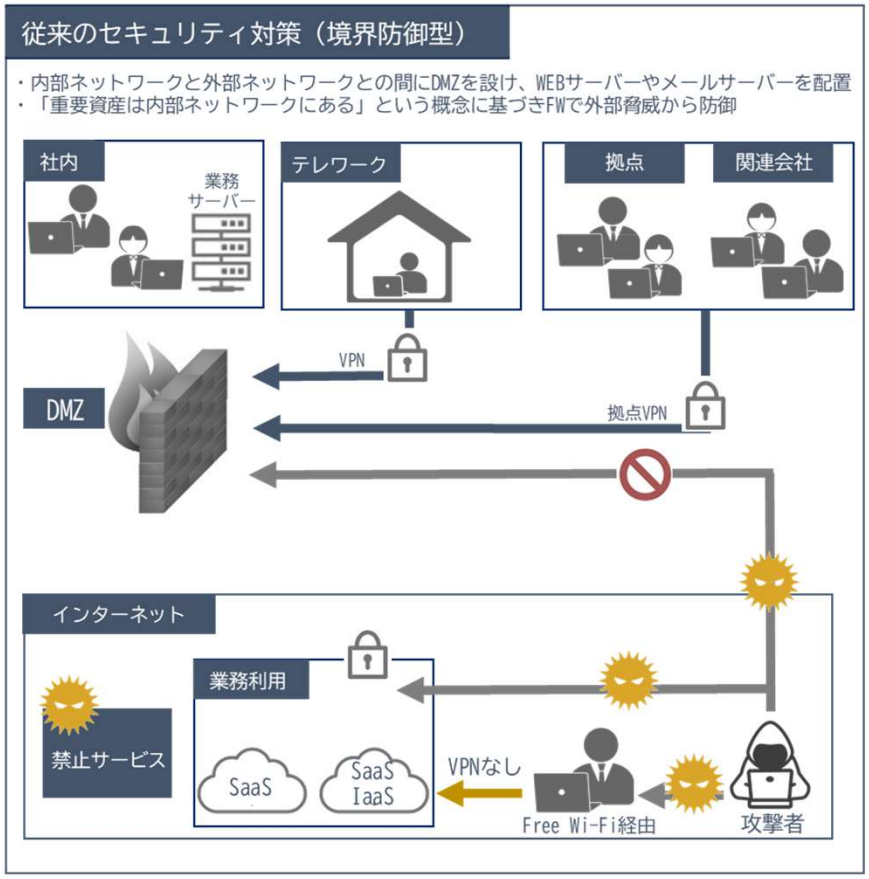
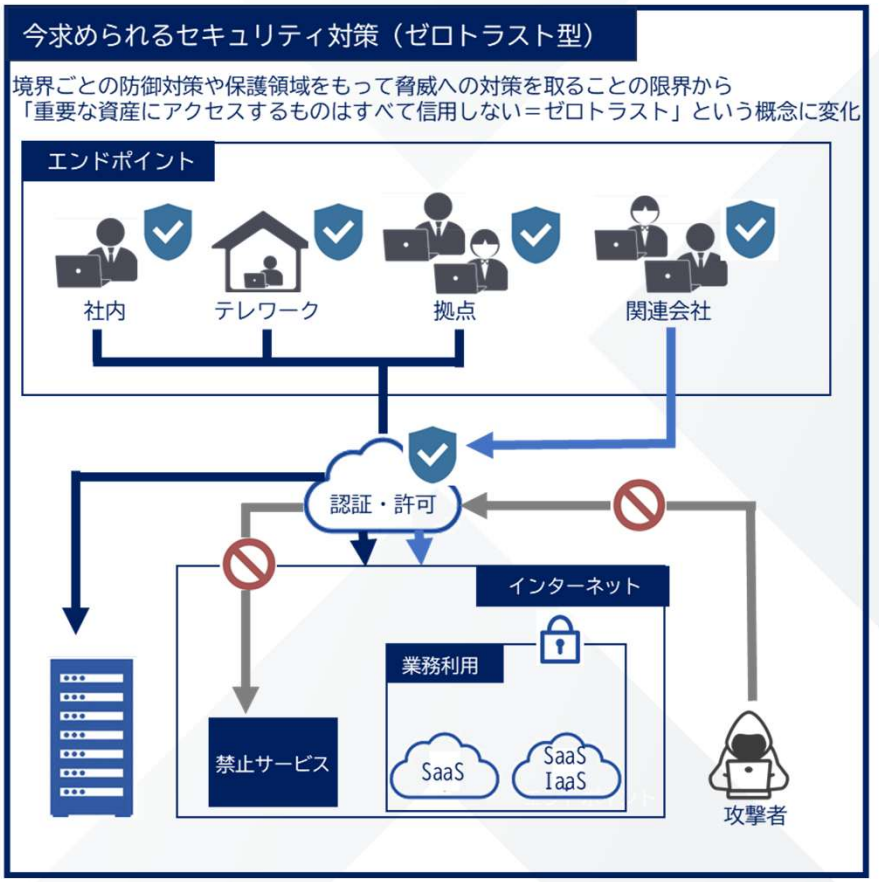

セキュリティリスク分析
V-Sec
～Visualizing Security～

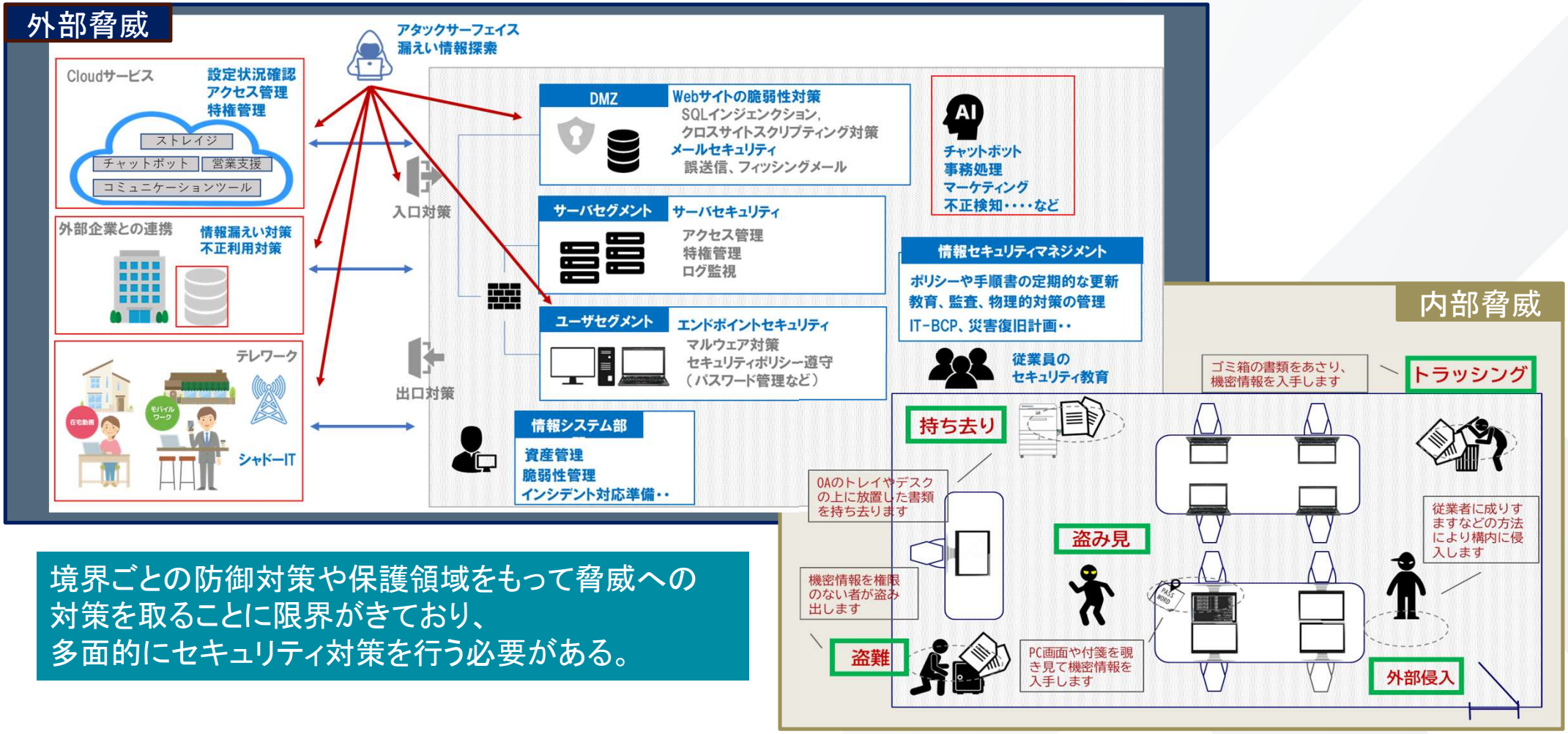
セキュリティリスク分析　実施企業増加の要因

セキュリティ対策の概念も境界防御からゼロトラストセキュリティの時代へと
変化しており、その概念に基づいた対策強化を図る企業が増えている。





脅威に対して迫られるセキュリティ対策



境界ごとの防御対策や保護領域をもって脅威への
対策を取ることに限界がきており、
多面的にセキュリティ対策を行う必要がある。

セキュリティ強化はアセスメントから始まる

現在では、様々なセキュリティガイドラインの発行やセキュリティ対策選択肢の複雑化などもあり、セキュリティ対策強化に取り組む企業では
〝何を・どうやって・誰が・どこまで実施すれば良いのか〟という課題が顕著です。
アセスメントにより現状を可視化し、強化すべきポイントや優先順位を決定し計画的なセキュリティ対策強化が費用対効果と有効性の維持につながります。

現状把握 アセスメント	対策優先 順位の決定	対策の実施	インシデント対応の 準備	インシデント 初動対応	収束支援

今回のご提案

【包括的リスクを可視化】
セキュリティリスク分析（V-Sec）

【人材育成のための可視化】
セキュリティ人材アセスメント

【ネットワークの脆弱性可視化】
侵入影響範囲調査

コンサルティング支援
- 各種ガイドライン準拠
- 認証取得
- サプライチェーン統制

人材教育・育成支援
- 人材アセスメントコンサル
- 各階層別トレーニング
- エンジニアトレーニング
- eラーニング

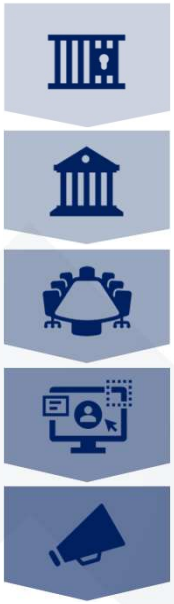
セキュリティツール実装支援
- 資産管理
- EDR/NDR等
- ID管理ツール

診断・調査支援
- Discovery（ASM）
- クラウド監査
- 各種脆弱性診断
- ペネトレーションテスト

インシデントへの備えが重要

【組織的備え】
- CSIRT構築支援
- インシデント対応ワークショップ
- CSIRT強化訓練
- リテイナーサービス
- CYBERGYM Express会員

【個人のスキルアップ】
各種インシデント対応の備えとなるトレーニングを提供
- インシデント対応初級
- エッセンシャル
- フォレンジック
- OTエッセンシャル
- 金融向けエッセンシャル



被害範囲の調査と確認

被害発生事実を適切な機関/組織へ報告および相談

第三者委員会を発足し対応にあたる

ダークウェブ上のリークサイト状況確認と漏洩情報の取得

外部への公表、IRについて

セキュリティリスク分析の目的

企業に潜むリスクを包括的に可視化をするセキュリティリスク分析は、下記目的のために多くの企業で実施されています。最終目標は費用対効果を考えたサイバーセキュリティ対策を実現になります。

多層防御の観点からセキュリティリスクを明確化

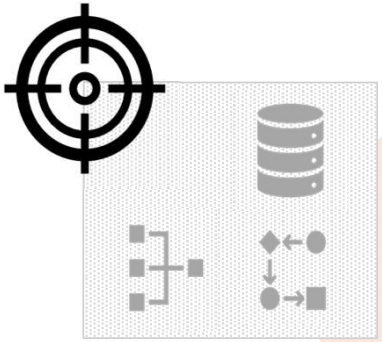
費用対効果を考えたセキュリティ対策立案

経営陣と現場のリスクレベル共有＝適切な対策

事業継続性の確保

セキュリティリスク分析の必要性

多くの組織が十分な検討を行わないままセキュリティ対策を実施するため、効果的かつ有効性が維持される対策がとられていないのが実情です。
セキュリティ対策（投資）をどのレベルで実施するかは、リスクを把握（即ち、守るべき情報資産・リスクレベル・リスク発生頻度などを検討）したうえで、計画的に取り組むことです。



アセスメントに基づかない
セキュリティ投資は暗闇に向かって
やみくもにダーツを投げるようなもの！

セキュリティリスク分析『V-Sec』 ― 評価基準 ―

■総合評価の基準

ISO/IEC27001の管理策の分類に基づき、組織的、人的、物理的、技術的の4分類に分け、各分類ごとでの対策レベルを評価します。

	組織的	人的	物理的	技術的
LEVEL 4	情報セキュリティは監視、レビューされ、見直され、常に最適化されている	情報セキュリティ意識醸成のためのプログラムは最新の脅威を反映してアップデートした内容となっている	重要な情報資産の設置区域へは組織の従業員による侵入も含め、身元確認、ボディチェック等により補完されている	認識したリスクに応じて、先端のテクノロジーを活用した網羅的な技術的対策が取られている
LEVEL 3	情報セキュリティは網羅性を確保した状態で文書化され、計画的に実施されている	情報セキュリティ意識醸成のためのプログラムは網羅性を確保したうえで組織的、計画的に行われている	重要な情報資産の設置区域へは組織の従業員のうち、当該業務の関係者のみが侵入可能なレベルである	認識したリスクに関して、網羅的に技術的対策が取られている
LEVEL 2	情報セキュリティは文書に従い実施されているが、網羅されていない	情報セキュリティ意識醸成のためのプログラムは組織的、計画的に行われているが対象のごく一部が網羅されていない	重要な情報資産の設置区域へは組織の従業員のみが侵入可能なレベルである	基本的な対策に加えてプラスの技術的対策が採用されているが、認識したリスクへの対策の一部が人的な管理に依存している
LEVEL 1	情報セキュリティは場当り的に行われているが、文書化されておらず組織だった取組みが行われていない	情報セキュリティ意識醸成のためのプログラムは行われているが場当り的、または部分的である	重要な情報資産の設置区域に第三者が侵入可能なレベルである	技術的な情報セキュリティはマルウェア対策ソフト、FWなどを中心に基本的なのものが行われている
LEVEL 0	情報セキュリティ対策が実施されていない	情報セキュリティ意識醸成のためのプログラムが存在しない	重要な情報資産の設置区域が把握されておらず、物理的対策についての必要性の認識がない	人的な運用に依存し、技術的なセキュリティ対策はほとんど存在しない

当社の認証取得事業および情報セキュリティ事業における3,000件超のコンサルティング支援実績をもとに評価したものです。あくまでアセッサーの定性的な判断によるものですのでご了承ください。

■対策優先度の考え方

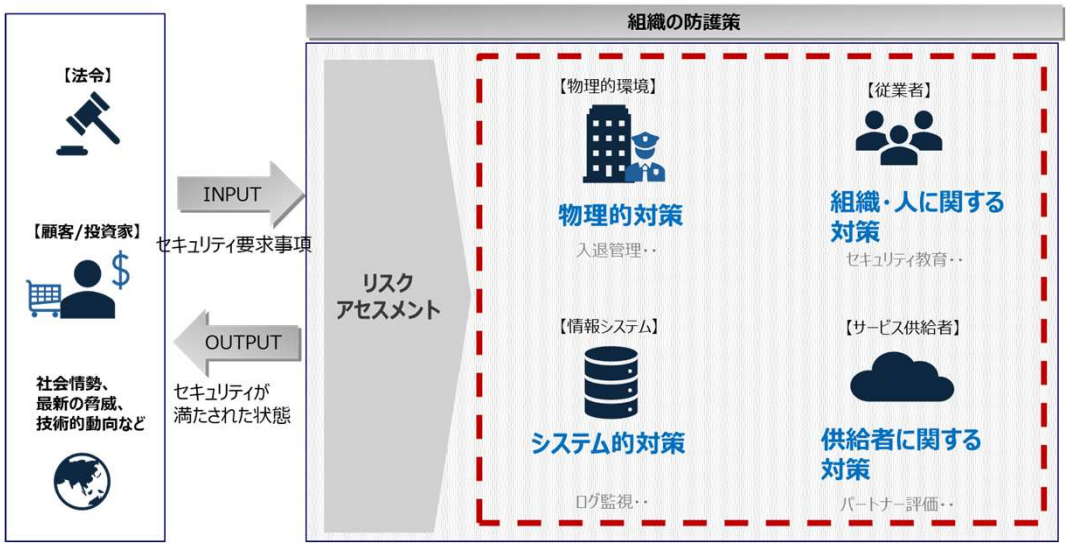
本セキュリティリスク分析は、リスクの定性的分析になりますので、各リスクの重大度・影響度や危険度などの定性的な部分を取り上げて分析します。一般的にISO27001で使われる分析手法を採用しています。

インパクト＼発生可能性	低	中	高
大	Mid.	High	High
中	Low	Mid.	High
小	Low	Low	Mid.

※“インパクト”は
直接的な影響を受ける資産の重要性を考慮し判定しています。
※“発生可能性”は
現状の対策を考慮のうえで想定するリスクの発生可能性を判定しています。

セキュリティリスク分析『V-Sec』 ― スコープ ―

V-Secは情報セキュリティを組織的な活動ととらえ、
ネットワーク（技術的）対策だけでなく、ガバナンスやマネジメントの観点からなど
多面的なセキュリティリスク分析を行います。



システムの対策だけでなく、人や組織に対する対策、物理的な対策などの各セグメントでのセキュリティ対策もバランスよく行われているか分析します。

平時における攻撃等からの防御と、非常における対応の両方の観点からもリスクを分析します。

セキュリティリスク分析『V-Sec』 ― サービス概要 ―

自社セキュリティ対策の方向性とゴールを定めて、今後のセキュリティ強化における費用対効果を最大限発揮！
お客様のご要望に応じて、セキュリティリスク分析V-Secの結果に基づいたセキュリティ強化実装に関しても総合支援が可能です。
※内部リスク：企業を包括的に（人的・組織的・物理的・技術的観点）リスク分析
※外部観点の分析：攻撃者目線で外部から見て攻撃対象となりうるリスクがあるかを分析

STEP1　V-Sec STandard・FActory・HOspital

【内部リスク分析】

V-Sec ST

一般企業向け
〈参照ガイドライン〉
✓ISO27001　✓NIST CSF

V-Sec FA

製造業向け
〈参照ガイドライン〉
✓工場におけるサイバー・フィジカル・セキュリティ対策ガイドライン
or
✓自工会ガイドライン

V-Sec HO

医療業界向け
〈参照ガイドライン〉
✓厚生労働省:医療情報システムの安全管理に関するガイドライン6.0

【本調査】
・ネットワーク図の把握
・セキュリティ規程査読
・ヒアリングシートのご記入
・ヒアリング実施

【分析・報告】
・脆弱性可視化
・現状課題
・強化の方向性
・セキュリティ対策のご提案

【外部視点の分析】

Security Scorecard
10項目を5段階評価
A B C D F

攻撃者が初期偵察で収集する貴社データを収集／調査／分析／評価することで、「攻撃者から狙われる脆弱性か否か」を知ることができる！	3. パッチの適用頻度	7. キューピッド・スコア
	4. エンドポイント・セキュリティ	8. ハッカーチャッター
1. ネットワークセキュリティ	5. IPレピュテーション	9. 機密情報漏洩監視
2. DNSの正常性	6. アプリケーションセキュリティ	10. ソーシャル・エンジニアリング

STEP2　別途オプション

コンサルティング支援
・各種ガイドライン準拠
・認証取得
・サプライチェーン統制

人材教育・育成支援
・人材アセスメントコンサル
・各階層別トレーニング
・エンジニアトレーニング
・eラーニング

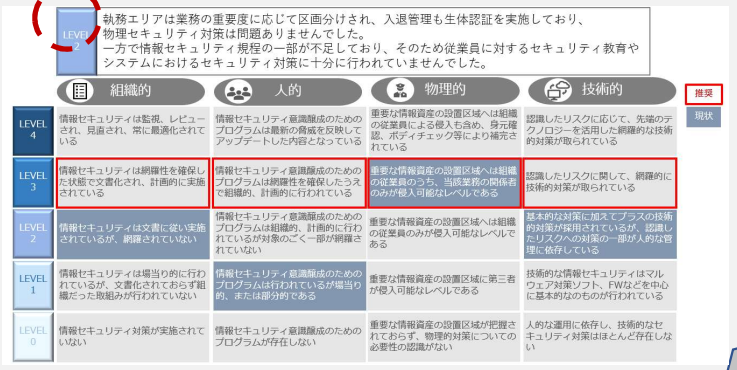
セキュリティツール実装支援
・資産管理
・EDR/NDR等
・ID管理ツール

診断・調査支援
・Discovery（ASM）
・クラウド監査
・各種脆弱性診断
・ペネトレーションテスト

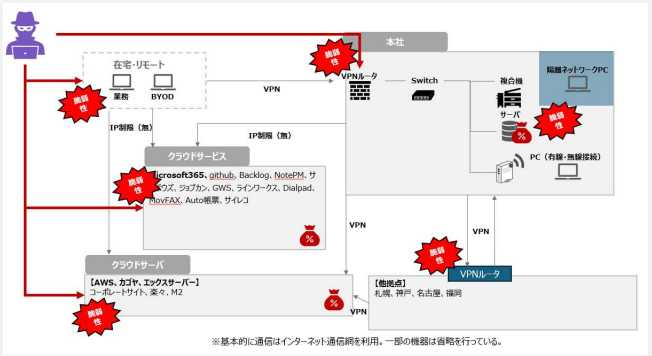
セキュリティリスク分析『V-Sec』 ― STEP1 内部リスク分析 ―

V-Secは自社の情報セキュリティリスクについて経営陣に把握していただくことを目的にしており
ビジュアル表現にこだわり直感的理解できるような報告書になるように工夫しています。

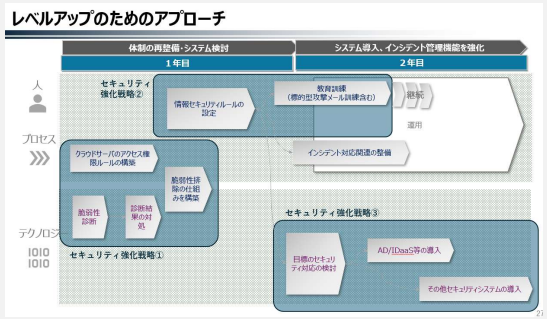
総合評価



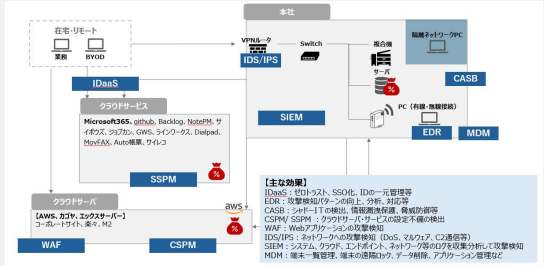
想定リスクシナリオ



対策の方向性のアドバイス



セキュリティの理想的像（ネットワーク構成イメージ）



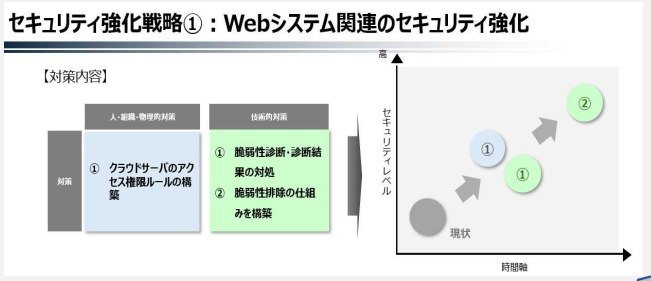
現状対策評価

誰にでも分かりやすい表記

	タイトル	検出事項	懸念領域	優先度	影響	発生可能性
10	アクセスコントロール	組織内の入退社に伴う権限変更は各責任者の申請に従って行われているが、組織内の異動については管理が行き届いていない可能性がある。また、定期的な棚卸なども行われていない。	不要なアクセス権限が残留してしまい、その権限を攻撃者に利用される、攻撃者が攻撃に使用する不正アカウントを作ってもそれを察知できない可能性がある。また、従業者が本来閲覧してはならない情報にアクセスできてしまう可能性がある。	Mid	高	低
11	アクセスコントロール	アクセス権の共有利用を行っている者に対して、退職時のパスワード変更などがルール化されていない。	退職者の不正ログインを防ぐことができない。	High	高	中
12	ネットワークセキュリティ	ネットワーク図の更新がなされていない。（組織のネットワークについて、部分的なものは存在するが、全体を示すものが作成されていない。）	組織のネットワークの最新状態を把握することができず、必要なリスク対策が漏れたり、インシデント発生時の対策に調りが出る可能性がある。	Low	中	低
13	ネットワークセキュリティ	内部ネットワークは部署などの観点からセグメント分けがなされていない部分があった。	外部の攻撃者による内部ネットワークへの侵入が成功した場合、他のデバイス等に被害が拡大する危険性がある。また、従業員があるべきアクセス権限を越えて情報システムにアクセスする危険性がある。	Low	中	低
14	ネットワークセキュリティ	Wi-Fi接続認証の仕組みが端末ごとではなく、全体で同一のパスワード設定を行っている。	パスワード漏洩、退職者の不正利用などによって組織内ネットワークに不正アクセスされる可能性がある。 ※パスワードを公開していなくても、PC上で接続実績のある通信のパスワードを知るすべが存在する。	Mid	高	低

対策選択肢の提示

具体的で想起しやすい例示



セキュリティリスク分析『V-Sec』 ― STEP1 実施プログラム ―

V-Sec ST(一般業界)、FA(製造業)、HO(医療業界)等各業界のガイドラインを参照し、
お客様のセキュリティリスクをベースにリスク分析を実施します。

Standardプラン

【ヒアリング対象者】

・セキュリティを主管する部門の責任者、または担当者

【実施内容】

・ヒアリングとネットワーク図による現状の対策確認

【対象範囲】

・組織のセキュリティポリシー、セキュリティ規程

・NW:LAN(インターネット境界から内側)、WAN、リモートアクセス

・内部利用の情報システム主管の主要数システム

【目的】

人的・組織的・物理的・技術的な多面的観点から、企業のネットワーク及び
ガバナンスやマネジメントにおける脆弱性やリスクレベルを分析する

※一般的なISO27001等の監査よりもサイバーセキュリティに踏み込んだリスク分析を実施します

オプション

- アセスメント対象 部署・拠点の追加
- 事業部制における 対象部署複数への実施
- 自社アプリ開発 プロセスへの実施
- 工場(製造ライン)
- 外部向け提供サービス への実施
- 業務プロセス/DFD (Data Flow Diagram) ベースでの評価
- 参照ガイドライン の追加
- 工場(OTセキュリティ)

etc

セキュリティリスクの可視化、対策を強化したい対象
に対して、柔軟に対応します。

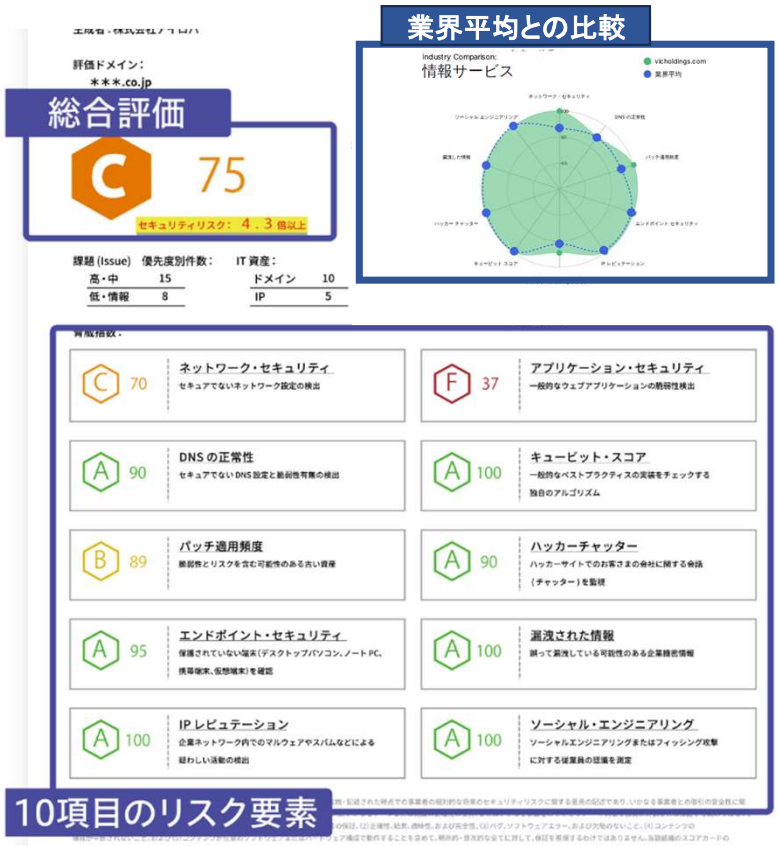
各種ガイドライン対応

- 各種ガイドラインへの文書適合確認
- 各種ガイドラインへの準拠状況の確認

ガイドラインの準拠状況、対応可否については
『ガイドライン対応アセスメント』にてご支援可能です。

セキュリティリスク分析『V-Sec』 ― STEP1 外部視点の分析 ―

巧妙化するサイバー攻撃に対して、貴社の外部から狙われやすい弱点を放置してはいませんか？
客観的な把握が難しい企業のセキュリティリスクを、攻撃者の目線からターゲットポイントを定量化します。



下記10個のカテゴリーをA～Fの5段階で評価

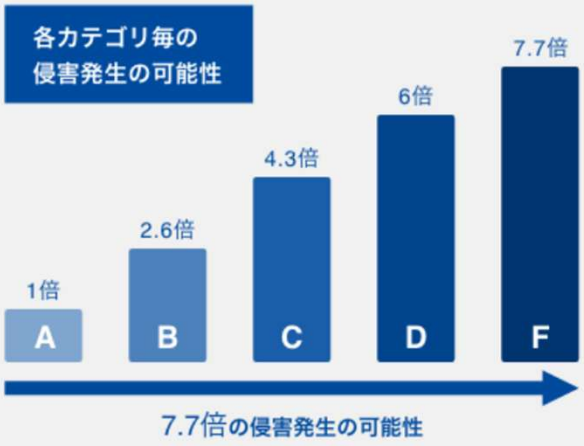
ネットワークのセキュリティ	インターネットからアクセスできるソフトウェアについて、安全性や設定の誤りなどの脆弱性が無いかを検出します。【SSL、RDP、SSH、LDAP、FTP等について】
DNSの正常性	DNSの設定や脅威について脆弱性が無いかを検出します。【SPF等について】
パッチの適用頻度	OSやアプリケーションに対し適切にパッチを適応しているかや、サポートが切れていないかなどを検出します。【CVE、EOS等について】
エンドポイント・セキュリティ	端末のIPとUser Agentの情報から古いブラウザやプラットフォームを利用していないかなどを検出します。【OS、ブラウザ等について】
IPレピュテーション	独自のシンクホールシステムで、マルウェアの通信を取り込み解析を実施し、通信もとIPを解析し、帰属する企業を特定します。【プロキシ、マルウェア、アドウェア等について】
アプリケーションセキュリティ	WebサイトやCMSなどの設定上の脆弱性を検出します。
キューピッド・スコア	外部から観測した情報を組み合わせて、実際の脅威リスクを判定します。【ランサムウェア等について】
ハッカーチャッター	一般にはアクセスが困難なアンダーグラウンドのハッカーサイト等をモニタリングし、御社に関する会話や情報のやり取りを検出します。
漏洩された情報	インターネット上に漏洩した機密情報から企業を特定し、漏洩した情報から御社が直面するセキュリティインシデントの可能性を検出します。
ソーシャル・エンジニアリング	SNSアカウント、個人金融アカウント、悪用可能なマーケティングリストなどに従業員が企業アカウントを使用するなど、ソーシャルエンジニアリングされるリスクを検出します。

※実際にお客様のシステムに負荷をかけることなくインターネット上から非侵入で収集できる情報に基づき分析します。

セキュリティリスク分析『V-Sec』 ― STEP1 外部視点の分析 ―

攻撃者の目線に立ったレイティング

本サービスは、攻撃者が標的企業の情報収集を行うフェーズにフォーカスし、攻撃者目線で企業のセキュリティ対策状況を診断し、レイティングを行います。
診断対象企業に内在する脆弱性のみならず、スコアを確認することによって「攻撃者からの狙われやすさ」を把握することができ、継続的に良好なスコアを保つことで、攻撃されにくい環境を維持することが可能となります。



スコアとセキュリティ侵害の相関関係

SSC社が評価したスコアとセキュリティ侵害との間には相関関係があることが、統計的に確認されております。
過去セキュリティ侵害が発生した数千社に対してSSC社が統計分析を行ったところ、Fスコアの企業では、Aスコアの企業と比較し7.7倍ものセキュリティ侵害が発生しており、SSCのスコアを改善することが、セキュリティ侵害の発生を低減させることにつながるといえます。

弊社のセキュリティリスク分析『V-Sec』 の強み

弊社の提供するセキュリティリスク分析『V-sec』は、官公庁を始め延べ5,000社以上の情報セキュリティ監査を実施している、経験と卓越した知識有するコンサルタントチームが実施します。高いアセスメント・監査品質を提供しますので安心してご利用いただけます。

強み1）内部だけでなく、外部観点（アタックサーフェス）での分析

企業内部における脆弱性の可視化だけでは無く、外部の攻撃者目線で攻撃対象となりうるリスクを可視化します。内部・外部両方の観点でのリスク分析が弊社の大きな特徴。

強み2）資格保有者によるリスク分析

システム監査技術者およびISO27001審査員補など、政府機関が実施するシステム監査・情報セキュリティ監査において求められる資格要件を満たす人材がアセスメントを行います。

強み3）公的に認められたサービス

V-secは経済産業省の「情報セキュリティ監査サービス基準適合サービス」の承認を受け、IPAの『情報セキュリティサービス基準適合リスト』に掲載されています。

情報セキュリティサービス基準適合サービスリストの公開：IPA 独立行政法人 情報処理推進機構

セキュリティリスク分析『V-Sec』 ― 費用 ―

項目	V-Sec ST	V-Sec FA	V-Sec HO
評価指標	・ISO27001 ・ISO27002 ・NIST-CSF	V-sec STの評価指標と合わせて、 以下のいずれかの参照ガイドライン ・工場におけるサイバー・フィジカル・ セキュリティ対策ガイドライン or ・自動車産業サイバーセキュリティガイドライン （自工会・部工会）	V-sec STの評価指標と合わせて、 以下の参照ガイドライン ・医療情報システムの安全管理に関する ガイドライン
期間	2～3週間		
お客様の作業	ヒアリングシートのご記入・ヒアリング対応　のみ		
提供依頼資料	ネットワーク図＋セキュリティポリシー		
V-sec Step1 内部リスク分析	V-sec報告書ご提出		
V-Sec Step2 外部リスク分析	セキュリティスコアカードご提出（詳細版ご希望の場合は別途お見積）		
価格(税抜)	80万円		

セキュリティリスク分析『V-Sec』 ― STEP2 オプション ―

V-Sec終了後にお客様の分析結果状況やご要望に合わせて様々なご支援が可能です。
サイバーセキュリティのトータルソリューションカンパニーとして、お客様を万全にサポートいたします！

今回のご提案

現状把握 アセスメント → 対策優先順位の決定 → 対策の実施 → インシデント対応の準備 → インシデント初動対応 → インシデント収束支援

【包括的リスクを可視化】
セキュリティリスク分析（V-Sec）

【人材育成のための可視化】
セキュリティ人材アセスメント

【ネットワークの脆弱性可視化】
侵入影響範囲調査

コンサルティング支援
- 各種ガイドライン準拠
- 認証取得
- サプライチェーン統制

人材教育・育成支援
- 人材アセスメントコンサル
- 各階層別トレーニング
- エンジニアトレーニング
- eラーニング

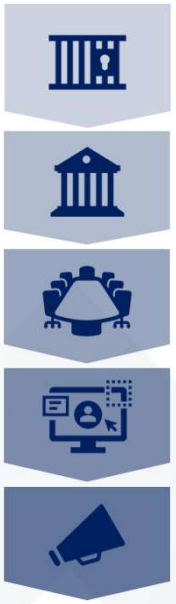
セキュリティツール実装支援
- 資産管理
- EDR/NDR等
- ID管理ツール

診断・調査支援
- Discovery（ASM）
- クラウド監査
- 各種脆弱性診断
- ペネトレーションテスト

インシデントへの備えが重要

【組織的備え】
- CSIRT構築支援
- インシデント対応ワークショップ
- CSIRT強化訓練
- リテイナーサービス
- CYBERGYM Express会員

【個人のスキルアップ】
各種インシデント対応の備えとなるトレーニングを提供
- インシデント対応初級
- エッセンシャル
- フォレンジック
- OTエッセンシャル
- 金融向けエッセンシャル



被害範囲の調査と確認

被害発生事実を適切な機関／組織へ報告および相談

第三者委員会を発足し対応にあたる

ダークウェブ上のリークサイト状況確認と漏洩情報の取得

外部への公表、IRについて

セキュリティリスク分析『V-Sec』 ― 実績例 ―

企業	業種	実施コース	実施結果内容
A社	東証一部上場　建設業	セキュリティリスク分析	テレワークのルール改善という課題を見つけることが出来ました。
B社	大手放送会社	セキュリティリスク分析	アセスメントにより最適なセキュリティツールを導入。セキュリティコストの削減に成功。
C社	石油製品卸売・小売業	情報セキュリティ監査	自社のルールが現場業務の負担となっておりルール改善に取り組む。
D社	メディアコンテンツ制作	セキュリティリスク分析	今後のセキュリティ対策の優先順位が明確になり、今後のセキュリティ対策計画に反映されました。
E社	イベント会社	セキュリティリスク分析	エンドポイントの対策と社員教育の強化が優先順位と分かり改善開始。
F社	教育関係	情報セキュリティ監査	上場に向けたセキュリティ対策のために実施。現状の強化と新しい対策が明確化し継続支援。
G社	コンサルティング会社	セキュリティリスク分析	委託先のセキュリティチェックとしてV-secを活用されました。
H社	小売業	情報セキュリティ監査	拠点でのルールの形骸化や未実施が多く分かり、監査およびセキュリティ対策強化されました。
I社	金融業	情報セキュリティ監査	TLPT（脅威ベースのペネトレイションテスト）実施の優先順位を決定するための分析でした。
J社	自動車部品製造業	セキュリティリスク分析	自工会ガイドライン準拠の体制構築のために実施したうえセキュリティ強化も実施。
K社	製造業	セキュリティリスク分析	ある程度の対策は実施していたが、第三者評価と今後の強化ポイントを知りたく分析されました。