資料5

経済産業省「工場セキュリティガイドライン」を活用したサプライチェーンセキュリティ向上の取組

フォーティネットジャパン合同会社

OTビジネス開発部　部長　佐々木　弘志

工場(OT)のサイバーセキュリティのビジネス課題

ビジネス環境の変化で必要性が高まっているのに対応できていない

セキュリティリスク増大

- DX進展による セキュリティ脅威 の接点増加
- 攻撃者の能力・ 手法の進化・ 被害発生

規制・ガイドライン強化

- グローバルで サプライチェーン 規制化の動き
- 業界別の規制・ ガイドライン強化

→

- そもそもの必要性の理解 （経営層・IT/OT部門）
- どうしていいかわからない （スタンダードがない）
- どこまでやっていいかわからない （費用感・正解は？）
- やる人がいない （コンサル・SI・ベンダーにも少ない）
- 海外拠点・事業部によって対策が違う （ITほど統一的にできない）

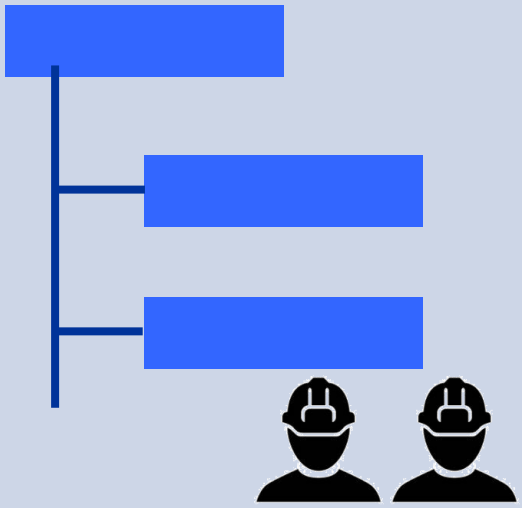
↓

「要検討」で放置

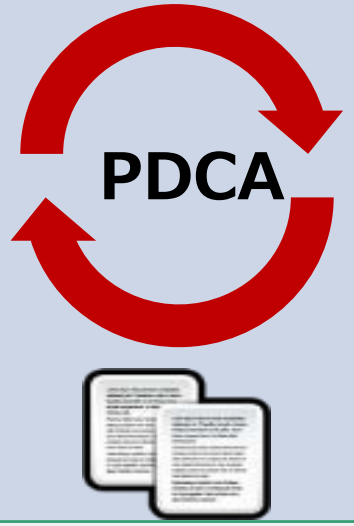
OTセキュリティの３要素

People（組織・人），Process（運用），Technology（技術）

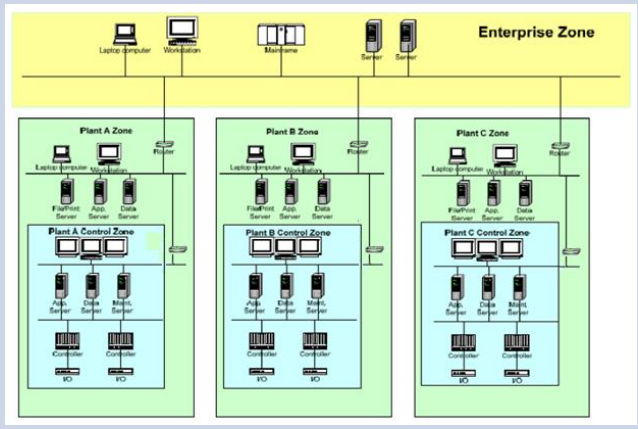
People



Process

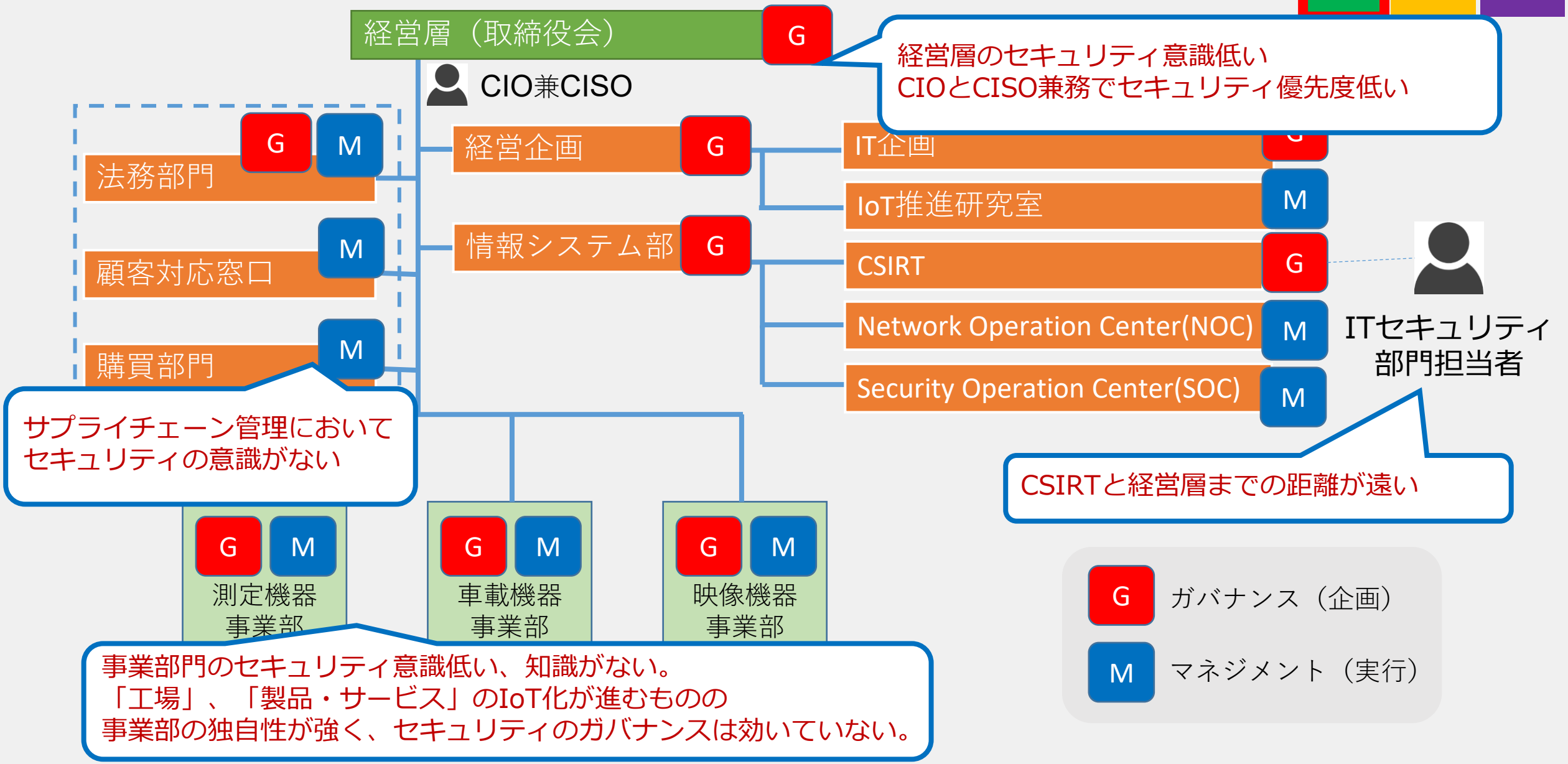


Technology

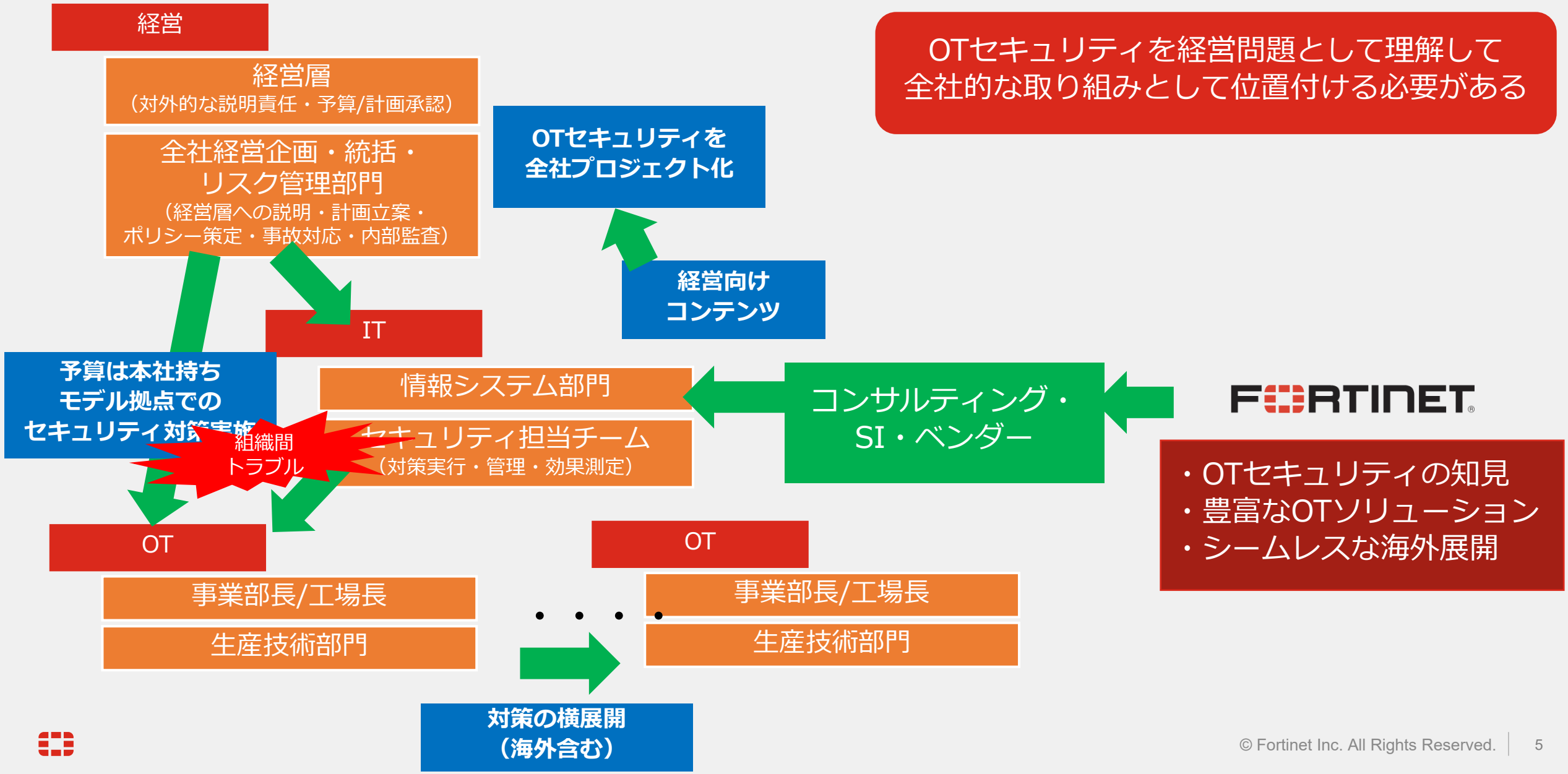


組織課題：誰も工場セキュリティ管理してない

Pe Pr Te



OTセキュリティを前に進めるために



OTセキュリティを経営問題として理解して
全社的な取り組みとして位置付ける必要がある

- OTセキュリティの知見
- 豊富なOTソリューション
- シームレスな海外展開

工場セキュリティガイドラインを OTビジネス開発に活用

経済産業省のガイドライン付録Eのチェックリスト

達成度を「１：未実施」「2：一部実施」、「3：実施済み」、「4：実施済みで、管理手順を文書化・自動化し、定期的に対策を見直し」、「5：実施済みで、管理手順を文書化・自動化し、随時見直し」に応じて評価する

カテゴリ	No.	確認項目	達成度
組織的対策	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。	
	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。	
	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。	
	1-4	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。	
	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	
運用的対策（システム関連等）	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	
	2-2	工場システムにおける専用のセキュリティポリシが規定されていて、認知されている	
	2-3	工場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。	
	2-4	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。	
	2-5	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。	
	2-6	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、システム構成図が作成している。	
	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。	
	2-8	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）を実施して、システムへの侵入を成功させるために使用できる攻撃手法や脆弱性を特定している。	
	2-9	工場内に外部記録媒体（USB メモリ、フラッシュカード）やポータルメディアの利用・持込みを制限している。	

経済産業省 公開資料より引用 https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000235644

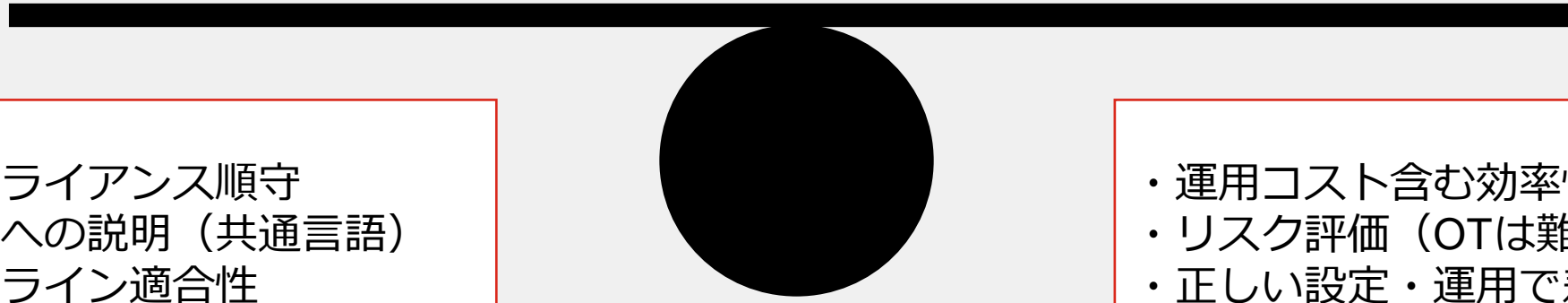
カテゴリ	No.	確認項目	達成度
運用的対策（システム関連等）	2-10	工場内のシステムのパスワードの強度と有効期限を含むパスワードルールがある。（安全に関わる緊急対応を必要とする表示器などの端末は除く）	
	2-11	工場内のシステムへのアクセス権で使用していない古いアカウント（退職者・異動者など）を削除している	
	2-12	工場ネットワーク内の接続機器について、事前にそれらがウィルスに感染していないことを確認する手順がある。	
	2-13	システム機能の完全な復旧を想定したバックアップを行い、定期的にバックアップデータからの復旧テストを行っている。また、その手順が明確化されている。	
技術的対策	3-1	ウィルス対策が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。	
	3-2	アプリケーション／オペレーティングシステム（OS）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。	
	3-3	制御端末のオペレーティングシステム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。	
	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。	
	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）。	
	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）やネットワーク侵入防護などの保護対策を行っている。	
	3-7	工場内のネットワーク（情報システムとの境界含む）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。	
	3-8	工場内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するか必要日数保存している。	
工場システムサプライチェーン管理	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。	
	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実施している。	
	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。	
	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（監査実施など）を把握できている。	
	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。	
	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。	

経済産業省 公開資料より引用 https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000235644

経済産業省の工場セキュリティガイドラインを活用して「説明責任」と「実効性」の両方を実現

説明責任

実効性



・コンプライアンス順守
・取引先への説明（共通言語）
・ガイドライン適合性
↓

但し、形骸化しやすいことに注意

・運用コスト含む効率性
・リスク評価（OTは難しい）
・正しい設定・運用で差がでる
↓

組織・運用・技術のバランス大事

“経済産業省のガイドラインに適合しています！”

“経済産業省のガイドラインを参考に自社のリスク応じた対策に落とし込んでいます！”

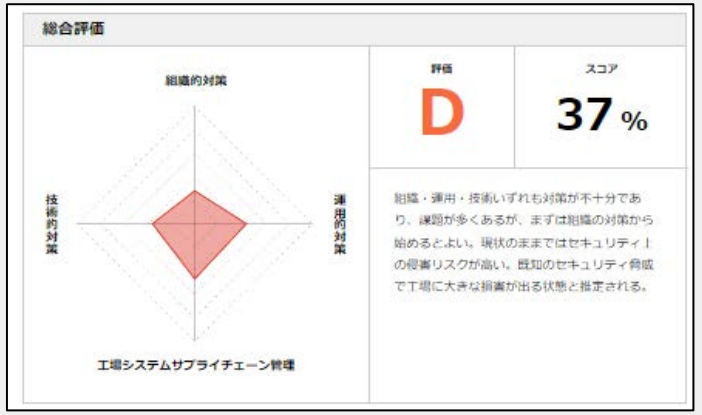
工場セキュリティWeb簡易診断サービス

チェックシート

- 組織（People）
- 運用（Process）
- 技術（Technology）
- 工場システムサプライチェーン管理（SCM）

早ければ15分で回答可能

診断結果 (スグに結果が出ます！)



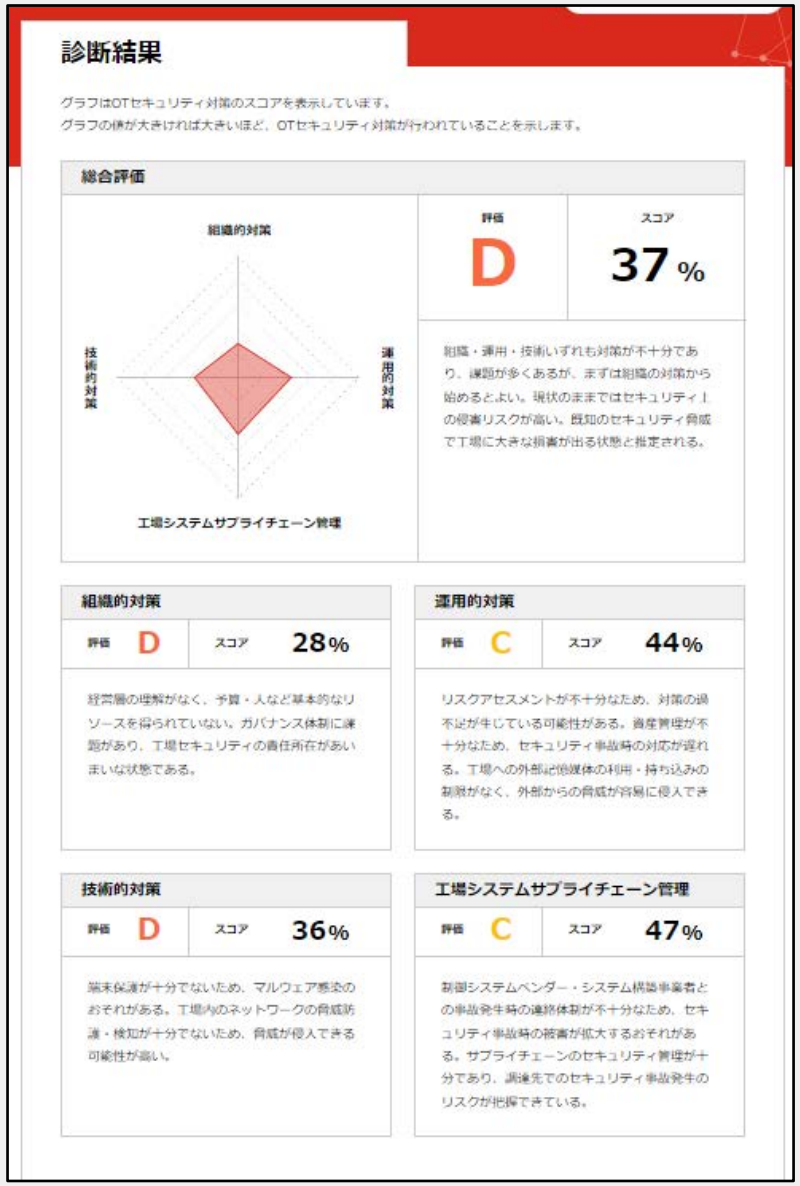
組織的対策			
評価	D	スコア	28%
運用的対策			
評価	C	スコア	44%
技術的対策			
評価	D	スコア	36%
工場システムサプライチェーン管理			
評価	C	スコア	47%

A	管理手順の文書化
B	対策実施済
C	一部の対策実施
D	ほとんど未実施

項目は「経済産業省ガイドラインのチェックリストを活用」

https://www.fortinet.com/jp/promos/ot-security-assessment

工場セキュリティ簡易診断の結果例



診断結果

グラフはOTセキュリティ対策のスコアを表示しています。
グラフの値が大きければ大きいほど、OTセキュリティ対策が行われていることを示します。

総合評価

工場システムサプライチェーン管理

評価 D　スコア 37%

組織・運用・技術いずれも対策が不十分であり、課題が多くあるが、まずは組織の対策から始めるとよい。現状のままではセキュリティ上の侵害リスクが高い。既知のセキュリティ脅威で工場に大きな損害が出る状態と推定される。

組織的対策
評価 D　スコア 28%
経営層の理解がなく、予算・人など基本的なリソースを得られていない。ガバナンス体制に課題があり、工場セキュリティの責任所在があいまいな状態である。

運用的対策
評価 C　スコア 44%
リスクアセスメントが不十分なため、対策の過不足が生じている可能性がある。資産管理が不十分なため、セキュリティ事故時の対応が遅れる。工場への外部記憶媒体の利用・持ち込みの制限がなく、外部からの脅威が容易に侵入できる。

技術的対策
評価 D　スコア 36%
端末保護が十分でないため、マルウェア感染のおそれがある。工場内のネットワークの脅威防護・検知が十分でないため、脅威が侵入できる可能性が高い。

工場システムサプライチェーン管理
評価 C　スコア 47%
制御システムベンダー・システム構築事業者との事故発生時の連絡体制が不十分なため、セキュリティ事故時の被害が拡大するおそれがある。サプライチェーンのセキュリティ管理が十分であり、調達先でのセキュリティ事故発生のリスクが把握できている。

効果：

現状をラフに可視化できて
関係者に共通認識を形成できる
「経営層でもわかる表現」

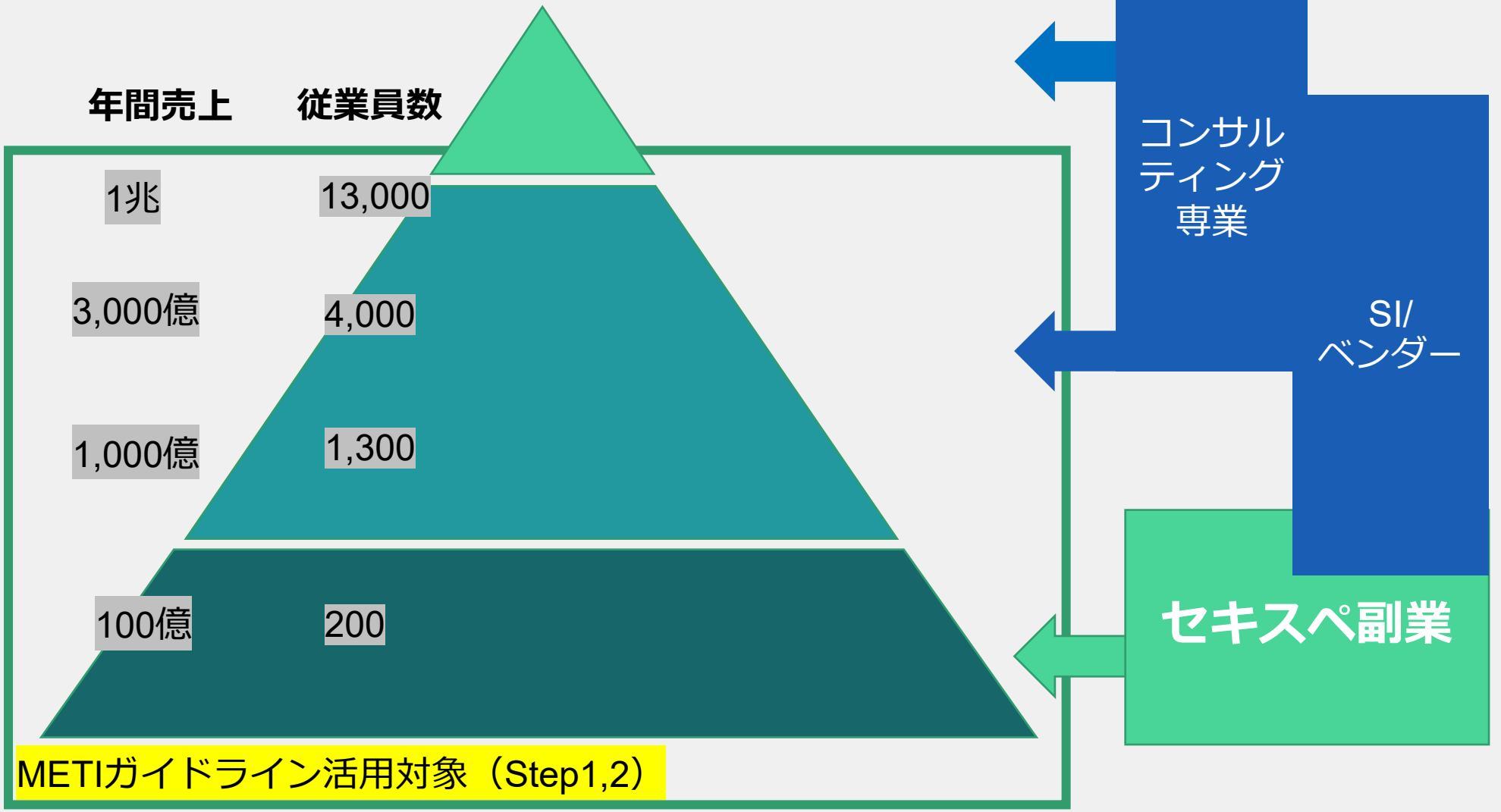
課題：

これからどうするの？
どこまでやればいいの？

人間の健康管理に例えると
「簡易の問診票」に相当する
具体的な対策を考えるなら
更なる診断が必要
（専門医の問診・血液検査、X線等）

アセスメント
を実施

日本OTセキュリティのサプライチェーン全体の底上げ



コンサルティング専業

SI/ベンダー

セキスペ副業

- ガイドライン準拠Web診断
- Web診断後の対策マニュアル
- Web診断後のコンサル教育・ビデオ
- 製品導入支援


FORTINET