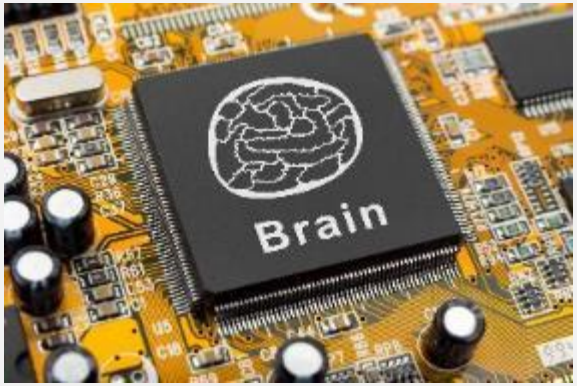
技術進歩と共に急速に高度化多様化

画像提供:Aflo

※投影資料を参照ください

急速な進化の要因

処理能力向上



小型化

通信高速化

低価格化

画像提供:Aflo

次世代テクノロジーにも新たな犯罪手口

画像提供:Aflo

明確な意思

人が意思を持って実行している
発生は確率ではない
誰が何を狙うかという目的で選択される

画像提供:Pixabay.com

犯罪目的の変化

画像提供:Aflo

攻撃者

オンライン犯罪者

ハクティビスト

テロリスト

悪意をもった内部関係者

国家

画像提供:Aflo

攻撃目的

諜報活動

模倣犯

画像提供:Aflo

裾野の広がり

国境を越えたリモートの攻撃

匿名性・攻撃コスト・複数同時攻撃
海外経由により法律が異なる

IT知識が乏しくても攻撃が可能

ダークウェブ（Dark Web）の発達
攻撃ツールが容易に手に入る
攻撃対象のアカウント情報・
カード情報・認証情報の売買
攻撃代行を安価で引き受ける

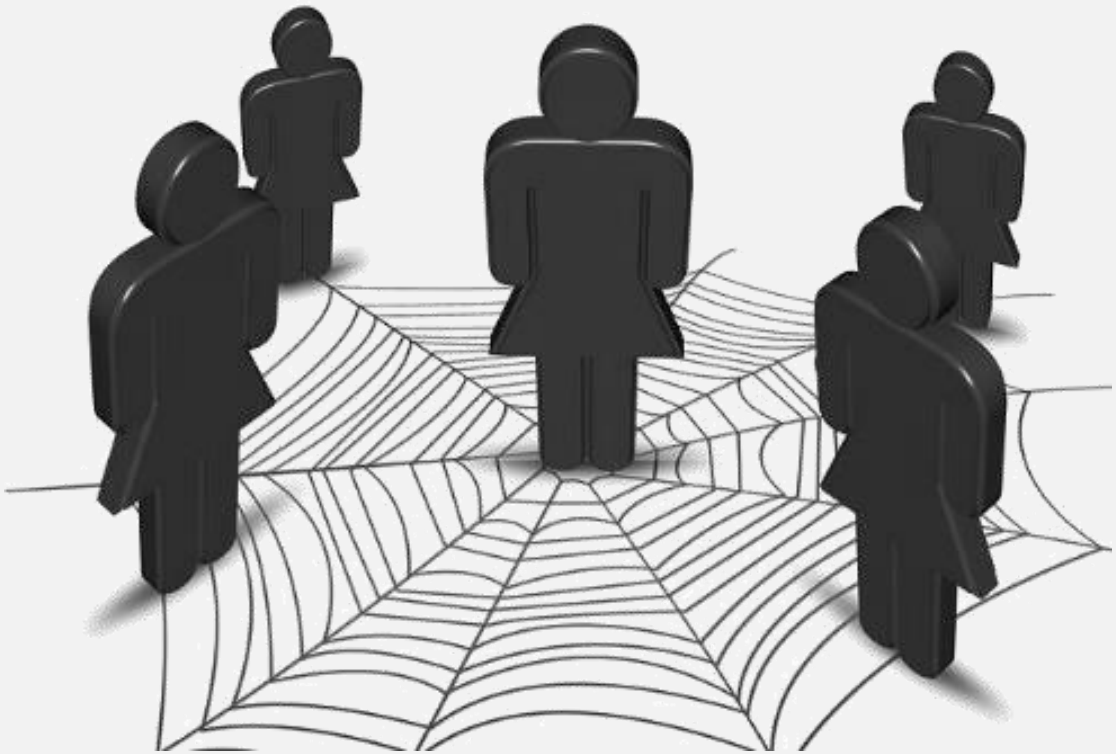
罪悪感の希薄

被害者が直接見えない
仮想空間のデータ処理

模倣犯の増加

気軽に安易な理由で攻撃者となる

犯罪エコシステム



画像提供:Pixabay.com

攻撃の分業化が進んでいる
攻撃者は闇サイトで繋がる
犯罪エコシステムの発達

※エコシステム　もともとは生態系という意味
そこから転じて複数の組織がある目的で
パートナーシップを組み、互いの技術・資本を
生かしながら共存共栄していく仕組み

犯罪の産業化も進む
組織で役割分担・階層化
大量処理で効率化
一網打尽が困難

攻撃者は常に知恵を絞る

画像提供:Aflo

自然災害やシステム障害とは異なる
想定外の手法を意図的に選択してくる

マーフィーの法則…ではない
ルールと運用のギャップが狙われる

攻撃は組織的に行われる
対抗する企業も総合力が問われる

技術力の評価競技ではない
ルール無視、時間制限なしの戦い

YAHOO! JAPAN

攻撃は常に進化する

画像提供:Aflo

攻撃者は規制ルールを順守しない

奪いやすいところから奪っていく

想定外の手法を意図的に選択してくる

ルールと運用のギャップが狙われる

心理の隙を突いてくる

画像提供:Pixabay.com

正面から攻撃されるとは限らない

画像提供:Aflo

セキュリティレベル
＝最も弱いところ

認識しにくい被害

画像提供:Aflo

痕跡が残らない
物理的変化がない
直接被害がない

防御側の厳しい現実

画像提供:Aflo

攻撃者は　利己的で強い目的意識をもっている
攻撃者は　豊富な経験を積んでいる
攻撃者は　情報を素早く共有する
攻撃者は　IT環境を駆使する
攻撃者は　急速に増加している

防御側は　セキュリティが本業ではない
防御側は　経験が少ない
防御側は　共有情報が少ない
防御側は　IT投資に制約がある
防御側は　インセンティブを得にくい

全ての企業が最前線

次の相手は常に未知の強敵

画像提供:Aflo

事業目標は見えやすくリスクは見えにくい

画像提供:Aflo

どうする？

企業が為すべき対応

社会的責任

画像提供:Aflo

事業継続

画像提供:Aflo

二次被害防止

画像提供:Aflo

Mission

画像提供:Aflo

なぜサイバー対策をするのか

画像提供:Aflo

緊急時の対応ポリシー

画像提供:Aflo

事例：サンフランシスコ市交通局（SFMTA）

画像提供:Aflo

※投影資料を参照ください

事例：米ロサンゼルス病院

画像提供:Aflo

※投影資料を参照ください

正解はひとつではない

画像提供:Pixabay

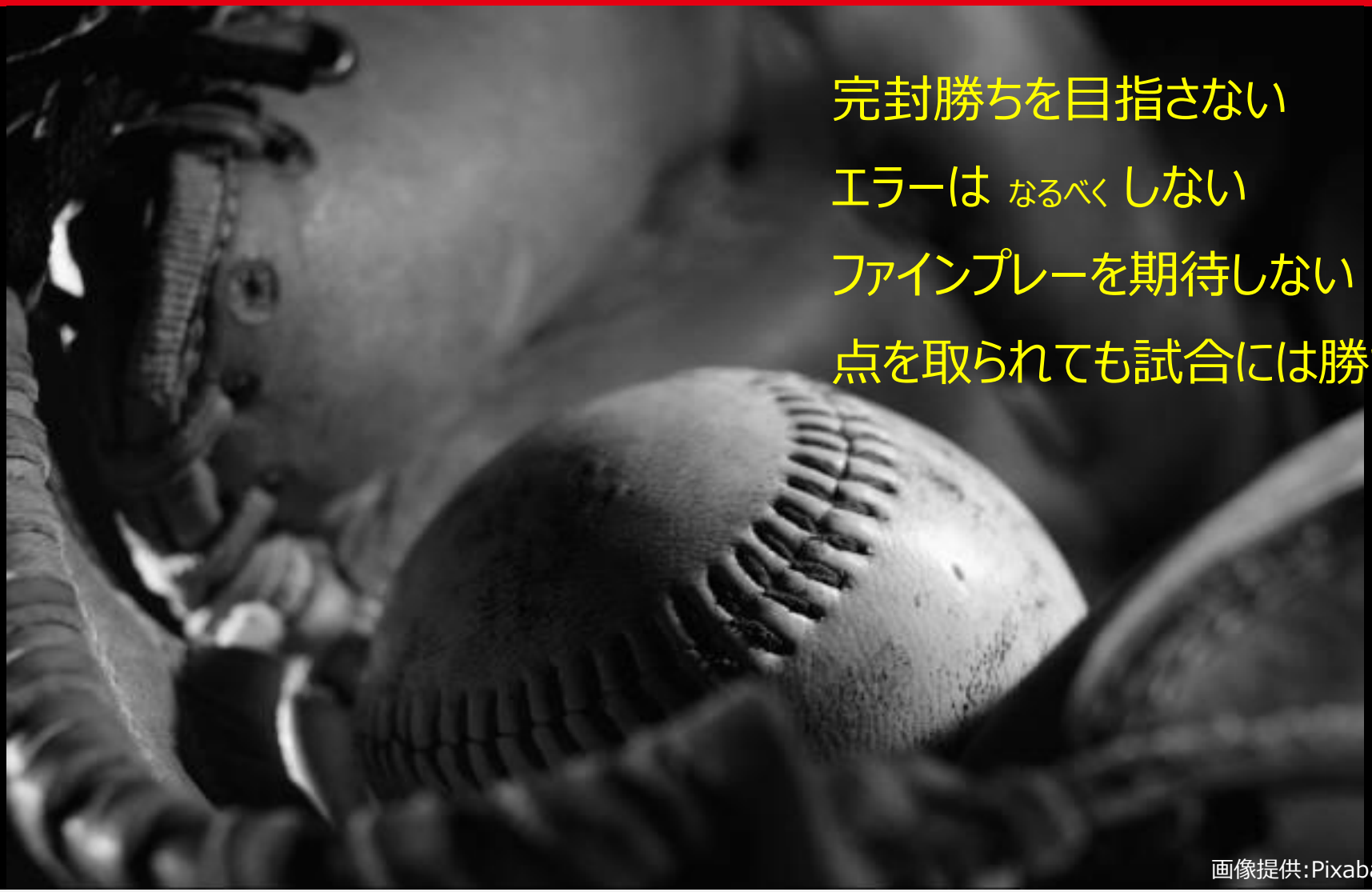
企業としての障壁

画像提供:Pixabay.com

経営資源は無尽蔵ではない

ダメージコントロール

完全勝利を前提にしない



完封勝ちを目指さない

エラーは なるべく しない

ファインプレーを期待しない

点を取られても試合には勝つ

画像提供:Pixabay.com

社会からどう見られるか

画像提供:Aflo

何のための事業か

企業はなぜ潰れる

インシデントにより潰れるのではない
対応の結果、信頼を失うことにより潰れる

平時の備え

画像提供:Aflo

装備以上に心構え

There is no sliver bullet.

銀の弾丸などない

テクノロジーによる防衛限界

かつて有効であった防御は
攻撃手法の転換により破られる

技術は使い方次第

※投影資料を参照ください

Cybercrimeの歴史はまだ80年

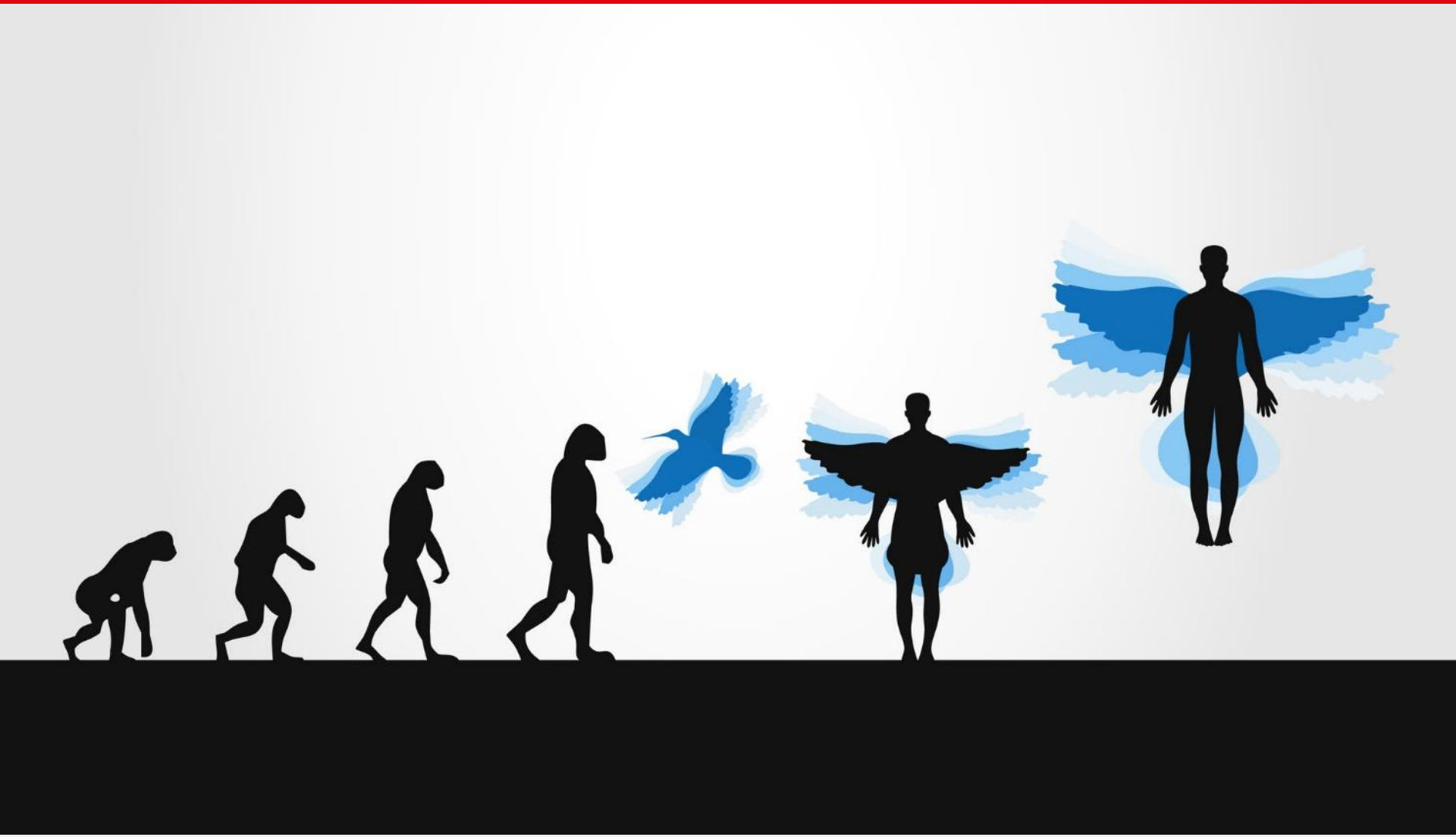
人の一生分の時間で急激に変化

※投影資料を参照ください

サイバージェネレーションのギャップ

YAHOO! JAPAN

変化はますます激化



決断と行動

何が致命的なのか

画像提供:Aflo

重要情報資産は
どのように守られているか

相手の意図を見極める

Skat
Koenig Dame
Bube

画像提供:Pixabay.com

Red Team によるシミュレーション

敵対した役割・視点を持つチームで
仮想攻撃を行い課題点を確認する

認知の重要性

彼を知り己を知れば百戦殆（あやう）からず

彼を知らずして己を知れば一勝一負す
彼を知らず己を知らざれば戦う毎に必ず殆し

抑止・予防だけではない

画像提供:Aflo

脅威抑制・発生予防

画像提供:Aflo

早期検知・早期報告

画像提供:Aflo

影響最小化・二次被害防止

運用精度を上げる

画像提供:Aflo

攻撃コストを上げる

画像提供:Aflo

個々の対策は簡易でも
突破に手間がかかる
検知の機会を増やす
攻撃側も費用対効果

情報収集

Intelligence

EU一般データ保護規則（GDPR）

画像提供:Aflo

脅威は技術だけではない

画像提供:Aflo

ソーシャルエンジニアリング

人間の心理的な隙や
行動のミスにつけ込んで
相手が持つ情報を不正に入手する

対策も技術部門だけではない

画像提供:Pixabay

初動対応の整備

インシデントレスポンスチーム
システム担当者
監視運用
経営層
サービス責任者

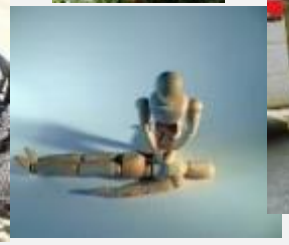
広報・CS・法務
人事・総務

再発防止対策チーム

※認知と行動開始

発生検知

異常検知
判断と初動対応
エスカレーション
緊急事態宣言



初期対応

被害拡大防止
影響範囲特定
原因分析
対応方針決定

事態収拾

情報開示
顧客対応
再発防止

顧客フォロー
課題振り返り
効果確認

対応人員補給入替

各フェイズで時間軸、中心となる人員が異なる
事故発生回避以上に二次被害発生回避
顧客対応の方針で対応に対する評価は大きく変わる

画像提供:Pixabay.com

リスクマネジメントの必要性

ご清聴ありがとうございました