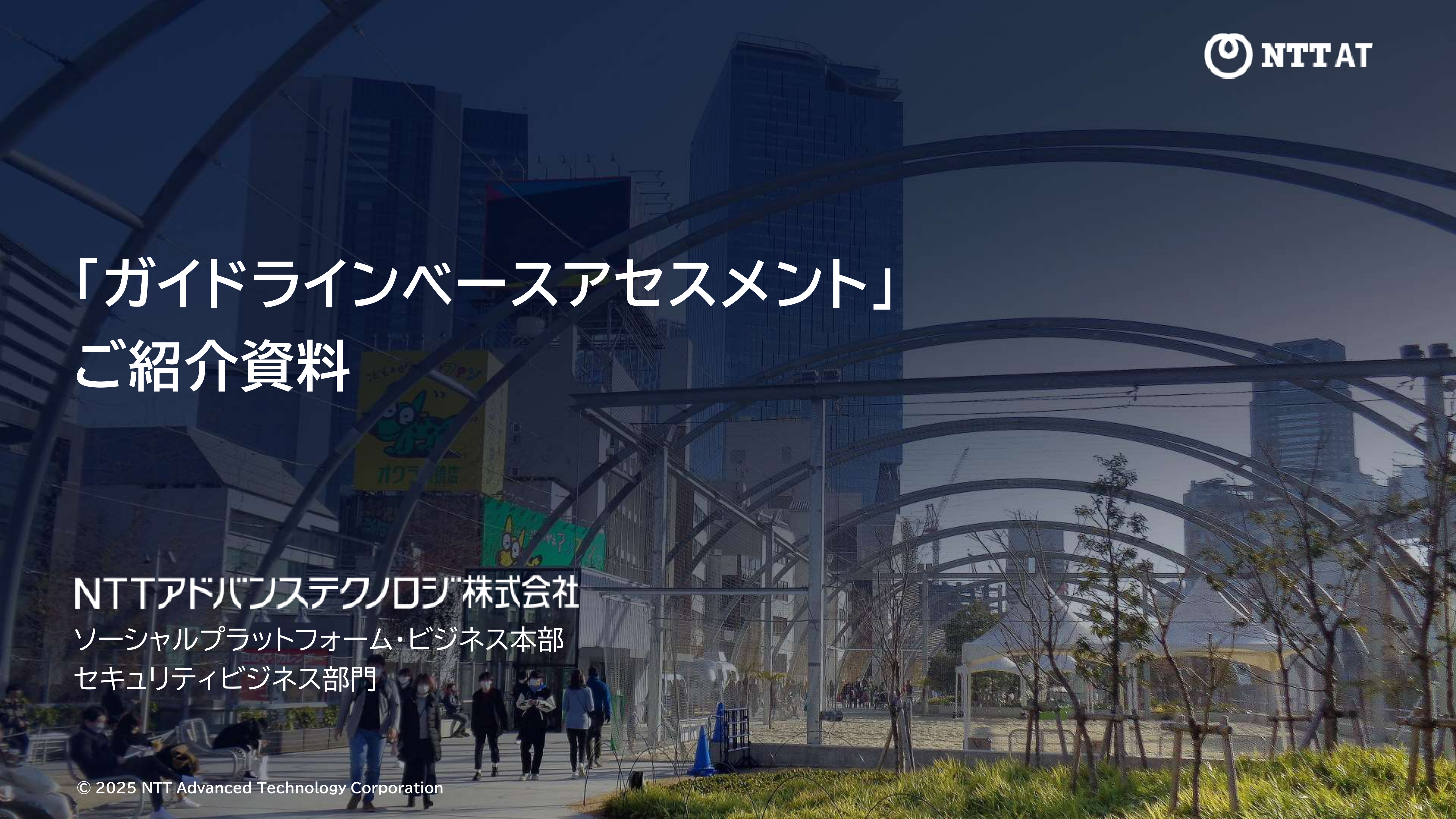


「ガイドラインベースアセスメント」ご紹介資料

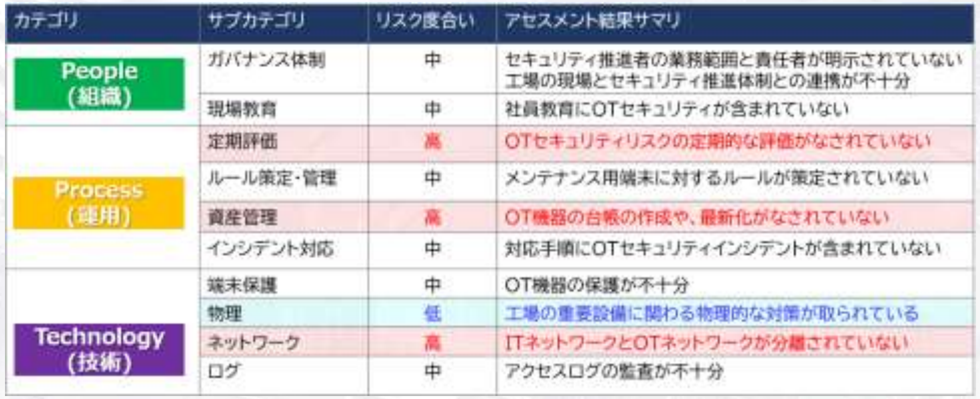
NTTアドバンステクノロジ株式会社
ソーシャルプラットフォーム・ビジネス本部
セキュリティビジネス部門

目次

ガイドラインベースアセスメント概要

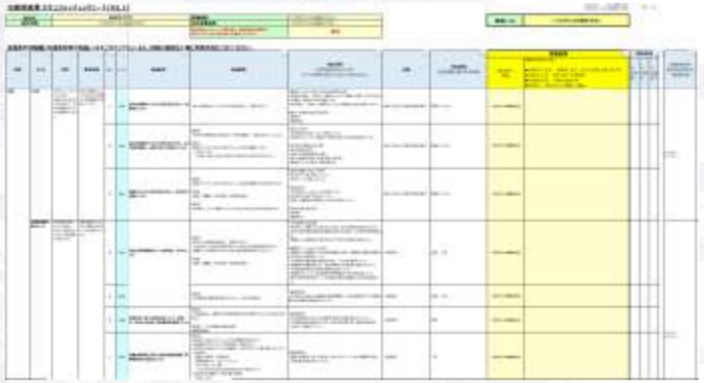
■ ガイドラインベースチェックリストを利用して組織、運用、技術の観点で俯瞰したセキュリティアセスメントを進めるとともに、ガイドラインを満たすセキュリティ対策案を提示します。

1. 経産省 チェックリストに従ったアセスメント結果



カテゴリ	サブカテゴリ	リスク度合い	アセスメント結果サマリ
People (組織)	ガバナンス体制	中	セキュリティ推進者の業務範囲と責任者が明示されていない 工場の現場とセキュリティ推進体制との連携が不十分
	現場教育	中	社員教育にOTセキュリティが含まれていない
Process (運用)	定期評価	高	OTセキュリティリスクの定期的な評価がなされていない
	ルール策定・管理	中	メンテナンス用端末に対するルールが策定されていない
	資産管理	高	OT機器の台帳の作成や、最新化がなされていない
	インシデント対応	中	対応手順にOTセキュリティインシデントが含まれていない
Technology (技術)	端末保護	中	OT機器の保護が不十分
	物理	低	工場の重要設備に関わる物理的な対策が取られている
	ネットワーク	高	ITネットワークとOTネットワークが分離されていない
	ログ	中	アクセスログの監査が不十分

2. 自工会 チェックシート（評価結果）



セキュリティ対策案の検討

具体的なソリューション検討
概算見積算出

経済産業省　チェックリスト

経済産業省では、「サイバー・フィジカル・セキュリティ対策フレームワーク(CPSF)」の策定を進めており、産業分野別に具体的適用のためのセキュリティポリシーを検討

ビル分野向けのものが「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」

- 2019/6/17 第1版 発表
- 2022/10/24 個別編：空調システム 第1版 発表
- 2023/4/20 第2版 発表

工場分野向けのものが「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」

- 2022/11/16 第1版 発表

自工会　チェックシート

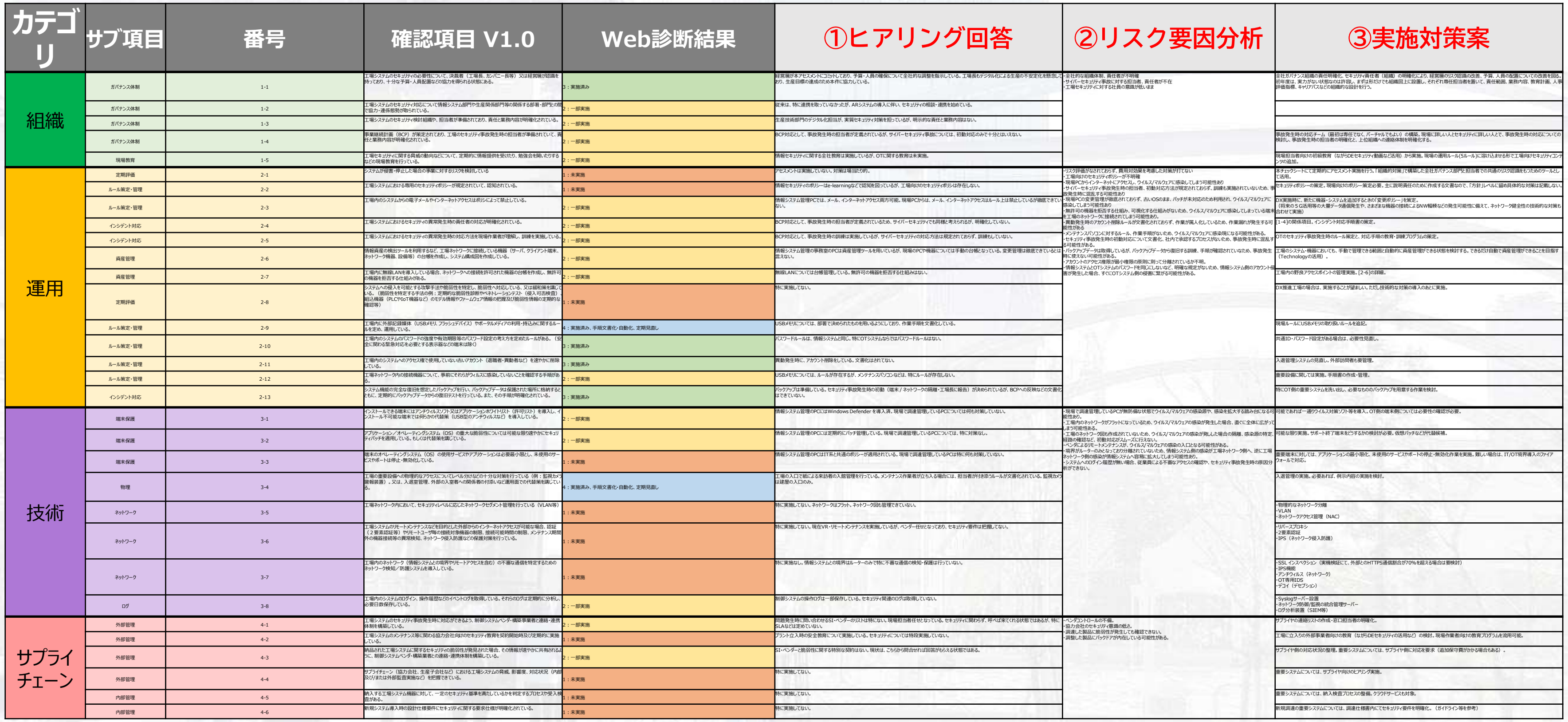
「経済産業省 サイバー・フィジカル・セキュリティ対策フレームワーク」を中核に、「NIST Cybersecurity Framework v1.1」、「ISO 27001」、「AIAG Cyber Security 3rd Party Information Security 1st Edition」、「IPA 中小企業の情報セキュリティ対策ガイドライン」をベンチマークし作成

- 2020/12/1 第1版 発表 「自工会/部工会・サイバーセキュリティガイドライン」
- 2022/4/1　第2版 発表

経産省チェックリストに基づいたアセスメントの特徴

- ✓ ガイドライン診断32項目について実情把握、リスク分析、実施対策案の提示により**対策の意思決定、対策計画の立案を支援**
- ✓ ヒアリング、およびインタビューによる実情把握について、国際標準IEC62443の観点を取り入れ効果的な現状把握を支援
- ✓ 一連の工程は有識者（CISSP/CCSP/情報安全確保支援士/IEC62443基礎資格）監督の元に実施

← OTセキュリティクイック診断ベース →　← セキュリティアセスメント →



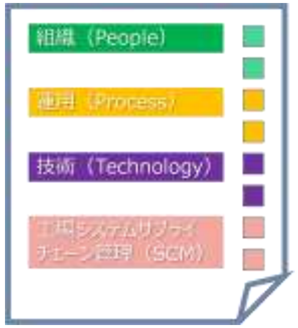
カテゴリ	サブ項目	番号	確認項目 V1.0	Web診断結果	①ヒアリング回答	②リスク要因分析	③実施対策案
組織	ガバナンス体制	1-1	工場システムのセキュリティの必要性について、決裁者（工場長、カンパニー長等）又は経営層が認識を持っており、十分な予算・人員配置などの協力を得られる状態にある。	3：実施済み	経営層が本アセスメントにコミットしており、予算・人員の確保について全社的な調整を指示している。工場長もデジタル化による生産の不安定化を懸念しており、生産目標の達成のため本件に協力している。	・全社的な組織体制、責任者が不明確 ・サイバーセキュリティ事故に対する担当者、責任者が不在 ・工場セキュリティに対する社員の意識が低いまま	全社ガバナンス組織の責任明確化、セキュリティ責任者（組織）の明確化により、経営層のリスク認識の改善、予算、人員の配置についての改善を図る。初年度は、実力がない状態なのは許容し、まずは形だけでも組織図上に設置し、それぞれ専任担当者を置いて、責任範囲、業務内容、教育計画、人事評価指標、キャリアパスなどの組織的な設計を行う。
	ガバナンス体制	1-2	工場システムのセキュリティ対応について情報システム部門や生産関係部門等の関係する部署・部門との間で協力・連係態勢が取られている。	2：一部実施	従来は、特に連携を取っていなかったが、ARシステムの導入に伴い、セキュリティの相談・連携を始めている。		
	ガバナンス体制	1-3	工場システムのセキュリティ検討組織や、担当者が準備されており、責任と業務内容が明確化されている。	2：一部実施	生産技術部門のデジタル化担当が、実質セキュリティ対策を担っているが、明示的な責任と業務内容はない。		
	ガバナンス体制	1-4	事業継続計画（BCP）が策定されており、工場のセキュリティ事故発生時の担当者が準備されていて、責任と業務内容が明確化されている。	2：一部実施	BCP対応として、事故発生時の担当者が定義されているが、サイバーセキュリティ事故については、初動対応のみで十分とはいえない。		事故発生時の対応チーム（最初は専任でなく、バーチャルでもよい）の構築。現場に詳しい人とセキュリティに詳しい人とで、事故発生時の対応についての検討し、事故発生時の担当者の明確化と、上位組織への連絡体制を明確化する。
	現場教育	1-5	工場セキュリティに関する脅威の動向などについて、定期的に情報提供を受けたり、勉強会を開いたりするなどの現場教育を行っている。	2：一部実施	情報セキュリティに関する全社教育は実施しているが、OTに関する教育は未実施。		現場担当者向けの初級教育（ながらDEセキュリティ動画など活用）から実施。現場の運用ルール(5ルール)に溶け込ませる形で工場向けセキュリティコンテンツの追加。
運用	定期評価	2-1	システムが侵害・停止した場合の事業に対するリスクを検討している	1：未実施	アセスメントは実施していない。対策は場当たり的。	・リスク評価がなされておらず、費用対効果を考慮した対策が打てない ・工場向けのセキュリティポリシーが不明確 ・現場PCからインターネットにアクセスし、ウイルス/マルウェアに感染してしまう可能性あり ・サイバーセキュリティ事故発生時の担当者、初動対応方法が規定されておらず、訓練も実施されていないため、事故発生時に混乱する可能性あり ・現場PCの変更管理が徹底されておらず、古いOSのまま、パッチが未対応のため利用され、ウイルス/マルウェアに感染してしまう可能性あり ・無許可の機器を拒否する仕組み、可視化する仕組みがないため、ウイルス/マルウェアに感染してしまっている端末を工場のネットワークに接続されてしまう可能性あり。 ・異動発生時のアカウント削除ルールが文書化されておらず、作業が属人化しているため、作業漏れが発生する可能性がある ・メンテナンスパソコンに対するルール、作業手順がないため、ウイルス/マルウェアに感染現になる可能性がある。 ・セキュリティ事故発生時の初動対応について文書化、社内で承認するプロセスがないため、事故発生時に混乱する可能性がある。 ・バックアップデータは取得しているが、バックアップデータから復旧する訓練、手順が確認されていなため、事故発生時に使えない可能性がある。 ・アカウントのアクセス権限が最小権限の原則に則って分離されているか不明。 ・情報システムとOTシステムのパスワードを同じにしないなど、明確な規定がないため、情報システム側のアカウント侵害が発生した場合、すぐにOTシステム側の侵害に繋がる可能性がある。	本チェックシートにて定期的にアセスメント実施を行う。「組織的対策」で構築した全社ガバナンス部門と担当者での共通のリスク認識をもつためのツールとして活用。
	ルール策定・管理	2-2	工場システムにおける専用のセキュリティポリシーが規定されていて、認知されている。	1：未実施	情報セキュリティのポリシーはe-learningなどで認知を図っているが、工場向けのセキュリティポリシは存在しない。		セキュリティポリシーの策定。現場向けのポリシー策定必要。主に説明責任のために作成する文書なので、「方針」レベルに留め具体的な対策は記載しない。
	ルール策定・管理	2-3	工場内のシステムからの電子メールやインターネットアクセスはポリシによって禁止している。	2：一部実施	情報システム管理PCでは、メール、インターネットアクセス両方可能。現場PCからは、メール、インターネットアクセスはルール上は禁止しているが徹底できていない。		DX実施時に、新たに機器・システムを追加するときの「変更ポリシー」を策定。 （将来の５G活用等の大量データ通信発生や、さまざまな機器の接続によるNW輻輳などの発生可能性に備えて、ネットワーク健全性の技術的な対策も合わせて実施）
	インシデント対応	2-4	工場システムにおけるセキュリティの異常発生時の責任者の対応が明確化されている。	2：一部実施	BCP対応として、事故発生時の担当者が定義されているため、サイバーセキュリティでも同様と考えられるが、明確化していない。		[1-4]の関係項目。インシデント対応手順書の策定。
	インシデント対応	2-5	工場システムにおけるセキュリティの異常発生時の対応方法を現場作業者が理解し、訓練を実施している。	2：一部実施	BCP対応として、事故発生時の訓練は実施しているが、サイバーセキュリティの対応方法は規定されておらず、訓練もしていない。		OTのセキュリティ事故発生時のルール策定と、対応手順の教育・訓練プログラムの策定。
	資産管理	2-6	情報資産の検出ツールを利用するなど、工場ネットワークに接続している機器（サーバ、クライアント端末、ネットワーク機器、設備等）の台帳を作成し、システム構成図を作成している。	2：一部実施	情報システム管理の事務室のPCは資産管理ツールを用いているが、現場のPCや機器については手動の台帳となっている。変更管理は徹底できているとは言えない。		工場のシステム・機器においても、手動で管理できる範囲と自動的に資産管理ができる状態を検討する。できるだけ自動で資産管理ができることを目指す（Technologyの活用）。
	資産管理	2-7	工場内に無線LANを導入している場合、ネットワークへの接続を許可された機器の台帳を作成し、無許可の機器を拒否する仕組みがある。	2：一部実施	無線LANについては台帳管理している。無許可の機器を拒否する仕組みはない。		工場内の野良アクセスポイントの管理実施。[2-6]の詳細。
	定期評価	2-8	システムへの侵入を可能とする攻撃手法や脆弱性を特定し、脆弱性へ対応している、又は緩和策を講じている。（脆弱性を特定する手法の例：定期的な脆弱性診断やペネトレーションテスト（侵入可否検査）、組込機器（PLCやIoT機器など）のモデル情報やファームウェア情報の把握及び脆弱性情報の定期的な確認等）	1：未実施	特に実施してない。		DX推進工場の場合は、実施することが望ましい。ただし技術的な対策の導入のあとに実施。
	ルール策定・管理	2-9	工場内に外部記録媒体（USBメモリ、フラッシュデバイス）やポータルメディアの利用・持込みに関するルールを定め、運用している。	4：実施済み、手順文書化・自動化、定期見直し	USBメモリについては、部署で決められたものを用いるようにしており、作業手順を文書化している。		現場ルールにUSBメモリの取り扱いルールを追記。
	ルール策定・管理	2-10	工場内のシステムのパスワードの強度や有効期限等のパスワード設定の考え方を定めたルールがある。（安全に関わる緊急対応を必要とする表示器などの端末は除く）	3：実施済み	パスワードルールは、情報システムと同じ。特にOTシステムならではパスワードルールはない。		共通ID・パスワード設定がある場合は、必要性見直し。
	ルール策定・管理	2-11	工場内のシステムへのアクセス権で使用していない古いアカウント（退職者・異動者など）を速やかに削除している。	3：実施済み	異動発生時に、アカウント削除をしている。文書化はされてない。		入退管理システムの見直し。外部訪問者も要管理。
	ルール策定・管理	2-12	工場ネットワーク内の接続機器について、事前にそれらがウィルスに感染していないことを確認する手順がある。	2：一部実施	USBメモリについては、ルールが存在するが、メンテナンスパソコンなどは、特にルールが存在しない。		重要設備に関しては実施。手順書の作成・管理。
	インシデント対応	2-13	システム機能の完全な復旧を想定したバックアップを行い、バックアップデータは保護された場所に格納するとともに、定期的にバックアップデータからの復旧テストを行っている。また、その手順が明確化されている。	3：実施済み	バックアップは準備している。セキュリティ事故発生時の初動（端末 / ネットワークの隔離・工場長に報告）が決められているが、BCPへの反映などの文書化はできていない。		特にOT側の重要システムを洗い出し、必要なもののバックアップを用意する作業を検討。
技術	端末保護	3-1	インストールできる端末にはアンチウィルスソフト又はアプリケーションホワイトリスト（許可リスト）を導入し、インストール不可能な端末では何らかの代替策（USB型のアンチウィルスなど）を導入している。	2：一部実施	情報システム管理のPCにはWindows Defender を導入済。現場で調達管理しているPCについては何も対策していない。	・現場で調達管理しているPCが無防備な状態でウイルス/マルウェアの感染源や、感染を拡大する踏み台になる可能性あり。 ・工場内のネットワークがフラットになっているため、ウイルス/マルウェアの感染が発生した場合、直ぐに全体に広がってしまう可能性ある。 ・工場のネットワーク図も作成されていないため、ウイルス/マルウェアの感染が発しした場合の隔離、感染源の特定、経路の確認など、初動対応がスムーズに行えない。 ・ベンダによるリモートメンテナンスが、ウイルス/マルウェアの感染の入口となる可能性がある。 ・境界がルーターのみとなっており分離されていないため、情報システム側の感染が工場ネットワーク側へ、逆に工場ネットワーク側の感染が情報システムへ容易に拡大してしまう可能性あり。 ・システムへのログイン履歴が無い場合、従業員による不審なアクセスの確認や、セキュリティ事故発生時の原因分析ができない。	可能であれば一通りウイルス対策ソフト等を導入。OT側の端末側については必要性の確認が必要。
	端末保護	3-2	アプリケーション／オペレーティングシステム（OS）の重大な脆弱性については可能な限り速やかにセキュリティパッチを適用している。もしくは代替策を講じている。	2：一部実施	情報システム管理のPCには定期的にパッチ管理している。現場で調達管理しているPCについては、特に対策なし。		可能な限り実施。サポート終了端末をどうするかの検討が必要。仮想パッチなどが代替候補。
	端末保護	3-3	端末のオペレーティングシステム（OS）の使用サービスやアプリケーションは必要最小限とし、未使用のサービスやポートは停止・無効化している。	1：未実施	情報システム管理のPCはIT系と共通のポリシーが適用されている。現場で調達管理しているPCは特に何も対策していない。		重要端末に対しては、アプリケーションの最小限化、未使用のサービスやポートの停止・無効化作業を実施。難しい場合は、IT/OT境界導入のファイアウォールで対応。
	物理	3-4	工場の重要設備への物理的なアクセスについてレベル分けなどの十分な対策を行っている（例：監視カメラ、警報装置）。又は、入退室管理、外部の入室者への関係者の付添いなど運用面での代替策を講じている。	4：実施済み、手順文書化・自動化、定期見直し	工場の入口で紙による来訪者の入館管理を行っている。メンテナンス作業者が立ち入る場合には、担当者が付き添うルールが文書化されている。監視カメラは建屋の入口のみ。		入退管理の実施。必要あれば、例示内容の実施を検討。
	ネットワーク	3-5	工場ネットワーク内において、セキュリティレベルに応じたネットワークセグメント管理を行っている（VLAN等）	1：未実施	特に実施してない。ネットワークはフラット。ネットワーク図も管理できていない。		・物理的なネットワーク分離 ・VLAN ・ネットワークアクセス管理（NAC）
	ネットワーク	3-6	工場システムのリモートメンテナンスなどを目的とした外部からのインターネットアクセスが可能な場合、認証（２要素認証等）やリモートユーザ毎の接続対象機器の制限、接続可能時間の制限、メンテナンス期間外の機器接続等の異常検知、ネットワーク侵入防護などの保護対策を行っている。	1：未実施	特に実施してない。現在VR・リモートメンテナンスを実施しているが、ベンダー任せとなっており、セキュリティ要件は把握してない。		・リバースプロキシ ・2要素認証 ・IPS（ネットワーク侵入防護）
	ネットワーク	3-7	工場内のネットワーク（情報システムとの境界やリモートアクセスを含む）の不審な通信を特定するためのネットワーク検知／防護システムを導入している。	1：未実施	特に実施なし。情報システムとの境界はルーターのみで特に不審な通信の検知・保護は行っていない。		・SSL インスペクション（実機検証にて、外部とのHTTPS通信割合が70%を超える場合は要検討） ・IPS機能 ・アンチウィルス（ネットワーク） ・OT専用IDS ・デコイ（デセプション）
	ログ	3-8	工場内のシステムのログイン、操作履歴などのイベントログを取得している。それらのログは定期的に分析し、必要日数保存している。	2：一部実施	制御システムの操作ログは一部保存している。セキュリティ関連のログは取得していない。		・Syslogサーバー設置 ・ネットワーク防御/監視の統合管理サーバー ・ログ分析装置（SIEM等）
サプライチェーン	外部管理	4-1	工場システムのセキュリティ事故発生時に対応ができるよう、制御システムベンダ・構築事業者と連絡・連携体制を構築している。	2：一部実施	問題発生時に問い合わせるSI・ベンダーのリストは特にない。現場担当者任せとなっている。セキュリティに関わらず、呼べば来てくれる状態ではあるが、特にSLAなどは定めていない。	・ベンダコントロールの不備。 ・協力会社のセキュリティ意識の低さ。 ・調達した製品に脆弱性が発生しても確認できない。 ・調整した製品にバックドアが内在している可能性がある。	サプライヤの連絡リストの作成・窓口担当者の明確化。
	外部管理	4-2	工場システムのメンテナンス等に関わる協力会社向けのセキュリティ教育を契約開始時及び定期的に実施している。	1：未実施	プラント立入時の安全教育について実施している。セキュリティについては特段実施していない。		工場に立入りの外部事業者向けの教育（ながらDEセキュリティの活用など）の検討。現場作業者向けの教育プログラムを流用可能。
	外部管理	4-3	納品された工場システムに関するセキュリティの脆弱性が発見された場合、その情報が速やかに共有されるように、制御システムベンダ・構築業者との連絡・連携体制を構築している。	2：一部実施	SI・ベンダーと脆弱性に関する特別な契約はない。現状は、こちらから問合せれば回答がもらえる状態ではある。		サプライヤ側の対応状況の整理。重要システムについては、サプライヤ側に対応を要求（追加保守費がかかる場合もある）。
	外部管理	4-4	サプライチェーン（協力会社、生産子会社など）における工場システムの脅威、影響度、対応状況（内部及び/または外部監査実施など）を把握できている。	1：未実施	特に実施してない。		重要システムについては、サプライヤ向けのヒアリング実施。
	内部管理	4-5	納入する工場システム機器に対して、一定のセキュリティ基準を満たしているかを判定するプロセスや受入検査がある。	1：未実施	特に実施してない。		重要システムについては、納入検査プロセスの整備。クラウドサービスも対象。
	内部管理	4-6	新規システム導入時の設計仕様要件にセキュリティに関する要求仕様が明確化されている。	1：未実施	特に実施してない。		新規調達の重要システムについては、調達仕様書内にてセキュリティ要件を明確化。（ガイドライン等を参考）

経産省チェックリストに基づいたアセスメントの流れ

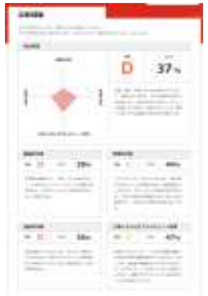
- 事前にお客様にてWeb上でOTセキュリティクイック診断を実施いただき、現状把握(ヒアリング、資料確認)を通じて、リスク要因の分析とセキュリティ対策案の検討を行います。

OTセキュリティクイック診断

4つの要素でWeb診断



結果はA-Dでスコアリング



A
B
C
D

現状把握（組織、運用、技術、サプライチェーン）

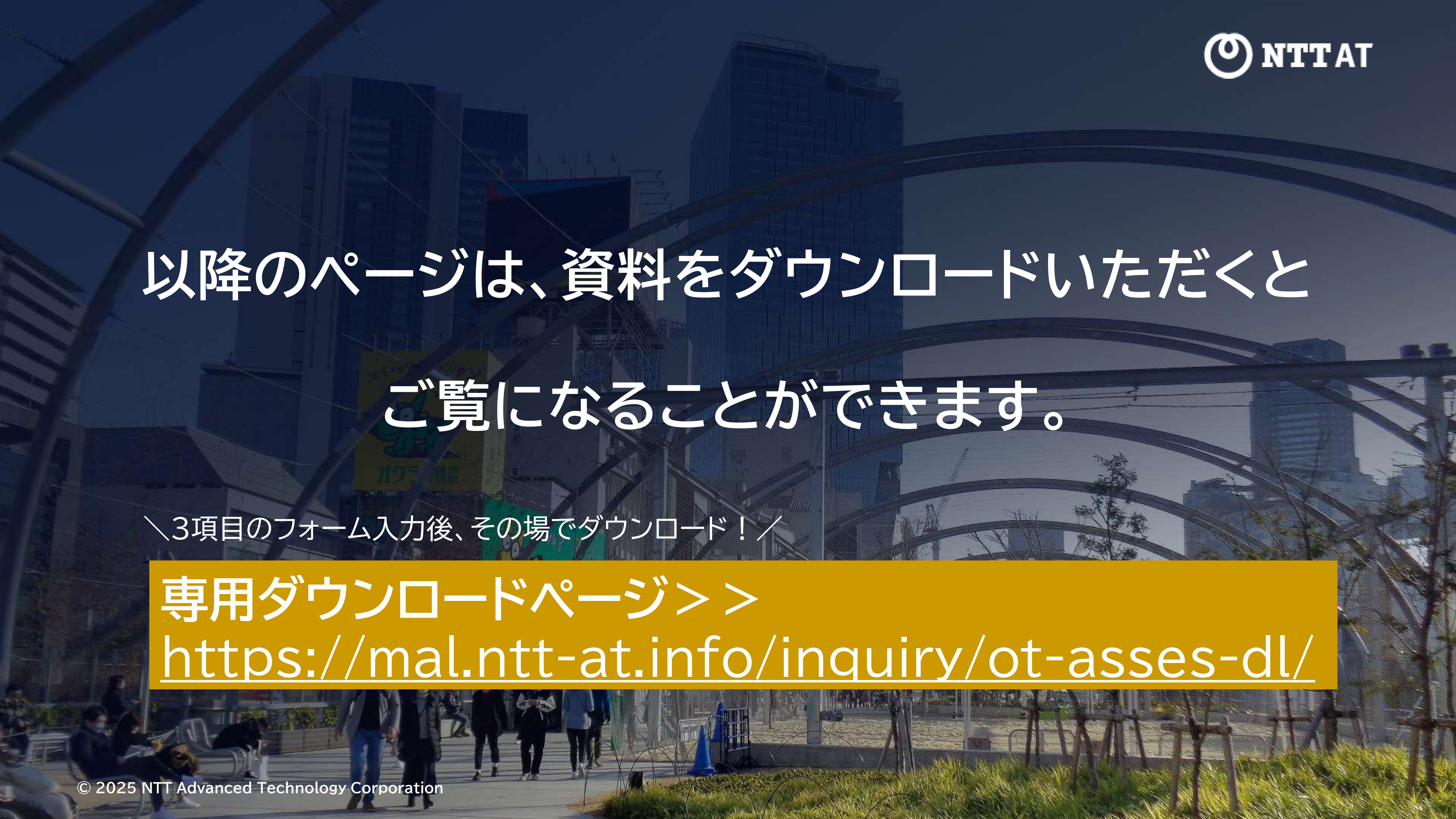
ヒアリング＋α(既存のNW図、ポリシーなどのドキュメント)を基にアセスメント実施

- キックオフ（アセスメントの目的説明）
- ガイドライン/IEC62443に則したヒアリング
- 現状把握
- リスクの洗い出しと分析
- 優先順位付け、実現対策案の検討

★ 成果物

アセスメント報告書

- ヒアリング結果
- リスク要因分析結果
- リスクを低減するための対策案の提示



以降のページは、資料をダウンロードいただくとご覧になることができます。

＼3項目のフォーム入力後、その場でダウンロード！／

専用ダウンロードページ＞＞
https://mal.ntt-at.info/inquiry/ot-asses-dl/