自社の抱えるリスクを可視化する

セキュリティリスク分析『V-Sec』

攻撃者に狙われるサプライチェーン

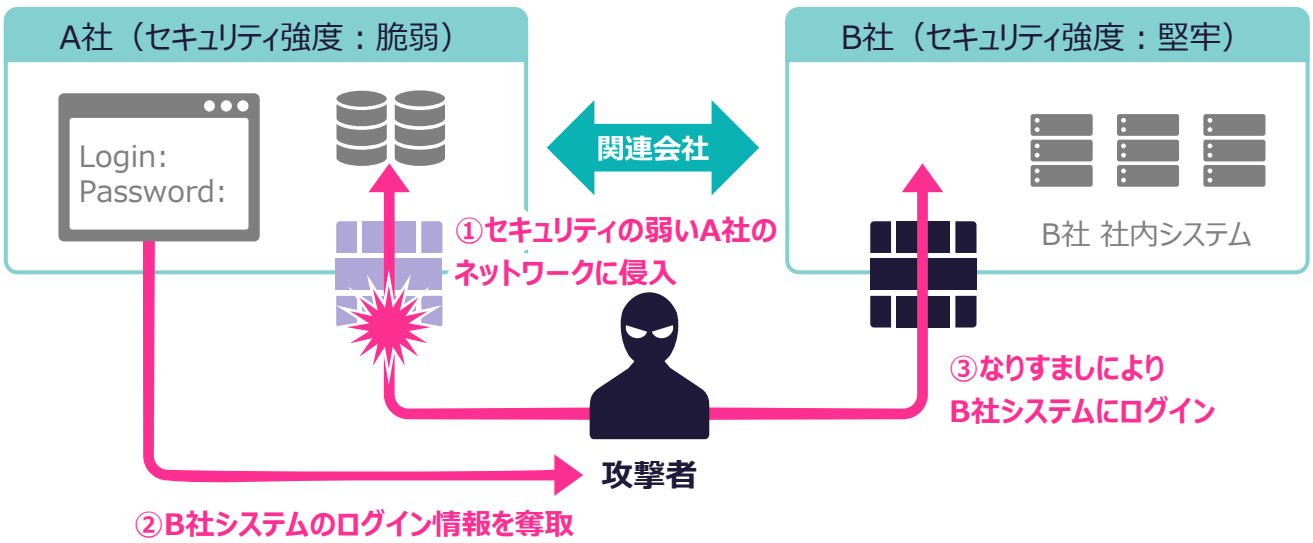
IPAの公開する「情報セキュリティ10大脅威 2024」において**「サプライチェーンの弱点を悪用した攻撃」**は2位にランクインしており、6年連続6回目の選出になっています。

同法人の公開する「サイバーセキュリティ経営ガイドライン」では、**「経営者が認識すべき3原則」**、**「サイバーセキュリティ経営の重要10項目」**のいずれにも、サプライチェーンに関する記述がされており、サプライチェーンにおけるセキュリティ対策はますます重要になっています。

攻撃者であるハッカーは、セキュリティの強固な大企業ではなく、**比較的セキュリティの脆弱な中小のサプライチェーン企業を経由**して大企業を狙います。

順位	組織向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した被害
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

引用： IPA「情報セキュリティ10大脅威 2024」



セキュリティリスクに対する適切な対策と自社の状況の可視化

「サイバーセキュリティ経営の重要10項目」の最初のステップとして、**「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」**が挙げられています。効果的かつ投資対効果の高いセキュリティを実現するための第一歩としてリスクアセスメントにより組織内部のリスクを可視化することが重要です。

セキュリティツールの導入だけでなく、社内規定の見直しや社員教育は実施できていますか？

- **個々のセキュリティリスクの分析と対策すべき優先順位の設定**
- **セキュリティにまつわる規定や運用フローの見直し**
- **費用対効果を考えたセキュリティ対策の立案**

セキュリティリスク分析 V-Sec とは？

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）対策だけではなく、各業界のガイドラインに準拠したガバナンスやマネジメント等の観点から、多面的なセキュリティリスク分析を行うアセスメントサービスです。結果はレポート形式でわかりやすく明示し、さらなる対策強化に向けたアクションまでご提案します。

V-Sec トライアル　15万円

お試しプラン

内容	現状レポート、情報漏洩発生確率
目的	本調査前のセキュリティリスクチェックにより、現状の情報漏洩発生確率を数値化し確認

V-Sec スタンダード　120万円

1 拠点向け

内容	管理者へのヒアリングとネットワーク図による現状の対策確認
目的	各業界のガイドラインに準拠した調査を実施し、企業のネットワークおよびマネジメント等における脆弱性やリスクレベルを分析

V-Sec プレミアム　個別見積

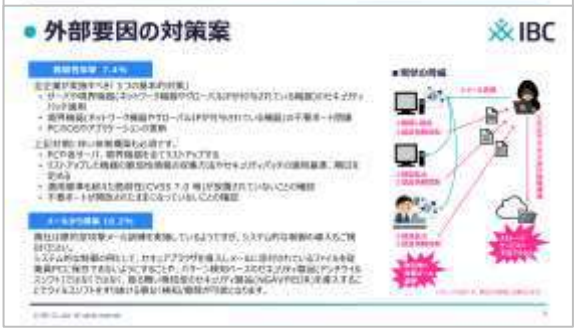
複数拠点向け。スタンダード＋下記

内容	現場担当者へのヒアリングによる業務現場実態調査
目的	現場のルール遵守状況や現場業務とルールとの乖離を調査分析。業務負担となっているルールの見直し等も検討

レポートサンプル　（抜粋 / 数値および内容はサンプルです）

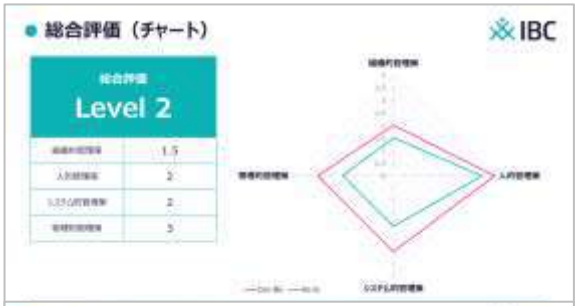
V-Sec トライアル

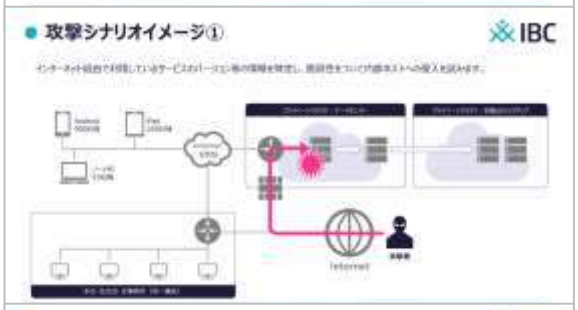
情報漏洩発生確率と対策ポイントを記載します。

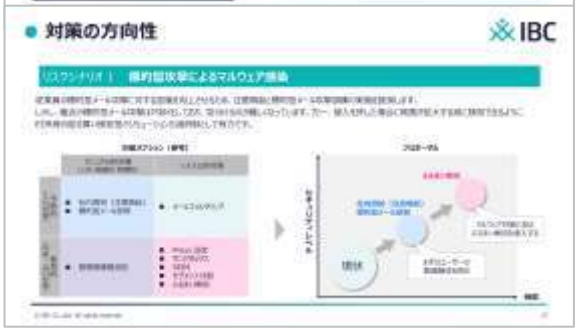


V-Sec スタンダード

より具体的な攻撃シナリオや、対策方針を記載します。







アイビーシー株式会社

本社
〒104-0033
東京都中央区新川1-8-8 アクロス新川ビル8F
tel.03-5117-2780　fax.03-5117-2781

西日本事業所
〒532-0003
大阪府大阪市淀川区宮原4-1-14 住友生命新大阪北ビル3F
tel.06-7653-1014　fax. 06-7177-0542