【サンプル】OTセキュリティ評価結果

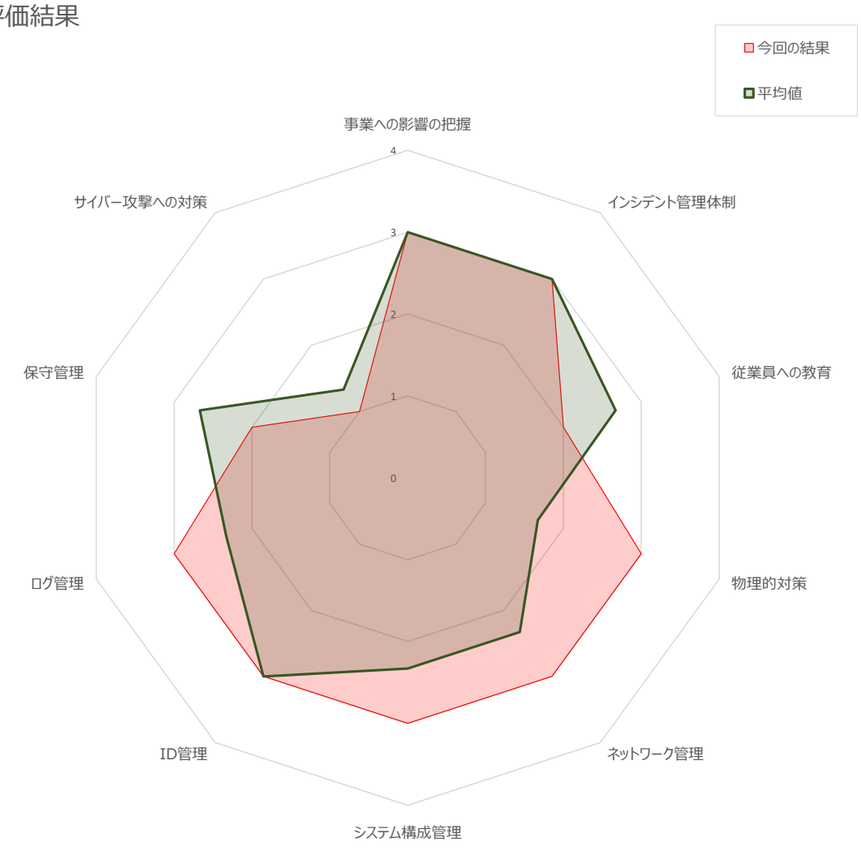
1．総評

評価結果の平均値	2.56
企業の平均値を上回る項目	4
企業の平均値に満たない項目	3

評価コメント

評価結果の平均値は2.56点でした。これは、企業の平均値と比較して高い評価結果となります。
企業の平均値を上回る項目が4項目、企業の平均値に満たない項目が3項目あります。
企業の平均値を上回る項目は「物理的対策」「ネットワーク管理」「システム構成管理」「ログ管理」です。企業の平均値に満たない項目は「従業員への教育」「保守管理」「サイバー攻撃への対策」です。「事業への影響の把握」「インシデント管理体制」「ID管理」については、企業の平均値と同等の対策が実施されています。
企業の平均値に満たない項目については、「３．項目別評価」の内容に従い、優先して追加対策を実施することを推奨します。

2．評価結果



3．項目別評価

大項目	質問内容	質問の意図	回答	平均値	今後実施すべき対応
事業への影響の把握	工場/生産ラインでインシデントが発生した場合の事業への影響度を経営層は把握していますか（していると思いますか）？	企業において、工場や生産ラインでインシデントが発生した場合の事業継続計画ができているかを確認しています。 生産ラインでインシデントが発生した場合、企業の存続に関わる影響度によって、準備しておくこと、優先順位が異なります。	3	3	内外環境変化に伴い、インシデント発生時の影響も変化します。経営層がタイムリーな意思決定を行うためには、定期的なBIAにより状況を把握する必要があります。
インシデント管理体制	工場/生産ラインにおけるインシデント（災害、障害、人災、セキュリティ事故など）発生時の体制はありますか？	工場や生産ラインでインシデントが発生した場合、速やかな対応をできる体制があるかを確認しています。従業員の安全、会社の資産の保全、顧客への情報提供等、インシデント対応は、インシデントの要因、規模、影響範囲などによって異なりますので、あらかじめインシデントの発生を想定し、体制を整えておくことが重要です。	3	3	DX、IoT化等の取組を進めると共にサイバー攻撃の脅威は高まります。サイバー攻撃によるインシデント発生時の手順、役割、責任を定めていくことが求められます。
従業員への教育	工場/生産ラインの従業員に対してセキュリティ教育を実施していますか。	工場/生産ラインに係る従業員へのセキュリティ教育の実施状況を確認しています。教育や訓練を通じて、従業員のセキュリティ意識の向上を図ることで、セキュリティリスクを低減することが重要です。	2	2.67	サイバー攻撃等のインシデントに対応していくためには、全ての従業員がセキュリティ意識を持つことが求められます。
物理的対策	工場/生産ラインへの入退室、機器の持ち込みを物理的に制限していますか。	工場/生産ラインの物理的なセキュリティ対策を確認しています。 工場/生産ラインへの部外者の立ち入りや不要な情報機器の持ち込みを制限・管理することで、セキュリティリスクを低減することが重要です。	3	1.67	工場/生産ライン内の特に重要な区画への立ち入り・機器持ち込みはより厳格な取り扱いが求められます。
ネットワーク管理	工場/生産ラインのネットワーク構成図を作成し、通信要件を一覧化していますか。	ネットワークを可視化し、セキュアなネットワークを構成しているかを確認しています。通信要件に従い、適切にネットワークを分離し、ネットワークに接続されている機器を把握することが重要です。	3	2.33	通信内容に基づきネットワークの分離や通信経路の制御を行うことで、不正通信の抑止や局所化、ネットワーク帯域の最適化を図ることができます。
システム構成管理	工場/生産ラインのシステム構成（ハードウェア資産、ソフトウェア資産及びそれらの設定内容・構成情報）を一覧管理し、脆弱性への対応を実施していますか。	工場/生産ラインを構成する機器及びソフトウェア並びにそれらの構成情報及び設定内容を把握しているかを確認しています。 インターネットからのサイバー攻撃は、機器及びソフトウェアの脆弱性を悪用します。システム構成を管理し、必要な脆弱性への対処をすることは有効な対策となります。	3	2.33	全てのシステムについてシステムの構成を把握し、堅牢な構成とすることで、新たに発生した脆弱性への対応を行うことが可能となります。
ID管理	工場/生産ラインを操作する際のIDを管理していますか。	工場/生産ラインを操作する際のID及び権限を管理しているかを確認しています。操作するIDと権限を管理することは、過失によるオペレーションミスや内部不正の抑止につながります。また、サイバー攻撃によりアカウントの不正使用が行われた場合も影響を最小限に抑えられます。	3	3	システムの設定を変更可能な特権IDについては、オペレーションミスや内部不正の影響が大きいことから、より厳格な取り扱いが求められます。
ログ管理	工場/生産ラインにおいてログを取得し管理していますか。	工場/生産ライン取得しているログの内容と管理内容を確認しています。 インシデントが発生した際の原因究明を行うためにはログの取得が重要です。また、インシデントの早期検知、影響範囲の極小化を実現するためには定期的にログの分析を行うことが有効な対策となります。	3	2.33	インシデントの早期検知、影響範囲の極小化を実現するためには定期的なログの分析を行うことが有効です。
保守管理	工場/生産ラインの保守管理を実施していますか。	工場/生産ラインの保守要員、作業内容、保守方法（オンサイト保守、リモート保守）及び保守環境（保守用端末、回線のセキュリティ対策内容）を管理しているかを確認しています。 保守員の不正や作業ミスによる影響や、リモート環境の脆弱性による外部からの攻撃を防ぐためには保守管理を実施することが重要です。	2	2.67	保守作業の実施状況を管理することにより、保守要員の作業ミスや不正を含むインシデント発生の早期把握、影響の採用化を図ることが重要です。
サイバー攻撃への対策	工場/生産ラインへの外部からの不正侵入、サービス停止攻撃またはマルウェア感染といったサイバー攻撃への対策を実施していますか。	ITNWとの接続を行っている際に、外部からのサイバー攻撃への対策を実施しているかを確認しています。 インターネットからのサイバー攻撃の脅威に対して通信制御や不正通信の検知を行うことが重要です。ITNWに接続していない場合でも、NW内に不正な通信が発生していないかを分析することは有効な対策となります。	1	1.33	サイバー攻撃への対応を行うためには、インターネット接続口の通信制御が重要です。