システムのサイバーセキュリティリスクを可視化し効果的な対策案を提示

サイバー攻撃ルート診断サービス

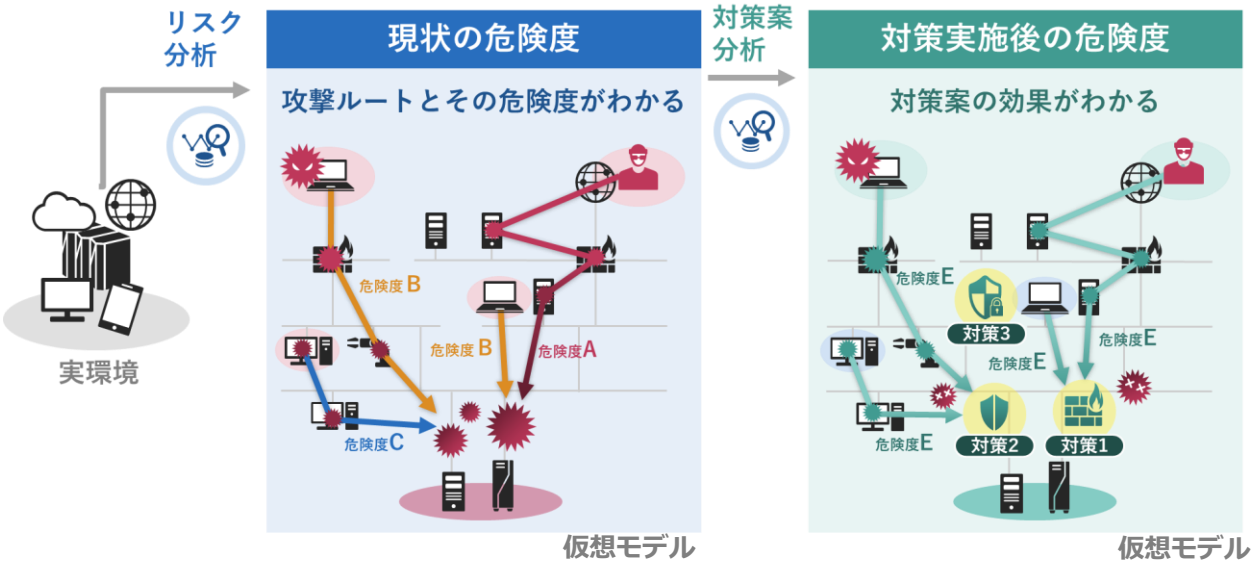
現状のシステムのセキュリティリスクの全体像と、危険度が高く対応を優先すべきリスクを明らかにします。さらに、セキュリティ対策を実施した場合の危険度の変化を可視化し、効果的な対策案を提示します。

このようなお客様に

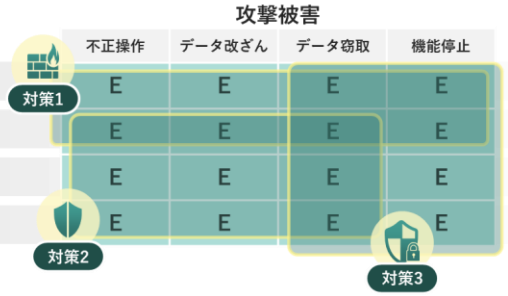
- システムの**実環境に影響を与えず**に、リスク診断を行いたい
- システムのどこにどのようなリスクがあり、一番の**弱点はどこかを把握**したい
- どのような対策を実施したらどの程度危険度が下がるか、**対策の効果・妥当性**を判断したい

サービスの特徴

- NEC独自の分析技術を活用することで、システムの脆弱性を繋いで実際に攻撃可能な複数の攻撃ルートを**仮想モデル上で網羅的に**検出
- それぞれの攻撃ルートの**リスクを可視化**し、最もリスクの高い攻撃ルートを明示
- システムのリスクと対策の効果を定量的に可視化し、**効果が高い対策**を優先対策案として提示
- 攻撃ステップに対して、特定された脆弱性の数・攻撃実証コードの有無を含む**リスク診断評価**を生成（特許出願済）



侵入口/攻撃目標	攻撃被害 不正操作	データ改ざん	データ窃取	機能停止
①Internet/ファイルサーバ	A	A	A	A
②社内端末/ファイルサーバ	B	B	B	B
③遠隔端末/ファイルサーバ	B	B	C	B
④操作端末/ファイルサーバ	C	D	D	C



効果

- 仮想モデル上で分析を実施するため、**実環境に影響無く**リスクや対策効果を把握することが可能
- システムの弱点とともに、対策を実施した場合にどの程度危険度が下がるかを確認でき、**対策の効果・妥当性を判断**することが可能
- 発見されたリスクに対して優先対策を施すことにより、システム環境を**効率的かつセキュア**に保つことが可能

事例

製造業 A社様

お客様背景／課題
- ◆ ほとんどの機器が修正プログラム未適用
- ◆ 危機感あり、なんらかの対策をしたいが、全ての機器の対応は費用的に不可能

お客様評価ポイント
- ◆ 実環境を触らずに診断できた
- ◆ 当初、想定していた対策機器数を**半分以下に削減**できた

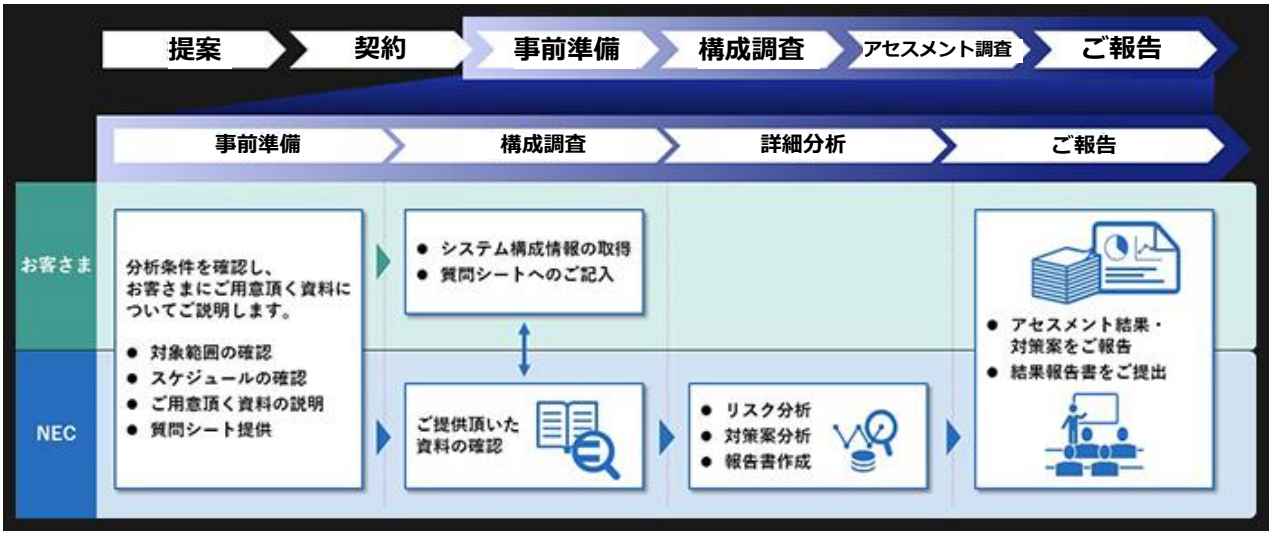
製造業 B社様

お客様背景／課題
- ◆ 多数の機器やネットワークが繋がっており、様々な経路で通信が発生している
- ◆ どこに対策を実施すると効果的か判断が困難

お客様評価ポイント
- ◆ 実環境を触らずに診断できた
- ◆ 発生し得る攻撃ルートとその危険度を洗い出すことで、**対策優先すべき箇所を把握**できた

サービスご提供の流れ

- サービスご提供の流れは、以下になります。



期間：構成調査からご報告まで2か月~

NEC　サイバーセキュリティ事業統括部

日本電気株式会社 〒108-8001 東京都港区芝五丁目7-1（NEC本社ビル）