インシデント対応の効率化による レジリエンスの実現

Internet Week 2021 C14

EYストラテジー・アンド・コンサルティング株式会社

Building a better working world

登壇者紹介

松下 直（まつした なおし）

EYストラテジー・アンド・コンサルティング株式会社
Technology Consulting / Cybersecurity - Partner
CISSP / CISA / CISM / RISS

情報セキュリティ・サイバーセキュリティの分野での25年以上の経験を有し、先端的セキュリティベンダーとの提携を通じ企業のITインフラを防御するマネージドサービス、インシデントの検知・対応を行う商用SOC/CSIRTの開発と提供、国内外でのセキュリティアセスメントなど幅広い経験を有する。セキュリティ専業会社・セキュリティサービスの海外拠点の立ち上げ、また、国内外の先端的ベンチャー企業への経営への参画などの経験も有する。現在は、EY Japan Region にてCybersecurity の Leader として、EY　Japan, Globalのリソースをミックスし、日系企業のセキュリティ対策支援を国内外で提供している。

登壇者紹介

森島 直人（もりしま なおと）

EYストラテジー・アンド・コンサルティング株式会社
Technology Consulting / Cybersecurity - Director
公認会計士 / 博士（工学） / CISA

我が国におけるインターネットの黎明期より大学院大学においてネットワークの研究に従事した後、通信会社等にて大規模システムの導入支援、構築運用などを実施。その後、監査法人において内部統制監査、システム監査、会計監査等に多数従事。

セキュリティコンサルタントに転身してからは、大学院大学や通信会社において培った情報技術の知識と、監査法人において培ったガバナンスや内部統制の知識を生かし、サイバーセキュリティコンサルティング業務を管理的な側面から技術的な側面までワンストップで提供し続けている。

Contents

SOCにおけるインシデント検知・対応の課題

企業におけるセキュリティインシデント検知と対応の課題

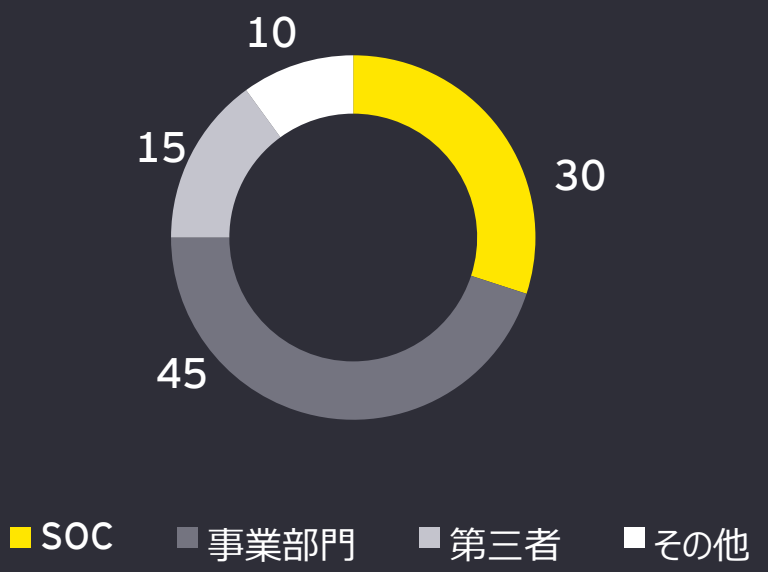
脅威の拡大

- ランサムウェアに加え二重・三重の脅迫などの脅威
- 攻撃対象の増加（脆弱性、クラウド、在宅環境）

課題

- 監視対象の構成把握不足による誤検知・過検知の多発
- インシデント対応プロセスの整備不足による対応の遅れ
- インシデント検知・対応の要員不足

セキュリティインシデントの検知(%)



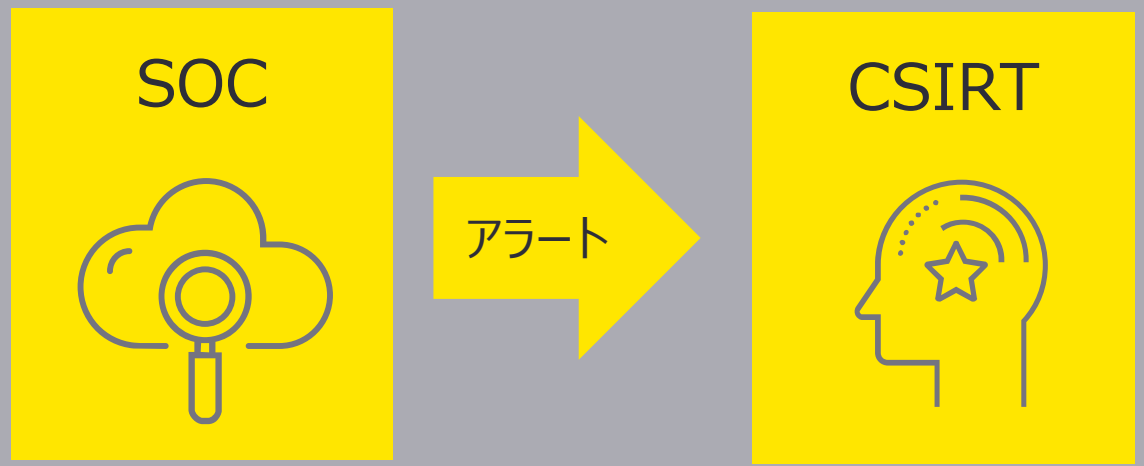
EY Global Information Security Survey 2020より

監視対象の構成把握不足による誤検知・過検知の多発

- SOCが構成を把握しておらずアラートが多発する（対象システム構成と一致しない脆弱性など）
- 構成情報がSOC導入時から変化しており意味のないアラートが送信される

SOCにおいて監視対象の構成を把握・活用することでアラートの精度を高めるべきです

インシデント対応プロセスの整備不足による対応の遅れ



- CSIRTがSOCからアラートを受領した後、対処方法をその場で考える
- インシデント対応手順が文書で書いてあるものの具体的な手順がわからない（複数のツールを使った複雑な手順、担当者のスキルに依存した手順など）

インシデント対応プロセスを事前準備し担当者への依存度を下げることで迅速な対応を実現すべきです

インシデント検知・対応の要員不足

セキュリティ業務増
- コンプライアンス
- 委託先チェック
- 脆弱性管理
- etc.

24/365 のインシデント対応ですら要員不足
プロアクティブなインシデント検知(Threat Hunting)まで手が回らない

インシデント対応
- 人手による煩雑な手順
- 対応できる要員が限定される

インシデント対応プロセスを自動化することでセキュリティ担当者の負担を下げ、他の業務へ時間を使うべきです

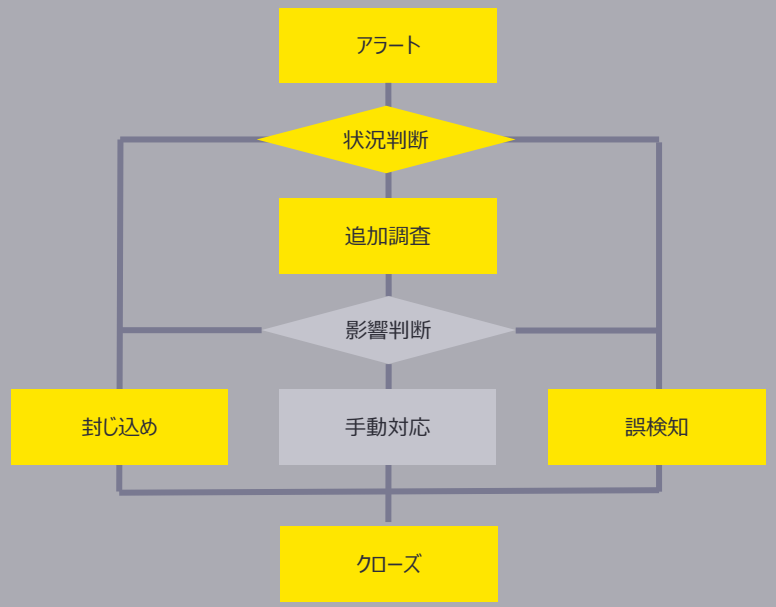
SOARによる課題の解決

SOARの導入によるサイバーレジリエンスの実現

サイバーレジリエンス

- セキュリティインシデントの発生を想定しインシデント対応手順を事前に準備する
- インシデント発生時に迅速な対応を行うことで被害を極小化し速やかな回復を行う

SOAR(Security Orchestration, Automation and Response)



SOARによる自動実行

- 構成情報を参照したうえで検知したアラートの状況を判断
- 過去のログ収集やIPアドレスのレピュテーションチェックなどの追加調査
- セキュリティデバイスと連携したインシデントの封じ込め
- チケットへの起票

人による判断と対応

- あいまいなケースや自動での封じ込めにリスクがある場合の判断
- 他チームとの連携が必要な場合などの個別対応

Webサイトへの攻撃検知と対応の事例

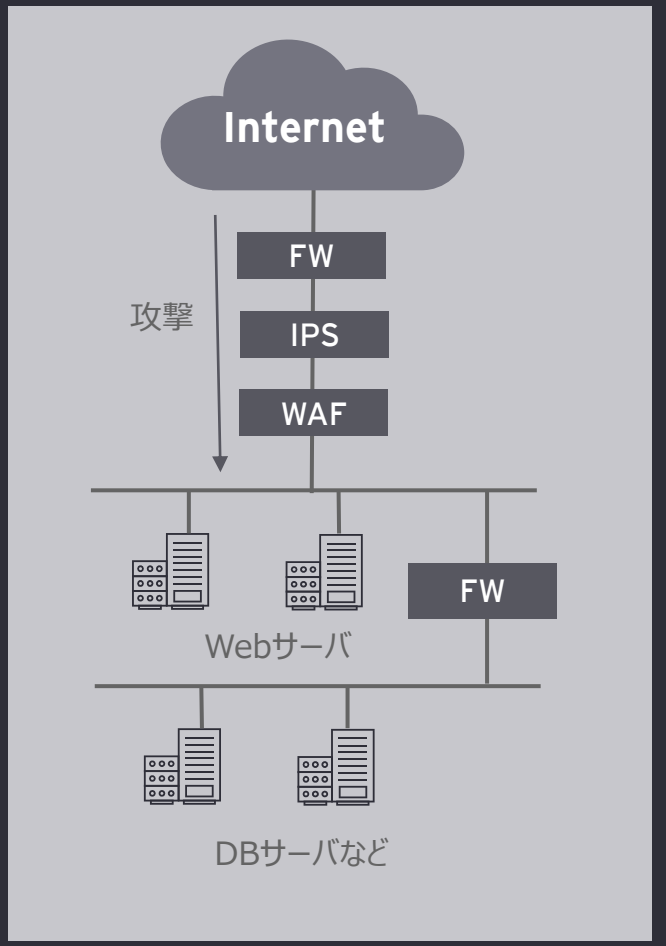
攻撃シナリオ　Webサイトの脆弱性をついた不正アクセス

インシデント調査

- 攻撃者のIPアドレスのレピュテーション調査
- 該当IPアドレスからの直近24時間以内の通信情報収集
- 攻撃対象の構成情報収集

インシデント対応

- 事前に用意した FWの Block 用ポリシーに該当IPアドレスを追加
- WAFにより一定時間通信を遮断



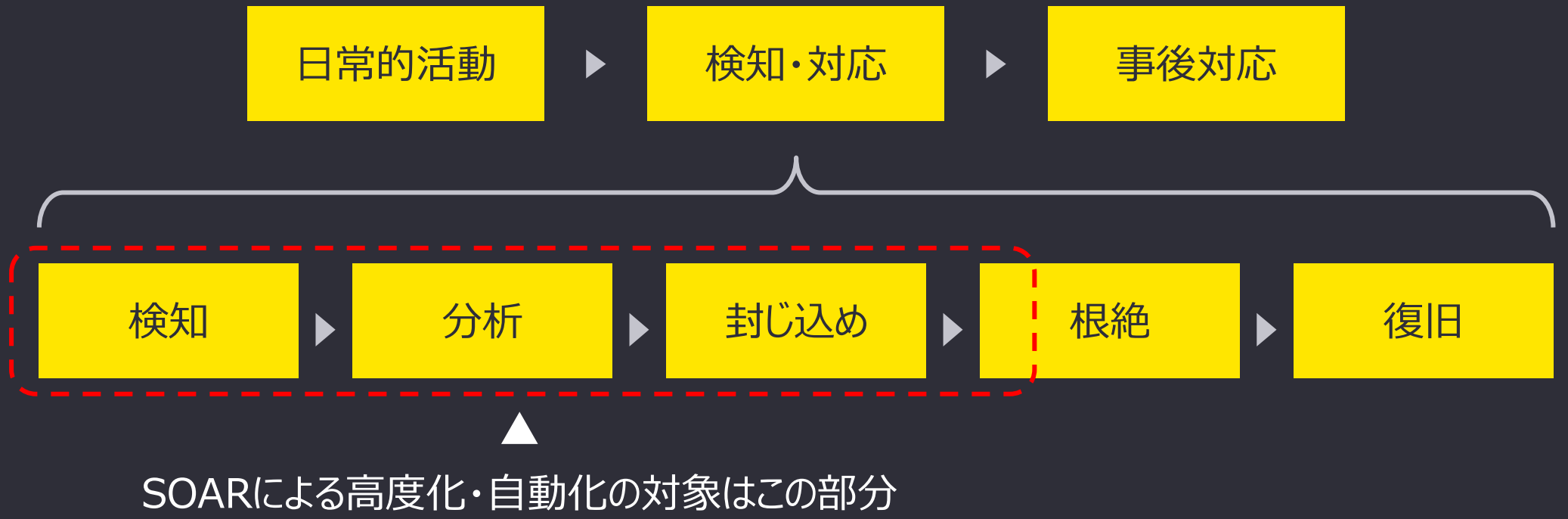
手動でのインシデント調査と対応時間　45分 を 5分に短縮

SOAR実装の勘所

インシデント対応のライフサイクルにおける高度化・自動化の対象

インシデント対応のすべてが高度化・自動化できるわけではない

- 検知と分析、封じ込めが主な対象



インシデント対応の各フェーズにおける高度化・自動化の内容

既存運用におけるSOC領域とCSIRT領域の密な連携が必要不可欠

	高度化・自動化の内容
検知	監視対象とする機能※全体の構成を踏まえた相関分析に基づく検知ロジックを投入
分析	各機器での追加情報取得と分析およびイベントの種別ごとに、レピュテーションチェックなどの定型的な分析業務を自動化
対処 （封じ込め）	監視対象とする機能※×（検知したイベント＋分析結果）に応じて、デバイスの設定変更やチケットの更新などの定型的な対処業務を自動化

※ 機能：あるサービスを提供するために構成されたデバイス群。例えば、Webサービスであれば、フロントサーバ、DBMS、それらを保護するWAFやIPS、DBFWなど。

「なにが検知できるか」ではなく「なにを検知、自動対処したいか」

SOC主導ではなく、CSIRT主導で推進することが重要

- SOCからエスカレーションされるアラートから考えるとゴールが見えない
- 脅威から自動対処したいイベントに落とし込み、検知すべきイベントを特定する

CSIRTが自動対処したい脅威を識別、それに基づいて検知したいイベントに特定

▶

SOCがCSIRTの特定したイベントを検知するためのロジックを設計、投入

SOCが監視対象となるデバイスのアラートをナレッジにより分析、エスカレーション

▶

CSIRTがSOCから受領しうるアラートを網羅的に把握し、そのすべてに対して自動化を検討

高度化・自動化推進のプロセス

CSIRT主導の高度化・自動化推進プロセスを整備する

監視対象とする機能の特定

- 機能ごとの重要性評価
- 監視対象とする機能の特定
- 監視対象とする機能の詳細構成把握

高度化・自動化の内容に関する検討

- 脅威の検討
- 相関分析の検討
- ログポイントの特定
- サービスレベルの検討
- 対応自動化可否の検討

高度化・自動化した運用

- Playbook異常動作時の対応

高度化・自動化の実装

- ログの取得
- 検知ロジックの開発と追加
- デバイス側のAPI等の設定
- Playbookの実装とテスト
- 自動設定に係るログの収集設定
- インシデント対応手順の策定・更新

高度化・自動化の実装に関する検討

- 自動設定可否の検討
- 自動設定のリスク評価
- ログの取得の可否検討
- 実装内容の決定

EYでは脅威分析に基づく検知すべきイベントの特定にMITRE ATT&CK®を活用

MITRE ATT&CK

- 米国連邦政府が支援する非営利組織であるMITREが策定
- 実際の観測に基づく攻撃者の戦術と技法を体系化したナレッジベース
- https://attack.mitre.org/

戦術 (Tactics)

Initial Access	Execution	...	Exfiltration	Impact
Drive-by Compromise	Command and Scripting Interpreter	…	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Container Administration Command	…	Data Transfer Size Limits	Data Destruction
External Remote Services	Deploy Container	…	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Hardware Additions	Exploitation for Client Execution	…	Exfiltration Over C2 Channel	Data Manipulation
⋮	⋮	⋱	⋮	⋮

技法(Techniques)

技法ごとに提供される情報
- 技法の基礎情報
- 技法の概要
- 実際の攻撃手順の例（過去事例）
- 緩和策
- 検知策

EYでは脅威分析に基づく検知すべきイベントの特定にMITRE ATT&CK®を活用

対象となる脅威の識別

監視対象となる機能において生じうるサイバー脅威を識別

- 組織において、SSDLC等で定められている既存の脅威評価フレームワークを利用

戦術の特定 (Tactics)

監視対象とすべき戦術を特定

- 識別した脅威をサイバー攻撃者が実現するための戦術を抽出
- 特定された戦術のうち、優先して対処すべき戦術を特定
  - 特定された戦術に対して最初から網羅的に対応しようと考えない

技法の特定 (Techniques)

検知すべき技法を特定

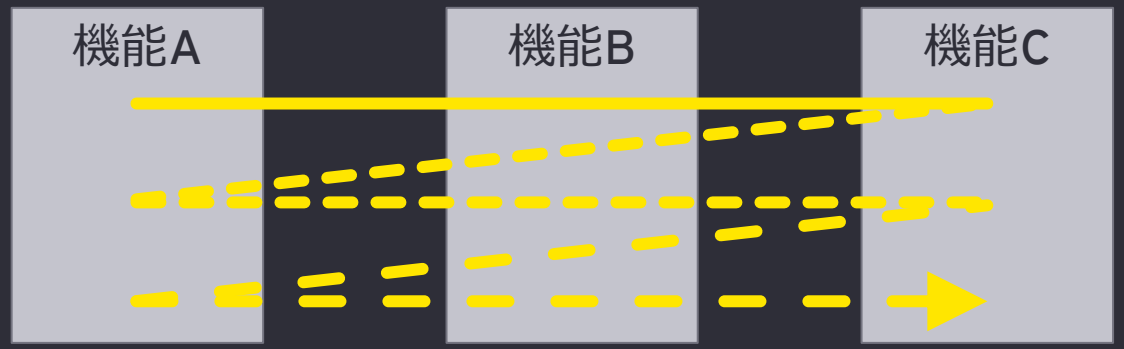
- 特定した戦術を構成する技法から、監視対象となる機能の現状を踏まえて特定
  - 監視対象となる機能が技法の標的とするプラットフォームと一致しているか
  - 技法に対する既存の防御策の状況も参考に、補完するように選定

高度化・自動化の結果を早期に享受するための進め方

効果の大きい部分から高度化・自動化に取り組む

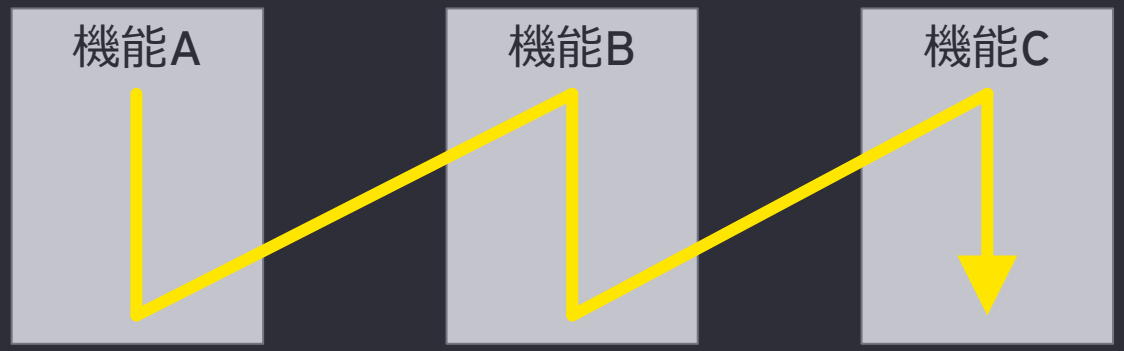
- 監視対象とする機能に対して網羅的に高度化・自動化をしようとしない
- まずはリスクの高い領域、日常的な業務において負荷の高い領域から着手する

○



早期に結果を得られるよう、機能ごとに、脅威分析に基づくリスクの高い領域、日常的に高負荷の領域から着手し、徐々に対象を広げていく

×



機能ごとに網羅的に高度化・自動化を実施しようとすると、コストに対して効果が見えにくく、経営層の納得感も得られにくい

まとめ

まとめ

サイバー攻撃の脅威がますます増大している一方、企業におけるセキュリティ人材の不足は解消のめどが立ちません。企業は今こそ SOARを活用して、限られたセキュリティリソースを抑えつつ、セキュリティインシデントへの速やかな対応と影響を極小化するレジリエンスを実現すべきです。

企業におけるインシデント検知の課題のSOARによる解決

- 監視対象の構成情報を利用してアラートの精度を向上
- 事前に用意したインシデント対応フローを自動化することで迅速な対応を実現
- 各種セキュリティ機器との自動連携により担当者のオペレーションスキルに依存しない対応の実現

SOAR導入の勘所

- システム構成を把握したうえで攻撃シナリオを作成
- 優先度の高い監視対象に対して実装後、インシデント対応の高度化と対象の拡大を継続

EY | Building a better working world

EYは、「Building a better working world（より良い社会の構築を目指して）」をパーパスとしています。クライアント、人々、そして社会のために長期的価値を創出し、資本市場における信頼の構築に貢献します。

150カ国以上に展開するEYのチームは、データとテクノロジーの実現により信頼を提供し、クライアントの成長、変革および事業を支援します。

アシュアランス、コンサルティング、法務、ストラテジー、税務およびトランザクションの全サービスを通して、世界が直面する複雑な問題に対し優れた課題提起（better question）をすることで、新たな解決策を導きます。

EYのコンサルティングサービスについて

EYのコンサルティングサービスは、人、テクノロジー、イノベーションの力でビジネスを変革し、より良い社会を構築していきます。私たちは、変革、すなわちトランスフォーメーションの領域で世界トップクラスのコンサルタントになることを目指しています。7万人を超えるEYのコンサルタントは、その多様性とスキルを生かして、人を中心に据え（humans@center）、迅速にテクノロジーを実用化し（technology@speed）、大規模にイノベーションを推進し（innovation@scale）、クライアントのトランスフォーメーションを支援します。これらの変革を推進することにより、人、クライアント、社会にとっての長期的価値を創造していきます。詳しくはey.com/ja_jp/consultingをご覧ください。

ED None

ey.com/ja_jp