サイバーセキュリティ
リスクアセスメント サービス

Secure Innovation

サービスユースケース

自社のセキュリティ対策の現状を確認したい

資産管理やアカウント管理の運用実態や体制面、手続き面などを把握することで、
自社がどういったラインにいるかを把握することが可能です。

漠然としたセキュリティへの不安を覚えている

漠然としている不安を、レポートにより明確化いたします。また、ご要望に応じて、話題となっているセキュリティインシデントについても触れることが可能ですので、賑わせているインシデントと自社のリスクの関係についてもお話致します。

セキュリティ投資の計画や最適化を図りたい

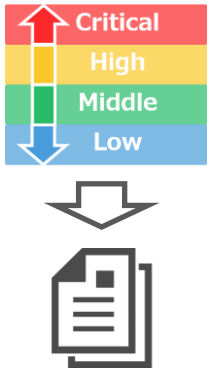
提出するレポートには、洗い出された課題だけではなく、それに応じた対策についても明記しております。優先順位なども含めてご報告いたしますので、自社の予算や年次スケジュール作成に有効な情報ソースとして頂くことが可能です。

企業買収や組織改編などの別組織の評価を行いたい

相手方のセキュリティベースラインや脆弱な状態か否かを把握することによって、
適切な価値の見極め、不必要な事故の防止につなげて頂くことが可能です。
※2018年にはマリオットホテルが、M&Aを引き金に大きな事故を起こしています。

サイバーリスクアセスメントサービスとは

戦略・技術的対策・組織的対策の3つの視点で、貴社の現状のセキュリティ対策の有効性を評価し、セキュリティリスクの全体像を可視化。今後の対策優先度をご提示します。

調査対象	調査手法	成果物
1.戦略（セキュリティ経営） セキュリティに関する経営方針、管理体制、経営資源の計画、確保 **対象者：CISO、セキュリティ責任者** **2.技術的対策** サイバー攻撃に対する技術的な対策の実装状況及びその運用について可視化を行い、有効性を評価する **対象者：情報システム担当者**	**✓インタビュー調査** ・CIS Controls ・サイバーセキュリティ経営ガイドライン ・NIST などの各種フレームワークやガイドラインを用いて、インタビュー調査を行います。	ランク付けや定量化によるリスク評価を行い、 事前知識のない方でも理解しやすい内容にてレポートを納品します。 
3.組織的対策 情報セキュリティに関わる規程・基準など、社内ルールの整備・文書化 **対象者：情報セキュリティ担当者**	**✓規定文書の精査** 社内規程文書の整備状況の確認 及び既存の規程文書内容の精査 (ルールの不備調査)	

+α
- (オプション) 詳細技術的対策 → ✓脆弱性診断サービス
- (オプション) 人的対策 → ✓標的型メール訓練..etc

Secure Innovation
沖縄から日本全国　そしてアジアへ

標準サービスのご案内

1.戦略（セキュリティ経営）

経産省
「**サイバーセキュリティ経営ガイドライン**」
の内容に基づいた**インタビュー評価**を実施し、
サイバーセキュリティに関わる経営方針、認識
を評価します。

経営者が認識する必要のある**3原則**

(1)サイバーセキュリティリスクの認識と対策
(2)サプライチェーンに対するセキュリティ対策
(3)情報開示など、関係者との適切なコミュニケーション

担当幹部が指示すべき重要**10項目**

サイバーセキュリティリスクの認識、組織全体での対応方針の策定
サイバーセキュリティリスク管理体制の構築
サイバーセキュリティ対策のための資源（予算、人材等）確保
サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
サイバーセキュリティリスクに対応するための仕組みの構築
サイバーセキュリティ対策におけるPDCAサイクルの実施
インシデント発生時の緊急対応体制の整備
インシデントによる被害に備えた復旧体制の整備
ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

※サイバーセキュリティ経営ガイドラインとは、
サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3原則」、
及び経営者が情報セキュリティ対策を実施する上での責任者となる
担当幹部（CISO等）に指示すべき「重要10項目」をまとめたドキュメントです。

2.技術的対策

18カテゴリの**インタビュー調査**を実施し、対象企業におけるセキュリティ対策の現状を分析・評価。推奨されるセキュリティ施策とその優先度をご提示します。

18カテゴリの例

1. 組織の資産のイベントリと管理
2. ソフトウェア資産のイベントリと管理
3. データ保護
4. 組織の資産とソフトウェアの安全な構成
5. アカウント管理
6. アクセス制御管理
7. 継続的な脆弱性管理
8. 監査ログ管理
9. 電子メールとWebブラウザの保護
10. マルウェアの防御
11. データ復旧
12. ネットワークインフラストラクチャ管理
13. ネットワークの監視と防御
14. セキュリティ意識向上スキルのトレーニング
15. サービスプロバイダーの管理
16. アプリケーションソフトウェアのセキュリティ
17. インシデントレスポンスと管理
18. ペネトレーションテスト

3.組織的対策

お客様の情報セキュリティ関連規程類の内容を精査・分析し、組織のルールとしての**不備・不足の有無を調査**します。

(例)情報セキュリティ関連規程類

[情報セキュリティ関連規程類]
情報セキュリティポリシー
情報セキュリティ基本規程
情報セキュリティガイドライン（従業員向け）
情報システム開発規程
情報システム管理規程
[その他]
従業員向けセキュリティ教育資料
IT全般統制関連資料
…etc

**下記の要素に基づいて
不備・不足を分析**

- 国際標準（ISO/IEC27001（ISMS））
- 法令遵守
- 業界ガイドライン
- 各種セキュリティガイドライン
- 各種セキュリティフレームワーク
- 同業他社、同規模企業との比較
- 最新の脅威動向
- 社会のトレンド（時勢・動向）
- 過去、もしくは本評価と並行して
  実施したインタビュー調査
- その他、コンサルタントの経験・知見

…etc

**標準サービスとして紹介しておりますが、ご要望をヒアリングさせて頂き、
対象物やスコープ、難易度を柔軟に調整することも可能となっております。
※場合によっては、採用ガイドラインやフレームワークも変更する可能性もあります。**

Secure Innovation
沖縄から日本全国　そしてアジアへ

実施プロセスのイメージ

評価の実施プロセス

アセスメントについては、プロジェクトのキックオフから最終報告会まで、約1.5ヶ月内での実施を想定しております。

キックオフ（1日）	調査・情報収集（1ヶ月内）	報告書作成（2週間程度）	報告会（1日）
本サービスの趣旨、評価内容及び評価対象部門、評価形式、実施スケジュールについて合意いただきます。	ご担当者様インタビュー、実機調査を通じてセキュリティ対策の現状に関わる情報を収集します。	収集したデータを集計・分析・評価し、貴社向けのご報告書を作成します。	最終報告会を実施し、評価結果のご報告及び、評価に基づいた改善提言を実施致します。

プロジェクトの実施体制

セキュリティコンサルタント、セキュリティエンジニア
1～2名での対応を予定

プロジェクトマネージャ セキュリティコンサルタント 1名	プロジェクト管理、調査データ収集、分析、レポート作成、報告会を担当
セキュリティエンジニア 1名	調査データ収集、分析を担当

プロジェクトの成果物（例）

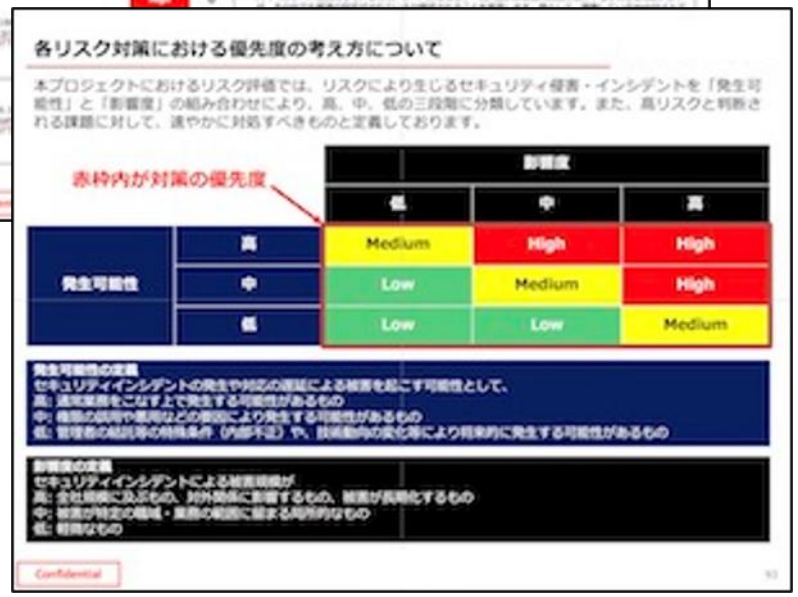
サイバーリスク評価報告書

1. プロジェクトの実施概要
   - 1-1. 評価の実施背景と目的
   - 1-2. 評価の実施内容
   - 1-3. 評価の実施スケジュール
   - 1-4. 評価の実施対象範囲
2. エグゼクティブサマリー
3. 詳細解説
   - 3-1. 戦略の評価
   - 3-2. 技術的対策の評価
   - 3-3. 組織的対策の評価
   - 3-4. 人的対策の評価
   - 3-5. 物理的対策の評価
4. 考察並びに今後推奨される対策

※プロジェクトの内容や期間は、対象物やスコープによって変化する場合もございます。

成果物のイメージ

以下は成果物の一例です。
成果物のフォーマット形式に関してご指定がある場合はお申し付けください。



お問い合わせ

資料請求やお見積依頼など、お気軽にお問い合わせください。
担当からすぐにご連絡いたします。

お問い合わせフォーム

https://www.secure-iv.co.jp/contact

pr@secure-iv.com

098-943-2718

受付時間 9:00～18:00（土日祝祭日を除く）

会社概要

会社名	株式会社セキュアイノベーション
所在地	本社　　：沖縄県那覇市上之屋1丁目18番36号　沖縄映像センタービル3F 東京オフィス　：東京都渋谷区広尾1-7-20　TH広尾ビル 4F-N 名古屋オフィス：愛知県名古屋市中川区尾頭橋4丁目13番7号　503号室 福岡オフィス　：福岡県福岡市中央区渡辺通二丁目4番8号　福岡小学館ビル5F サービスオフィス福岡薬院18号室
設立	2015年10月21日
代表取締役社長	栗田 智明
事業内容	セキュリティ機器・ソフトウェアの運用監視 セキュリティコンサルティング、セキュリティ診断 セキュリティ人材の派遣 システム・サイトの構築および開発 地域活性化プロジェクトの企画実施
許可・認定等	JIS Q 27001:2014(ISO/IEC 27001:2013) ISMS認定取得(登録番号 IS127) ［本社・東京オフィス取得］ JASA情報セキュリティサービス基準審査登録（セキュリティ脆弱性診断サービス） 労働派遣事業（許可番号：派47-300169）
会社ホームページ	https://www.secure-iv.co.jp/