# セキュリティリスクレポート

NTTコムウェア

**経営者様、情報セキュリティご担当者様**

## こんなお悩みありませんか？

自社のセキュリティリスクを把握したい

簡単にセキュリティリスクを診断したい

どこから手を付けたらいいか分からない

外部に委託しようにもどこも費用が高い

## セキュリティ対策を疎かにすることで想定されるリスク

- 信用の失墜
- 取引停止
- 競争力低下
- 機会の損失
- 株価下落
- 風評被害
- 行政指導
- 費用損害
- 業務停止
- 損害賠償

**気づいていないリスクが最大の脅威**

## 情報セキュリティリスクを可視化してみませんか？

お客様のセキュリティリスクの可視化と
適切な対策案をご提示します。

## セキュリティリスクレポートとは？

| 技術的対策 | 物理的対策 | 人的・組織的対策 |
|---|---|---|
| ・インターネット出入口対策<br>・端末管理<br>・サーバ/ミドルウェア管理 | ・入退室管理<br>・大規模災害にも耐えられるデータセンタの選定 | ・セキュリティポリシー等ルール作り<br>・セキュリティ専門家の育成 |

情報セキュリティ対策の種類は大きく3つに分けられます。本サービスでは"技術的対策"についてお客様環境の現状把握とリスクの有無を調査します。その後リスクへの対応策を提示いたします。

## サービスの流れ（ヒアリングから最終報告まで1～1.5ヵ月程度で実施）

**01 ヒアリング**

セキュリティ診断項目に基づく現状対策の調査

※お客様作業(ヒアリングシート作成)：2～3時間程度

**02 実機確認**

業務端末を用いた実際のセキュリティ対策状況の確認

※打合せ：1～2時間程度

**03 分析**

ヒアリング内容および実機の確認をもとにリスク評価の実施

※弊社作業：3週間程度

**04 中間報告**

リスク提示と認識の共有、分析結果に関する詳細レポートの提示、およびご報告

※打合せ：1～2時間程度

**05 最終報告**

想定されるリスクに対する具体的な対策案のご提案

※打合せ：1～2時間程度

## レポート内容

- ●現構成のセキュリティリスクを解説
- ●分析結果の共有
  1. 分析結果
  2. 検出された箇所
  3. 主なリスクにおける事例紹介
- ●リスクに対する対策案の提示

※対策案の一例

ゼロトラスト型セキュリティサービス

サイバー保険付き脆弱性診断サービス

s-WorkProtector

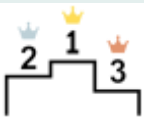
お客様の業務環境、及び、セキュリティ対策の現状を幅広くヒアリングし、リスクの見える化と推奨する対策をレポートにまとめて報告いたします。

## セキュリティリスクレポートで得られるメリット

**メリット1**

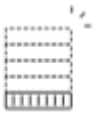
現状のセキュリティリスクの見える化

**メリット2**




優先順位を付けた対策を提示

**メリット3**



低コストで効果的なレポートを提供

NTTコムウェア

詳細をご希望の際は、営業担当者までお問合せください

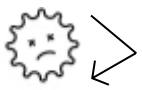
dreams-ml@nttdocomo.com

## 診断項目例

**入口対策（メール）**
- 危険度の高い拡張子を持つ添付ファイルのメール受信を拒否する
- メールの添付ファイルのウィルスチェックを行う

**ID管理**
- クラウドサービスのID管理が適切に行われている
- 従業員の雇用/退出と連動したID管理ができている

**リモートアクセス**
- 社内NWへのリモートアクセスにおいて適切に認証が行われている



**社内からのWebアクセス/社外でのWebアクセス**
- 業務に不要なWebサイトへのアクセスをフィルタリングする
- マルウェア設置サイトおよびC＆Cサーバへの通信をブロックする
- HTTP/HTTPS通信ログを取得する

**端末管理等**
- ウィルス対策ソフトで既知のウィルスをブロックする
- パターンファイルが最新化されている
- ふるまい検知型のエンドポイントセキュリティを導入している

**クラウドサービス**
- 利用可能なクラウドサービスを制限している
- クラウドサービスの利用において、アクセス元の制限や多要素認証を実装している

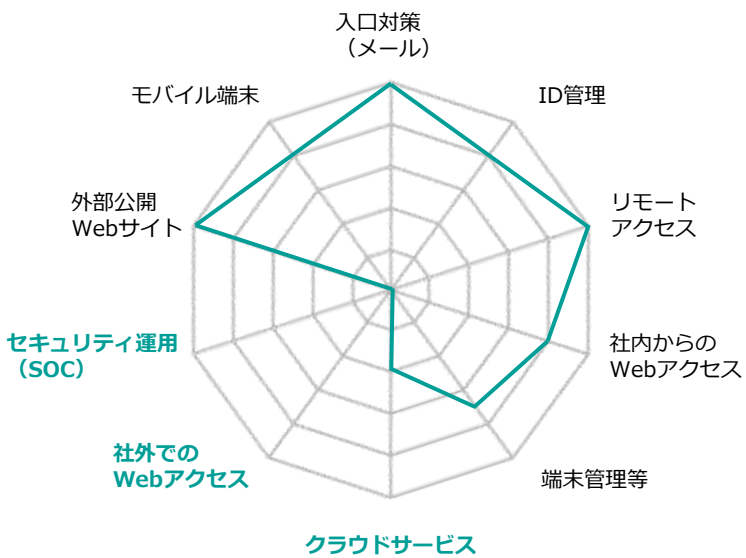
**セキュリティ運用（SOC）**
- ファイアウォールやIPS/IDS、プロキシサーバ等のログ監視・分析を行う
- セキュリティ状況を定期的に分析する

**外部公開Webサイト**
- 自社公開Webサイトへのセキュリティ対策がされている

**モバイル端末**
- スマートフォンなどのモバイル端末にて業務を行う場合にモバイル端末の管理、セキュリティ対応がとられている

## A社の事例（各項目に対する対応状況）

### ココがリスク！ セキュリティ運用（SOC）
- セキュリティ運用がされていないためインシデントを見過ごすリスクがある
- インシデント発生時の対応が迅速に行われない可能性がある

### ココがリスク！ 社外でのWebアクセス
- PCの社外持出時に不正サイトへのアクセスによるマルウェア感染により業務停止や情報漏洩のリスクがある

### ココがリスク！ クラウドサービス
- クラウドサービス全般の制限や管理が不足しており情報漏洩につながるリスクがある