工場セキュリティハンドブック
リスク対策集 Ver.1.0

JNSA 日本ネットワークセキュリティ協会
西日本支部
今すぐ実践できる工場セキュリティ対策のポイント検討WG

本リスク対策集の活用にあたって

セキュリティ対策には残念ながら万能薬はありません。効果が期待できる対策を行うには、まず、どこに課題があるのかをしっかりと把握する必要があります。そのためには、是非、工場セキュリティリスクアセスメントハンドブックを参考にしていただき、自社工場のアセスメントを実施することをお勧めします。
https://www.jnsa.org/result/west/2022/index.html

アセスメントの結果、全く懸念がない脅威の入口以外は何らかの対策が必要と考えられますが、どの対策を選択するかは企業を取り巻く環境や経済状況、社会的位置付けなどによって異なります。また、対策はどれか一つを選択すればいいというものでもありません。
本ハンドブックのリスク対策集は、中小企業の工場にとってそれほどハードルが高くない対策を中心に整理をしました。基本的には、リスクアセスメントハンドブックで定義した「13の脅威の入口」に対する対策としてまとめられています。

各対策は、以下のように分類されています。
- 防御：被害に遭わないための対策
- 検知：被害（異常）を早期発見するための対策
- 復旧：被害から早期復旧するための対策

なお、各脅威の入口に対する個別対策だけではなく、すぐに取り組むべき基礎的な共通対策も最初に記載しました。

是非、本ハンドブックを有効に活用していただき、セキュリティ事故リスクの軽減対策を進めて下さい。

※一部のイラストは「いらすとや」さんのフリー素材を利用させていただきました

情報セキュリティ対策の考え方（一般的なフレームワーク）

※本ハンドブックでは、検知と対応を一体として取り扱います。

対策グループの位置づけ（多層防御）

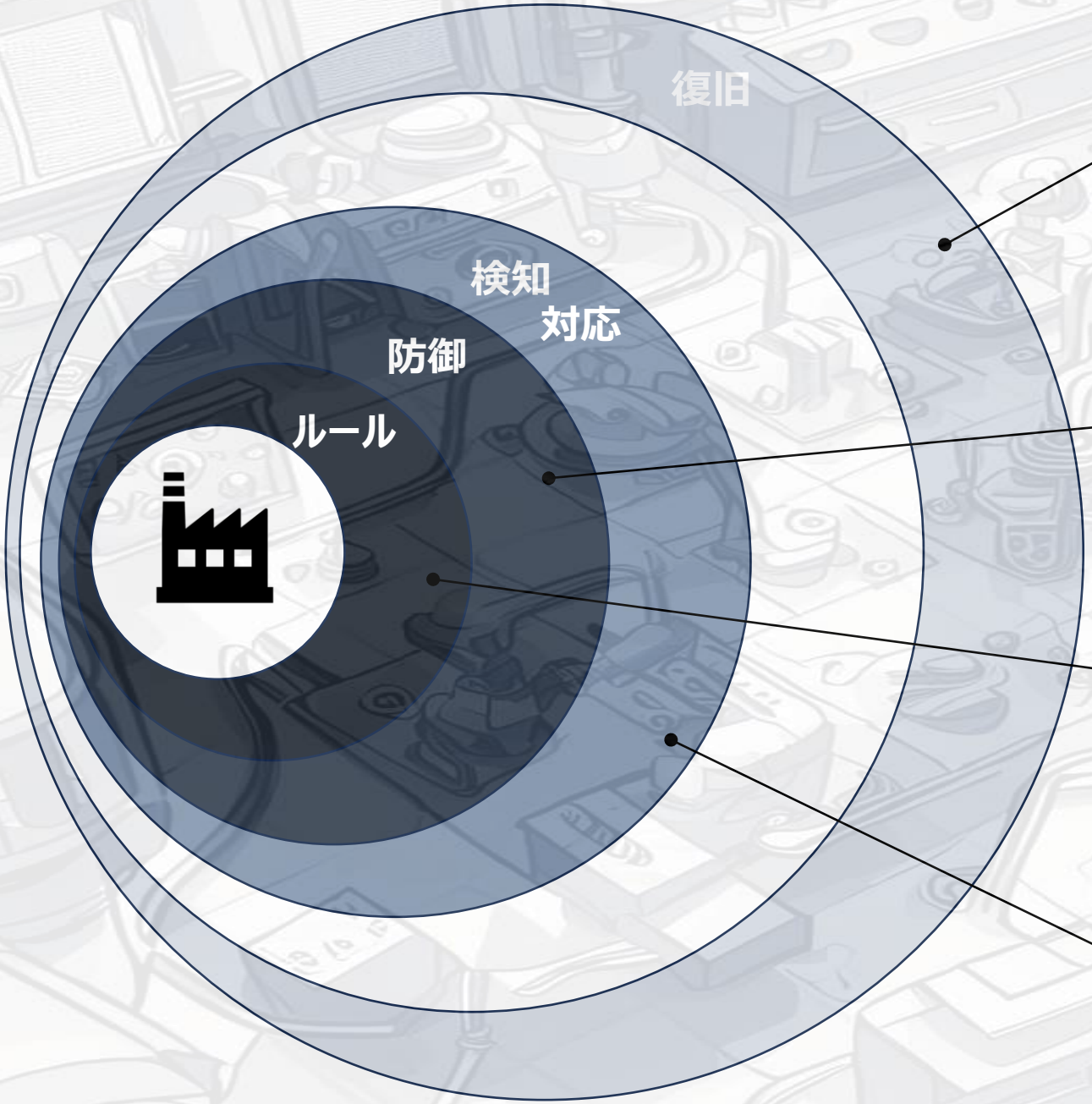
高度な共通対策（E-01~03）

各脅威ごとの対策（01-01~13-02）

- USBメモリー（01-01~03）
- 持込パソコン（02-01~04）
- スマホ・タブレット（03-01~02）
- IoT機器・センサー（04-01~03）
- 複合機（05-01~05）
- ハンディターミナル（06-01~05）
- OAネットワーク（07-01~04）
- インターネット（08-01~04）
- Wi-Fi（無線AP）（09-01~02）
- 保守用ネットワーク（10-01~02）
- クラウドサービス（11-01）
- 部品・原材料（12-01~03）
- 新規購入機器（13-01~02）

基礎的な共通対策（C-01~05）

基礎的な共通対策



C-02🛡,C-03🛡,C-04💰🛡,C-05🛡
事故に備える

C-02🛡,C-03🛡
工場内のすべてのモノを管理する

C-01💰💰🛡
工場出入口及び場内行動を管理する

C-03🛡
予兆と不正を見逃さない

🛡推奨対策 💰投資

対策No.C-01	関連する脅威の入口：共通

具体的な内容：ルールの策定とファシリティ（物理的）対策

●対策内容

工場の出入及び工場内の行動について、部外者を立ち入らせないためのルールを策定する。
工場敷地及び重要な施設の出入口にはゲートを設け、入退出を管理する。

●運用のポイント

名札等の着装を行い、外部からの訪問者と従業員が外見で区別できるように工夫すること。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：☑物理的対策　☑人的対策　□技術的対策

備考：守衛室の設置、重要施設の鍵付き扉など。

対策No.C-02	関連する脅威の入口：共通

具体的な内容：アセット（資産）管理

- **対策内容**

  設備、ネットワーク構成、システムのID/PW、機密情報などを正確に把握するために管理簿を作成する。

- **運用のポイント**

  定期的に棚卸を行い、管理情報が正しいことを確認する。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：アセット管理簿の作成や棚卸は社内要員で実施可能。ネットワークに接続されている機器情報を自動的に収集する製品もある。

対策No.C-03	関連する脅威の入口：共通

具体的な内容：従業員教育

●対策内容

情報セキュリティ教育を定期的に行う。特に工場がマルウェアに感染する原因やどのような被害が発生するかを正しく理解することが重要。

●運用のポイント

教育計画を立案し、できるだけ全員が受講・参加できるように準備をする。
受講状況と理解度を把握し、次回の教育計画に反映させる。

対策の種類：☑被害に遭わないための対策　☑被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：教育はIPAなどが提供する関連資料を利用する方法もある。集合教育やオンライン教育など、さまざまな形態・内容のものがベンダーからも提供されている。

対策No.C-04	関連する脅威の入口：共通

具体的な内容：セキュリティ侵害発生時の訓練

●対策内容

セキュリティ侵害が発生した際の行動および分担を決め周知する。
侵害発生時を想定した机上演習を定期的に行う。

●運用のポイント

経営層も交えて演習を行い、下記の効果が期待できるように実施する。
-演習参加者が高い意識を持って課題の洗い出しを行う。
-経営層がセキュリティ侵害時の課題と残存リスクをしっかりと認識する。

対策の種類：□被害に遭わないための対策　□被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：社内要員で実施することも可能。また、数百円/人で実施できる定型の安価な訓練サービスもある。

対策No.C-05	関連する脅威の入口：共通

具体的な内容：製造装置の動作不良原因調査手順の整備

●対策内容

製造装置に動作不良が発生した際、その原因調査を行う手順に情報セキュリティ攻撃の影響の有無を確認するためのチェック項目を追加する。

-動作不良発生前の通信内容の確認（装置ログなどで通常と異なる相手からの通信がないかなどを確認）

-他の製造装置での動作不良の確認（情報セキュリティ攻撃の場合は複数の装置が影響を受ける場合がある）

●運用のポイント：

情報セキュリティに関わる攻撃と判断する基準を明確にしておく。最終的な判断ができない場合は、外部ベンダーなどに協力が要請できる関係を構築しておくこと。

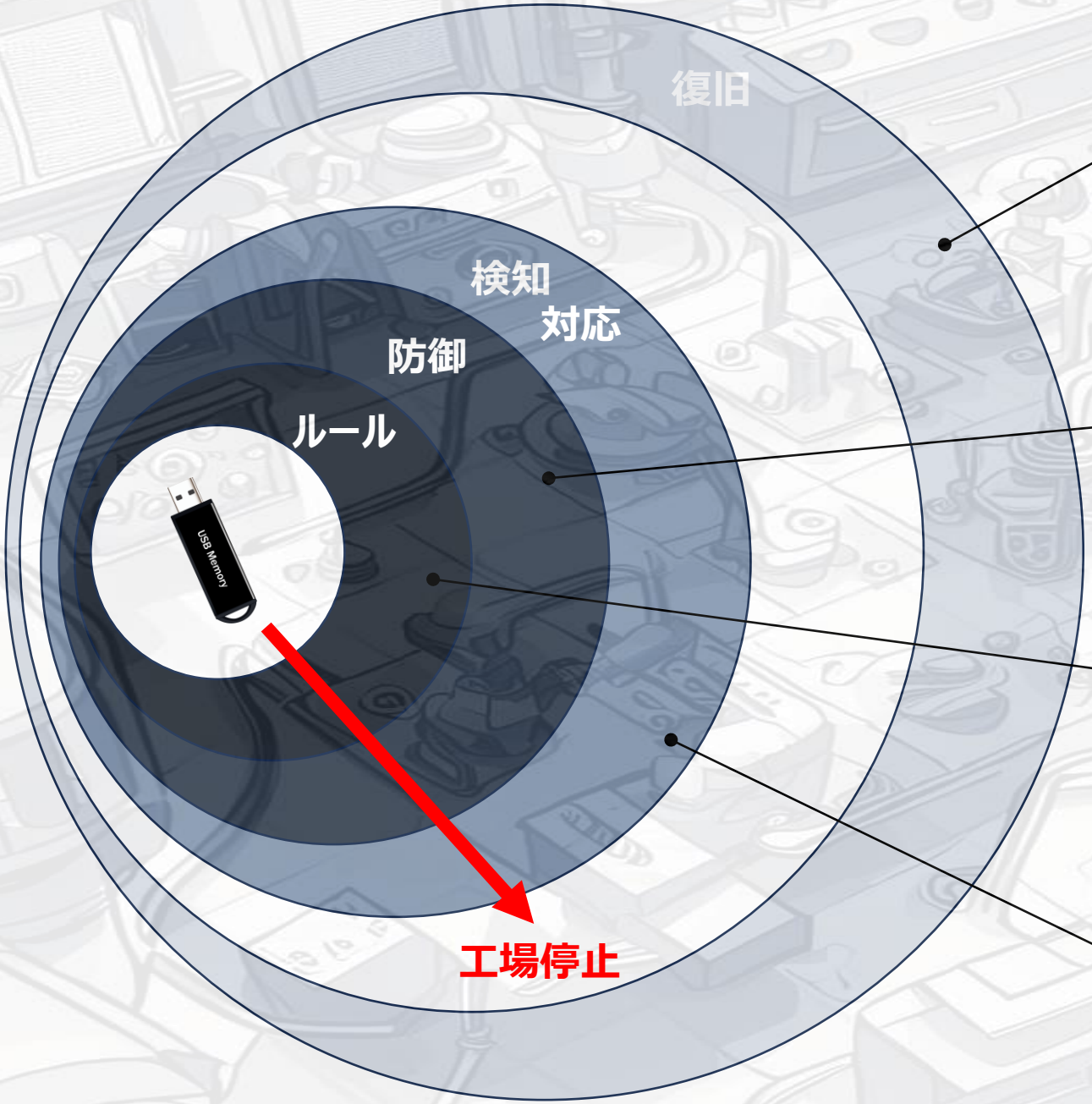
工場全体の操業を停止する判断ができる権限と体制を確立しておくこと。

対策の種類：□被害に遭わないための対策　□被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：製造装置のログを確認する方法は予め機器ベンダーに確認しておく。また、併せて機器のOSの種類なども確認しておくことが望ましい。（マルウェアはWindowsをターゲットにするものが多い）

USBメモリー



01-01🛡,E-02💰,E-03💰
ルールによる使用管理は復旧に役立つ

01-02💰🛡,01-03
USBの脅威は水際で防御可能

01-01🛡
利用のルールとその徹底が最重要

E-01💰💰
USBの使用を検知するのは困難

🛡推奨対策 💰投資

対策No.01-01	関連する脅威の入口：USBメモリー

具体的な内容：USBメモリー使用ルールの策定と管理の徹底

●対策内容

工場内で使用を許可するUSBメモリーとその取り扱い方法をルールとして明文化し周知徹底する。

記載内容の具体例

-使用を許可するUSBメモリーの指定（社給USBメモリーのみなど）

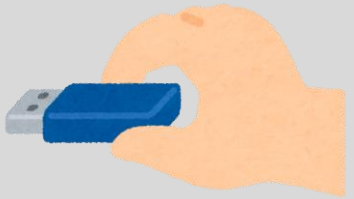
-使用目的、使用対象機器

-管理方法（USB台帳管理）

-管理責任者、識別番号、保管場所、ウイルスチェックデータ更新日※1

-使用記録（USB作業記録）

-作業日、作業者、使用USB識別番号、使用機器、ウイルスチェック※2、不要ファイル削除



●運用のポイント

USBメモリーの識別番号表示（シール等）は目立つものにして管理外のものが混入しないように注意すること。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：※1 対策No.01-02を行う場合　※2 対策No.01-03を行う場合

対策No.01-02	関連する脅威の入口：USBメモリー

具体的な内容：ウイルスチェック機能付きUSBメモリーの導入

●対策内容

ウイルスチェック機能付きのUSBメモリーを用意し、工場内ではこの使用のみを許可する。なお、対策No.01-01と併せて実施するとより効果的である。

●運用のポイント

USBメモリー内に組み込まれたウイルスチェックプログラムやウイルスパターンファイルは適宜アップデートが必要なため、インターネットに接続可能なパソコンにUSBメモリーを定期的に接続し、管理台帳に実施記録を残すこと。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：☑物理的対策　□人的対策　□技術的対策

備考：対応製品は複数のメーカーが販売している。USBメモリーの容量が2GBの場合、6,500円～（2024.1時点）

対策No.01-03	関連する脅威の入口：USBメモリー

具体的な内容：USBメモリーの検疫

●対策内容

工場内でUSBメモリーを使用する場合は、必ず使用前にウイルスチェック機能が導入されたパソコンに接続し、USBメモリーのウイルスチェックを行った後に使用する。対策No.01-01と併せて実施するとより効果的である。

●運用のポイント

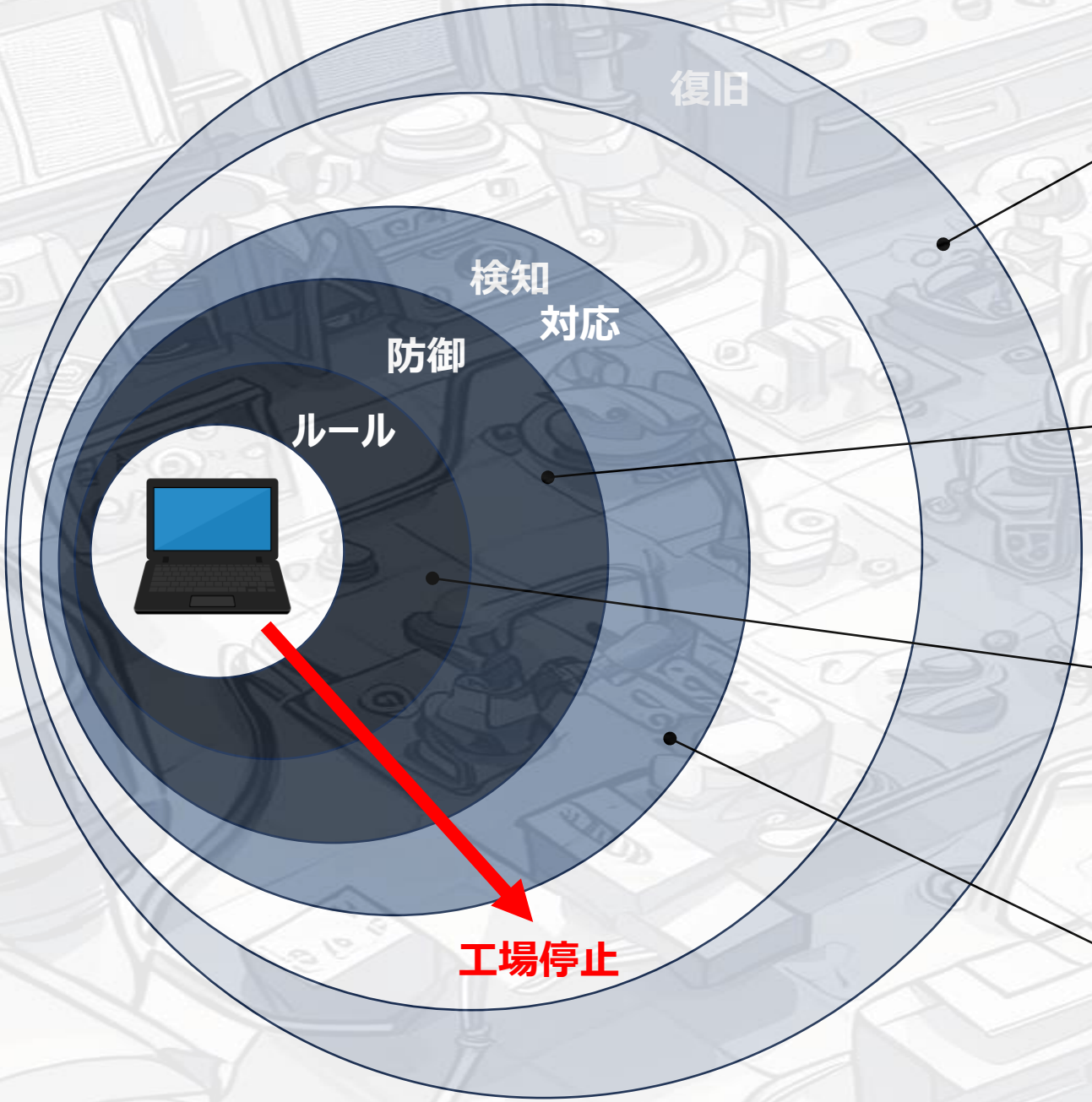
使用記録にウイルスチェックを実施した記録を残すこと。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：使用するウイルスチェックソフトは特に指定はないが、接続したUSBメモリーのチェックが行われることが必要。通常は情報系で使用しているソフトウェアと同じもので問題ない。

持込パソコン



02-01🛡,E-02💰,E-03💰
ルールによる使用管理は復旧に役立つ

02-02💰🛡,02-03💰
持込パソコンの脅威は水際で防御可能

02-01🛡
利用のルールとその徹底が最重要

02-04💰,E-01💰💰
パソコン接続を検知した後の運用が重要

🛡推奨対策 💰投資

対策No.02-01	関連する脅威の入口：持込パソコン

具体的な内容：持込パソコン使用ルールの策定と遵守

●対策内容

工場内で使用を許可する持込パソコンとその取り扱い方法をルールとして明文化し周知徹底する。

記載内容の具体例

-使用を許可する際の条件（OSバージョン、パッチ適用、ウイルスチェック※1、ネットワーク設定など）

-使用を許可する際の承認プロセス（現物確認や持込許可申請書など）

-持込パソコンの管理方法（許可済パソコンであることを示すタグ付けやシールなど。特に保守ベンダー持込時）

-持込記録

-作業日、承認者、作業者、使用パソコン、パッチ適用確認、ウイルスチェック確認

●運用のポイント

使用を許可されていない持込パソコンが工場内ネットワークに接続されないように注意すること。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：※1 パソコンのウイルスチェックは必須。より堅牢なチェックを行う場合は対策No.02-02を実施する。

対策No.02-02	関連する脅威の入口：持込パソコン

具体的な内容： 高度なアンチウイルスソフトの導入

●対策内容

工場内で使用される持込パソコンにはアンチウイルスソフトの導入を義務付けるが、従来のパターンマッチング技術ではマルウェアの検知に限界があるため、次世代のAIを使った未知のマルウェアが検出できるソフトを導入する。

●運用のポイント

工場内ネットワークにパソコンを接続した際に、アンチウイルスソフトが何らかの異常を検知した時は、速やかにネットワークからパソコンを切り離し、工場管理者等にエスカレーションする。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：持込パソコンに導入する高度なアンチウイルスソフトのライセンス料　10,000円～／年

対策No.02-03	関連する脅威の入口：持込パソコン

具体的な内容：持込パソコンの検疫･情報セキュリティ診断

●対策内容

持込パソコンを事前に検査し、状態が適正であることを確認するための検疫環境や情報セキュリティ診断ツールを導入する。対策No.02-01と併せて実施するとより効果的である。
（検疫環境や診断ツールでは、持込パソコンのパッチ適用状況やウイルスチェックの状況などが確認できる）

●運用のポイント

検疫環境や診断ツールのソフトウェアバージョンと使用するデータを最新状態に保つこと。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：診断ツール　10,000円～／月

対策No.02-04	関連する脅威の入口：持込パソコン

具体的な内容：工場ネットワークに接続されたデバイスの検知

●対策内容

デバイスがLANに接続(有線/無線)されたことを検知する仕組みを導入する。

-LANに接続するデバイスは申請制とし、MACアドレス、利用者、利用場所などを含むデバイス情報を管理する。

-LAN接続時（通信時）に出されるARP要求を監視するツールの導入を検討する。
（ツールには許可していない機器のLAN接続を阻止する仕組みを持つものもある）

-LANに接続されている機器を定期的に棚卸し現状を正確に把握する。
（ツールには自動で情報を収集できるものもある）

●運用のポイント

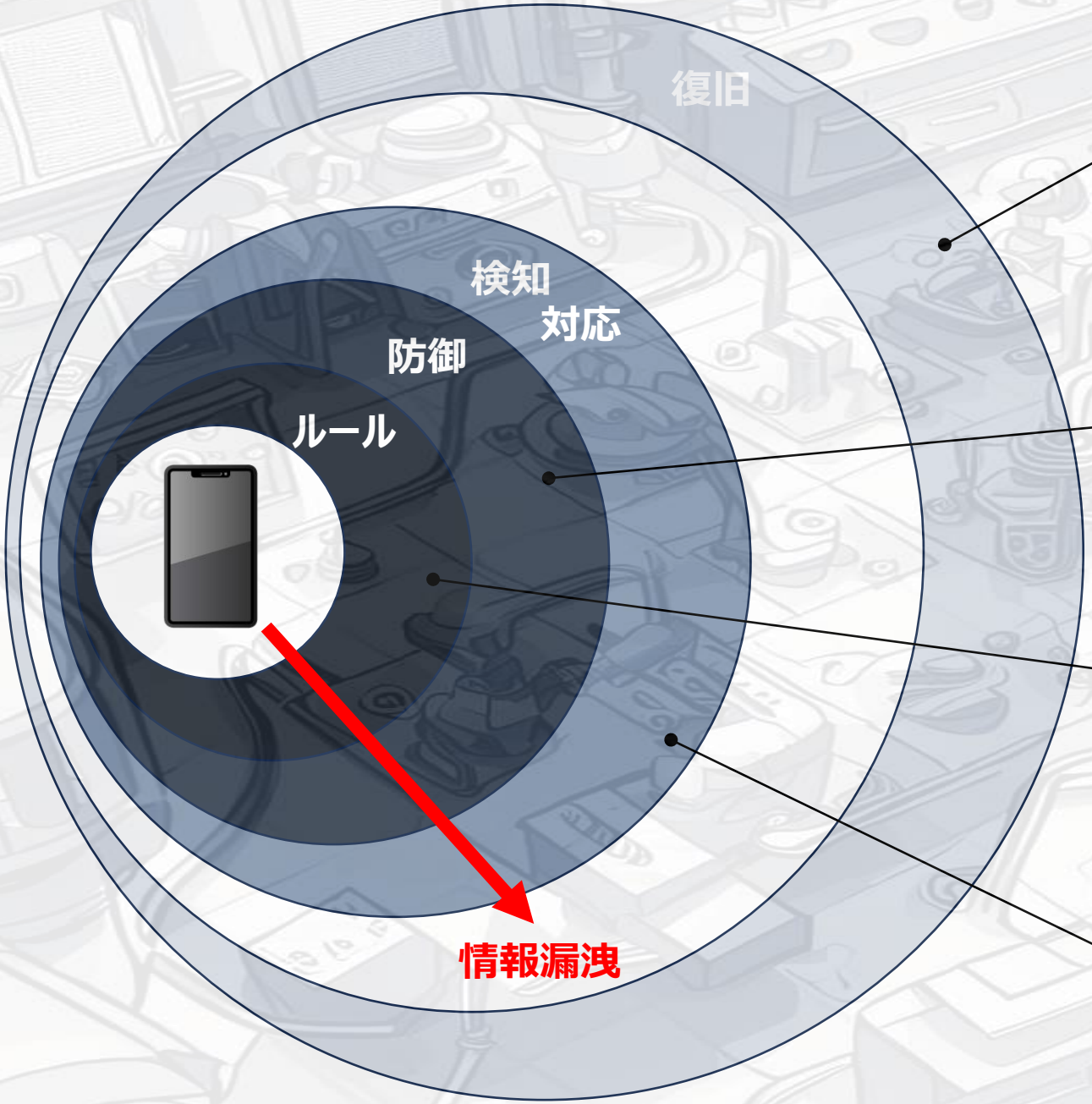
デバイスには資産管理番号など一意な記号を貼付け、目視でも不審なデバイスが無いか確認できるようにすること。

対策の種類：□被害に遭わないための対策　☑被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：無償ツールあり（有償ツールだと接続制限が可能　30万円～ ）

スマホ・タブレット



E-03💰
情報漏洩は発覚後の対応が重要

03-01💰、03-02
未許可で持ち込ませない、使わせない

03-01🛡️
利用のルールとその徹底が最重要

E-01💰💰
撮影や録音による情報漏洩は検知不可

🛡️推奨対策 💰投資

対策No.03-01	関連する脅威の入口：スマホ･タブレット

具体的な内容：スマホ･タブレット使用ルールの策定と遵守

●対策内容

工場内で使用を許可するスマホ･タブレットとその取り扱い方法をルールとして明文化し、周知徹底する。

記載内容の具体例

-使用を許可する際の条件（個人所有物の可否、WiFi/Bluetooth使用の可否、カメラ･マイクの使用可否、アンチウイルスソフトの導入など）

-使用を許可する際の承認プロセス（現物確認や持込許可申請書など）

-スマホ･タブレットの管理方法（許可済であることを示すタグ付けやシールなど。特に保守ベンダー持込時）

-持込記録（持込日、承認者、持込者、持込機器、持込目的など。外部からの訪問者も対象）

●運用のポイント

使用が許可されていないスマホ･タブレットが工場内に持ち込まれないように注意する

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　☑技術的対策

備考：工場内で無線機器の電波の影響を考慮する必要がある場合は、持ち込まれたスマホやタブレットのテザリング機能の使用を制限するなどの注意も必要。アンチウイルスソフトのライセンス　5,000円～／年

対策No.03-02	関連する脅威の入口：スマホ･タブレット

具体的な内容：工場内無線LANのフィルタリング設定

●対策内容

工場内LANにスマホやタブレットの接続を許可している場合は、無線LAN装置のフィルタリング設定によって未許可の機器が接続されないように制限（MACアドレスによるフィルタリングなど）する。対策No.03-01と併せて実施するとより効果的である。

●運用のポイント

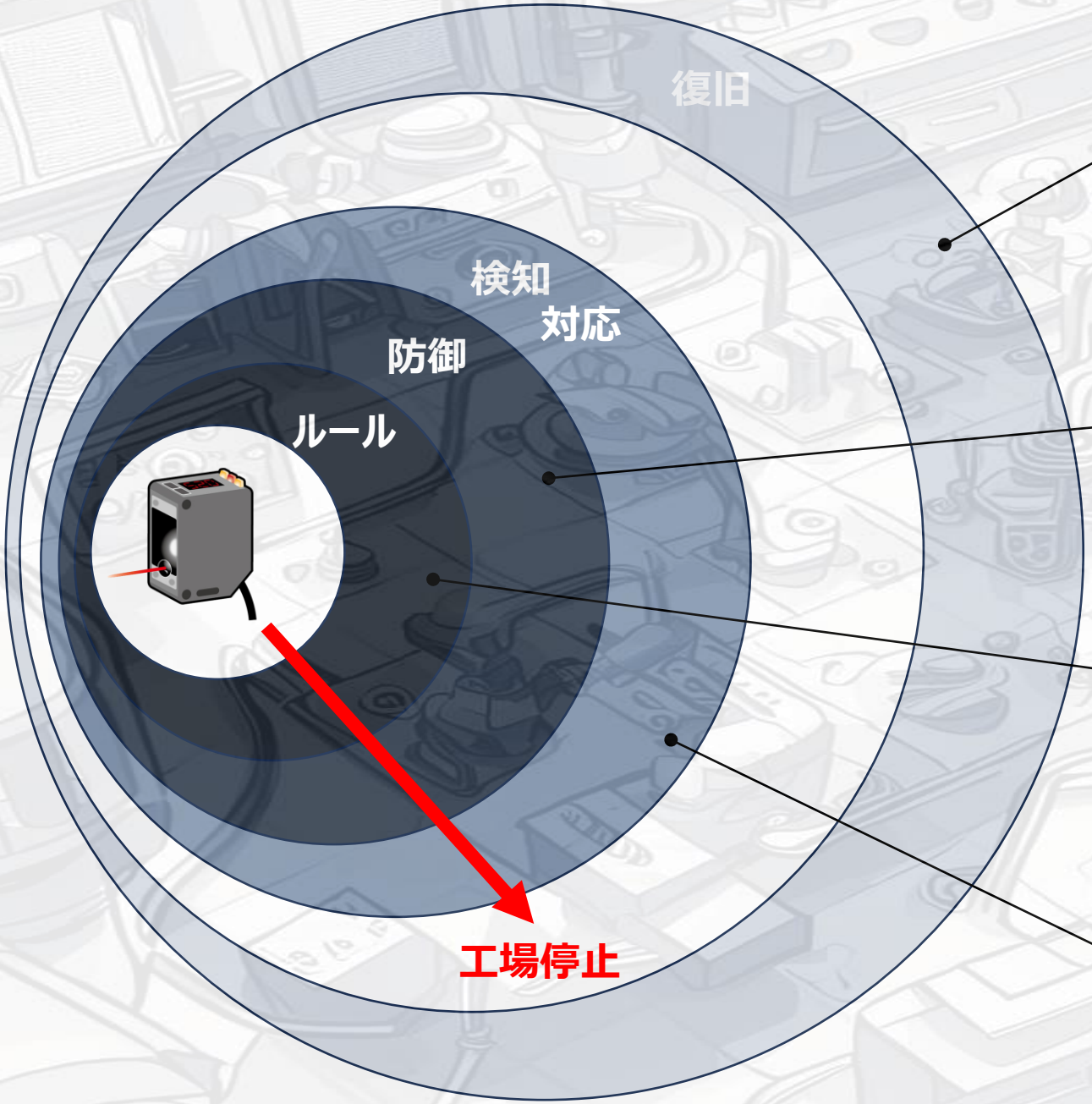
無線LANのフィルタリング設定は、都度、登録するには運用負荷が高いため、あらかじめ決められた機器のみに限定する方がよい。ただし、無線LANへの接続が許可されていないスマホやタブレットでも、自身が契約するキャリアネットワークには接続が可能なため、対策No.03-01によるルールとの整合性をよく検討すること。（カメラやマイクを許可すれば情報漏洩リスクは残る）

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：無線LAN装置に登録できるMACアドレスの数は、装置によって異なるためあらかじめ確認しておく必要がある。

IoT機器・センサー



04-01,E-02,E-03
一般的な復旧手段

04-03
IoT機器のセキュリティ設定は確実に行う

04-01,04-02
ネットワーク設計と実態把握は重要

E-01
攻撃の可能性を判断するスキルが必要

推奨対策 投資

対策No.04-01	関連する脅威の入口：IoT機器･センサー

具体的な内容：構成管理（デバイスリスト）でIoT機器･センサーの所在と数を把握

●対策内容

工場内LANにデバイスを接続するためのルール（申請･承認フロー）を策定し、無断で接続されることがないように管理する。

工場内LANに接続されているデバイスを把握し、工場内LANにつながるIoT機器･センサーの実態を確認する。

●運用のポイント：

継続的にデバイスリストを更新すること。

人手による管理が難しい場合は、ネットワークに接続された機器の情報を自動的に収集する方法もある。（対策No.02-04参照）

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　☑技術的対策

備考：IoT機器やセンサーのアップデートも確実に行う必要がある。

対策No.04-02	関連する脅威の入口：IoT機器･センサー

具体的な内容：ネットワークデザイン（基本設計）と再構築

●対策内容

ネットワークをゾーン（ネットワークセグメント、VLAN）に分け、IoT機器やセンサーなどのデバイスが接続されるネットワークと生産機器が接続される工場内LANは物理的に分離、もしくはファイアウォールを設置し、必要最小限のアクセスに限定させるように構成を見直す。
また、現行の設計が既に上記のような方針である場合、実態と設計に乖離がないことを確認する。

●運用のポイント：

ネットワーク構成図を最新化し、実態と乖離がないように保つこと。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：ベンダーにネットワークデザインや構築を依頼した場合の費用　100万円～

対策No.04-03	関連する脅威の入口：IoT機器･センサー

具体的な内容：IoT機器･センサーに備わる最低限のセキュリティ設定

●対策内容

IoT機器･センサーの認証機能を正しく設定する。（デフォルトパスワードのまま使用しない）
IoT機器･センサーへの接続制限機能（フィルタリング、ファイアウォール）があれば設定し、不必要な接続の試みを遮断する。
導入時は重大な脆弱性がないできるだけ最新のファームウェアを適用する。

●運用のポイント：

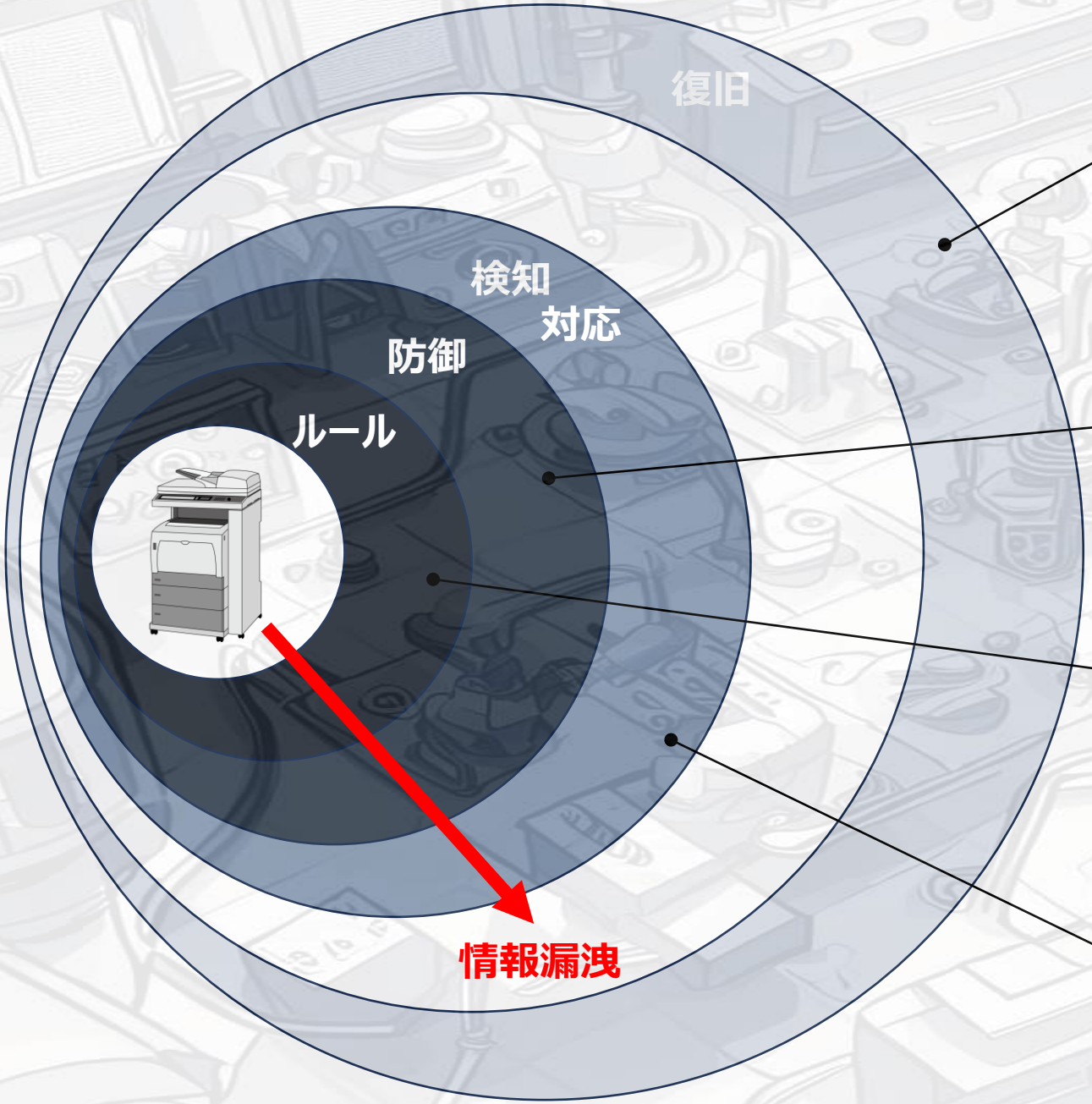
IoT･センサーの脆弱性情報に注意し、適切にアップデートを行うこと。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：導入済のIoT･センサー機器の設定変更のみでもセキュリティ強度はかなり向上する。

複合機



E-03 💰
情報漏洩は発覚後の対応が重要

05-01🛡,05-02🛡,05-03,05-04
管理者・利用者を特定する

05-05
ルールではないが、考慮すべき対応

05-02🛡,E-01💰💰
定期的なログの確認が有効

🛡推奨対策 💰投資

対策No.05-01	関連する脅威の入口：複合機

具体的な内容：複合機の管理者権限を設定する

●対策内容

複合機の各種設定メニューにアクセスできる権限者を限定し、アクセスのためのパスワードを設定する。

●運用のポイント

管理者権限者はできるだけ少人数に絞ること。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：複合機によっては上記のような機能がないものもあるため、新規導入、リプレースの際にはできるだけ機能を有する製品を選ぶ

対策No.05-02	関連する脅威の入口：複合機

具体的な内容：運用時の不正アクセス対策のための設定

●対策内容

以下、複合機の設定を実施する。

-利用者のIDとパスワードを設定する。

-パスワードロック（パスワードを複数回間違えるとロックアウト機能が働く）機能を有効にする。

-利用ログ、アクセスログの保存を有効する。

●運用のポイント

利用ログ、アクセスログを定期的にサンプリングして確認すること。

対策の種類：☑被害に遭わないための対策　☑被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：複合機により設定機能のないものがある。

対策No.05-03	関連する脅威の入口：複合機

具体的な内容：通信における情報漏洩対策のためのネットワーク設定

●対策内容

複合機の保守ベンダーに以下の設定を依頼する。

-インターネット等外部との接続はファイアウォールまたはルータを経由して接続する。
-不要なネットワークプロトコルはOFFにする。
-IPフィルタリング機能を有効にし、複合機にアクセスできるIPアドレスを制限する。
-外部からリモートで管理する場合は、IPSec、SSL/TLS等の暗号化通信を使用する。
-無線機能を使用する場合は、WPA2/3暗号化通信を使用する。
-リモートメンテナンスは電話回線に限定する。（上記のような対策ができない場合）

●運用のポイント

セキュリティ設定が第三者によって変更されないように、IDとパスワードを設定しておくこと。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：複合機により、ネットワークの設定機能がないものもある

対策No.05-04	関連する脅威の入口：複合機

具体的な内容：暗号化と自動削除の設定

●対策内容

複合機の保守ベンダーに以下設定及び対応を依頼する。

-印刷するデータの暗号化機能がある場合はこれを有効化する。また、自動削除機能がある場合はできるだけ短い時間で削除されるように有効化する。

-TPM（Trusted Platform Module）搭載機の場合は暗号鍵をTPMに保存する。

-TPMの有無に関わらず廃棄または返却時は上書き消去機能でデータを消去する。

●運用のポイント

複合機保守ベンダーまたは製造メーカーにデータが消去されたことを確認する方法を確認し、消去担当者以外の人に確認させること。

暗号化や自動削除などの設定が変更されないように、管理者権限の設定も合わせて実施することが望ましい。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：複合機によっては上記のような機能がないものもあるため、新規導入、リプレースの際にはできるだけ機能を有する製品を選ぶ。

対策No.05-05	関連する脅威の入口：複合機

具体的な内容：廃棄または返却時のデータ消去依頼

●対策内容

複合機の廃棄または返却時は保守ベンダーにデータを消去依頼する。

●運用のポイント

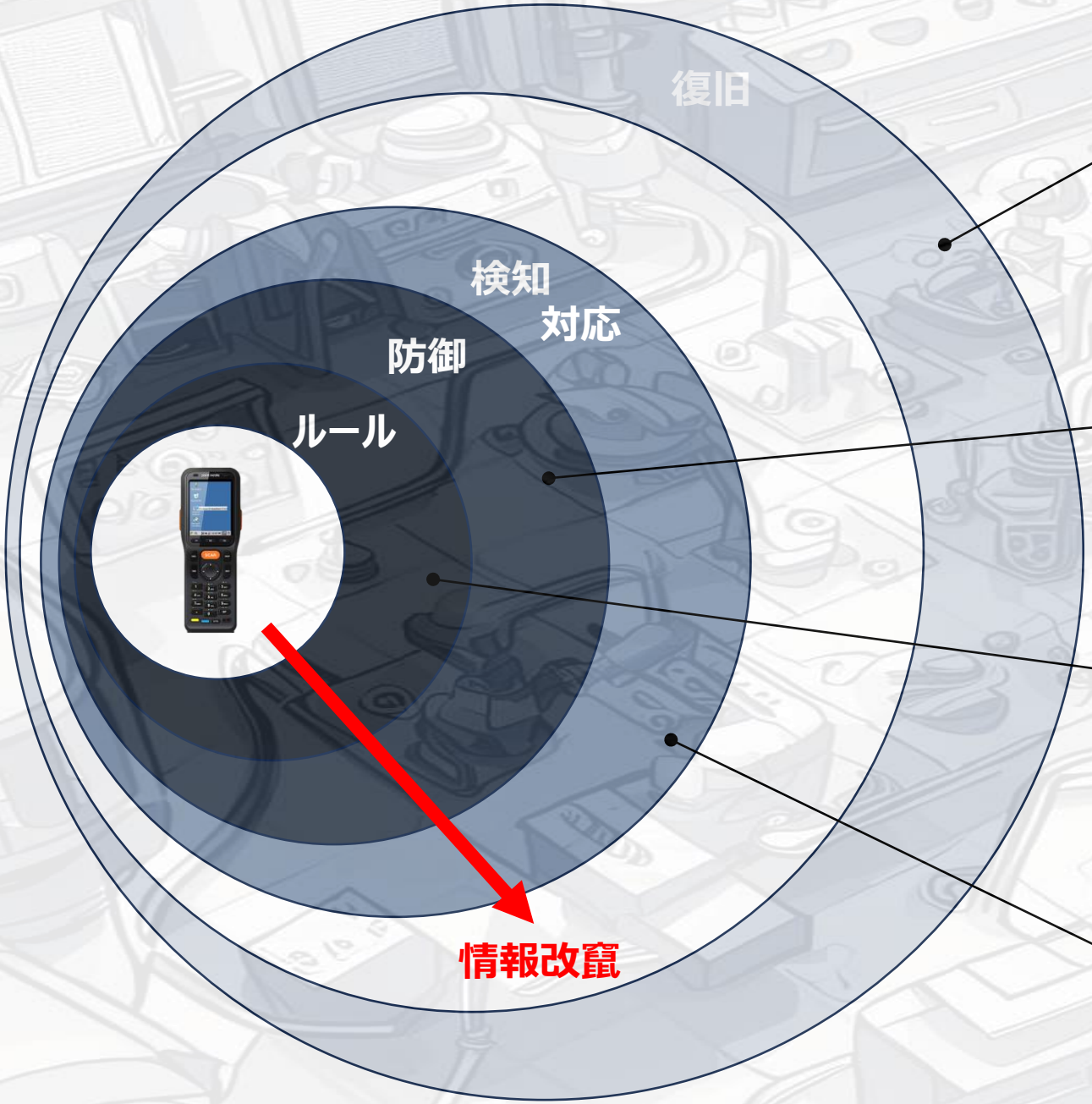
保守ベンダーがデータを消去する場に社員が立ち会うこと。もしくは、データ消去証明書等を受領すること。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：複合機のリユースなどにより情報が漏洩するリスクがあることを認識しておくことが重要

ハンディターミナル



06-01🛡,E-03💰
使用管理は調査や復旧に役立つ

06-02🛡,06-03💰
アプリケーションの最新化が重要

06-01🛡,06-04
保管と利用の管理が最重要

06-04,06-05
チェック体制の構築が必要

🛡推奨対策 💰投資

対策No.06-01	関連する脅威の入口：ハンディターミナル

具体的な内容：保管場所と使用の管理

●対策内容

ハンディターミナルを保管する場所を明確にし、第三者が無断で触れることのないように管理する。
ハンディターミナルの使用を都度、記録する。

●運用のポイント

管理台帳・使用台帳として最新の状況が把握できるように確実に運用する。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：☑物理的対策　☑人的対策　□技術的対策

備考：保管場所は、部外者が立ち入らない場所か施錠ができる場所を選ぶ

対策No.06-02	関連する脅威の入口：ハンディターミナル

具体的な内容：ハンディターミナルのOSやアプリケーションの最新化

●対策内容

ハンディターミナルの製品ベンダーサイトなどから情報を入手し、OSやアプリケーションのバージョンを最新化する。

●運用のポイント

OSやアプリケーションの更新を行う責任者を決め、管理台帳などにバージョンアップを行った記録を残すこと。
（更新機能がない場合は、念のために製品ベンダーに安全性を確認する）
必要な機能のみの使用に制限すること。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：ハンディターミナル自体をネットワークに接続しない場合でも、データの取込みなどを行うためのステーションがパソコンやネットワークに接続されている場合は、セキュリティ侵害を受ける可能性がある。

対策No.06-03	関連する脅威の入口：ハンディターミナル

具体的な内容：ウイルスチェック

●対策内容

ハンディターミナルもしくはステーションを接続するパソコンにウイルス対策ソフトを導入し、定期的にウイルスチェックを行う。

●運用のポイント

ウイルスチェックを行うタイミングなどを明確にし、ハンディターミナルごとにウイルスチェックの実施有無が分かるように管理すること。（管理台帳など）

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：パソコンのウイルスチェックソフト　5,000円～／年

対策No.06-04	関連する脅威の入口：ハンディターミナル

具体的な内容：データ誤入力対策のための運用ルールの設定

●対策内容

工場内で使用するハンディターミナルの運用ルールを定める。具体的な記載内容は以下の通り。

-定期的（例えば、4半期ごと）にハンディターミナル製造メーカーの脆弱性情報を確認

-脆弱性がある場合のファームウェアー及びパッチの適用

-定期的な棚卸の実施

●運用のポイント

購買、会計情報との齟齬、棚卸時に齟齬が発生した場合、理由（ハンディーターミナルを通さずに従業者が物を持っていった、ハンディターミナルの誤動作等）を明らかにすること。

対策の種類：□被害に遭わないための対策　☑被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：機種によりセキュリティパッチの適用ができないものがある

対策No.06-05	関連する脅威の入口：ハンディターミナル

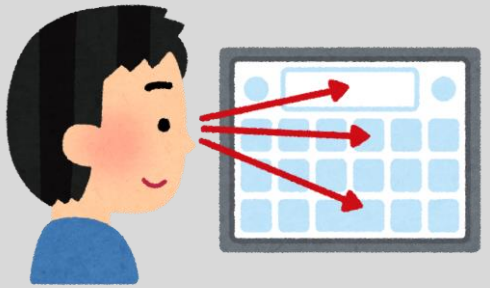
具体的な内容：データ不整合検出時の対応

●対策内容

ハンディターミナルで取り込んだデータを処理した際に何らかの不整合が見つかった場合、ハンディターミナルがセキュリティ侵害を受けている可能性を考慮する。具体的には、該当のハンディターミナルの使用は見合わせ、可能であればウイルスチェックを実施するか、製品ベンダーに相談する。

●運用のポイント

不整合の原因がハンディターミナルからのデータか、情報処理系の問題かを早期に見極められる体制やチェック機能を設けること。

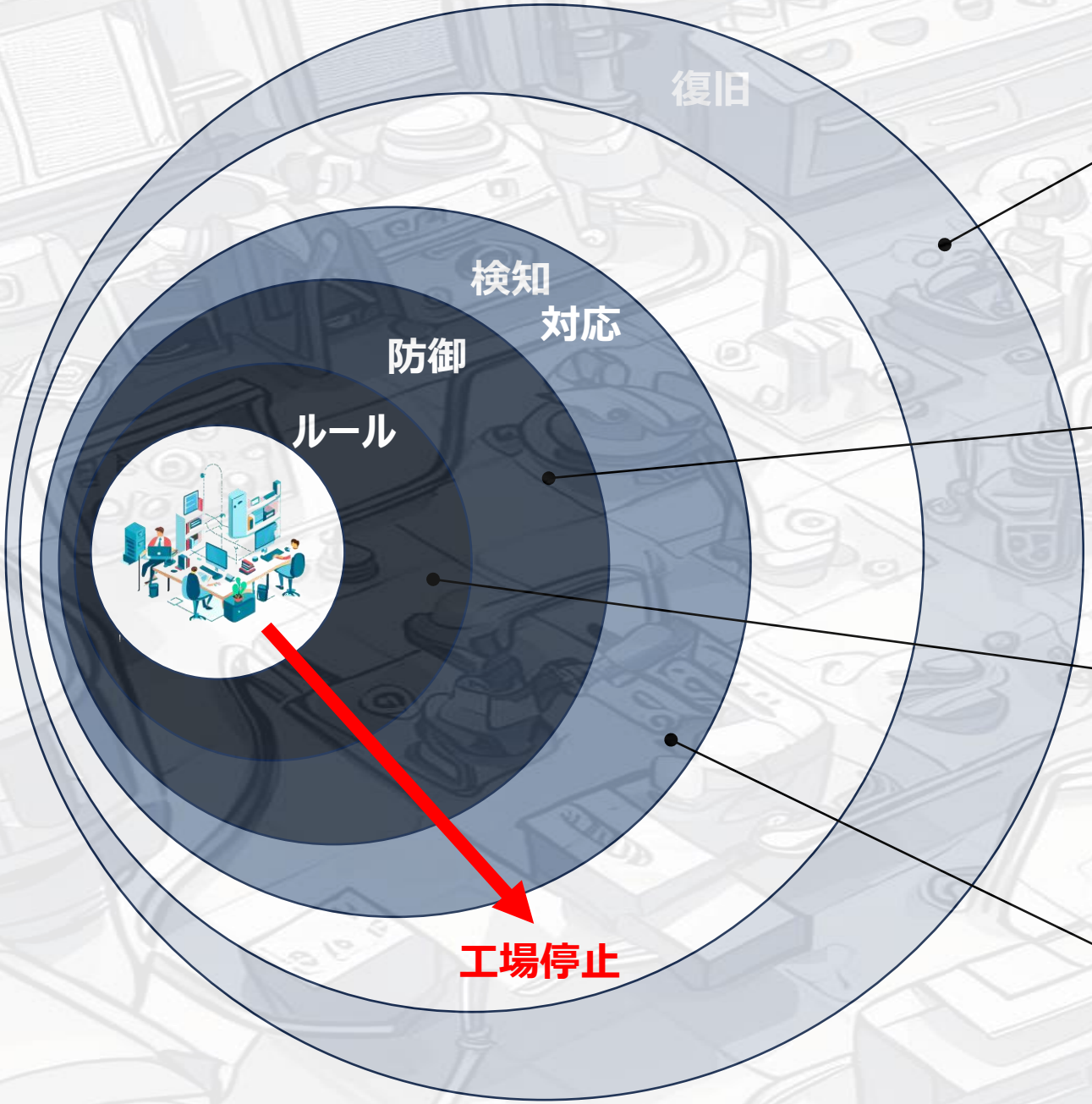


対策の種類：□被害に遭わないための対策　☑被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：

OAネットワーク



07-04,E-02💰,E-03💰
一般的な復旧手段

07-03💰💰🛡
ネットワーク境界で防御する

07-01🛡,07-02🛡
現状確認とリスクの把握が最重要

07-04💰🛡,E-01💰💰
ネットワーク境界の防御が前提

🛡推奨対策 💰投資

対策No.07-01	関連する脅威の入口：OAネットワーク

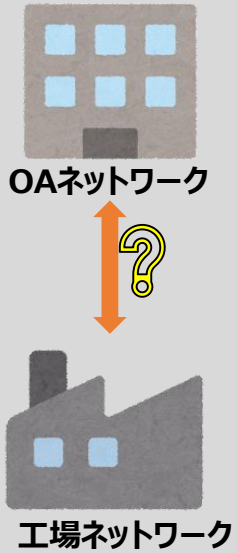
具体的な内容：ネットワークの接続状況の確認

●対策内容

ネットワーク構成図と機器設置状況や配線を目視確認することにより、工場ネットワークとOAネットワークの接続の有無を確認する。

●運用のポイント：

直接接続されている場合は、No.07-03の対策を検討する。
パソコンやサーバーにLAN線を2本つなぐ方法でOAネットワークと接続している場合も安全な方法ではないため、No.07-03の対策を検討する。



対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：☑物理的対策　☑人的対策　□技術的対策

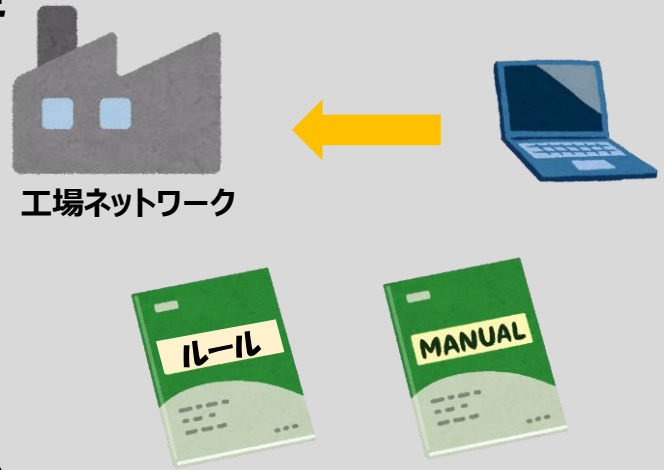
備考：目視で確認できない場合は、工場ネットワーク側のパソコンからOAネットワーク側のサーバー等に向けたpingを送信してみる方法で確認できる場合もある。

対策No.07-02	関連する脅威の入口：OAネットワーク

具体的な内容：OAネットワーク側で使用しているPCや機器の持ち込みルールの策定

●対策内容

工場ネットワークにOAネットワークで使用しているPCや機器を持ち込む際の条件を明確にしたルールを作成し運用する。
運用マニュアルやガイドラインの中にOAネットワークのPCや機器を無断で接続してはいけない旨を記載し、周知徹底する。



●運用のポイント：

ルールだけではなく、業務上、接続せざるを得ない場合の手順書も用意すること。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：工場ネットワーク内の機器は十分なセキュリティ対策ができないものが多く、不用意な接続は大きな事故に繋がる

対策No.07-03	関連する脅威の入口：OAネットワーク

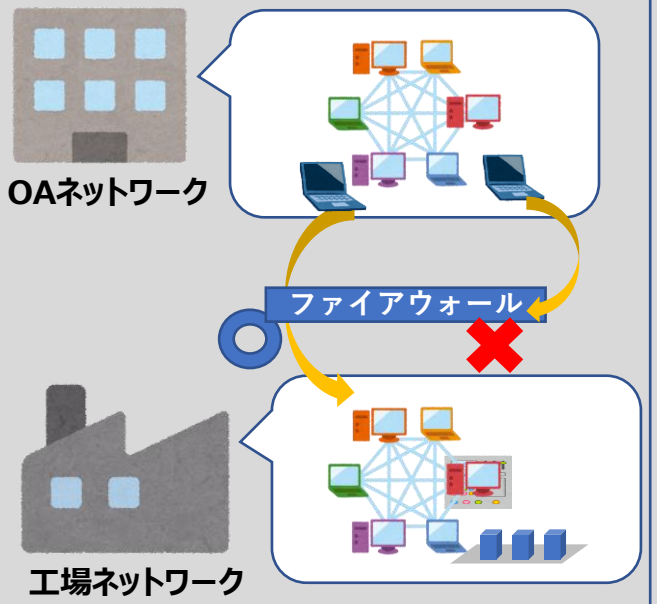
具体的な内容：OAネットワークからの接続制限

●対策内容

工場ネットワークにOAネットワークで使用するPCや機器を無条件に接続させない為の仕組みを構築し運用する。具体的には、OAと工場の境界にファイアウォールを導入し、工場ネットワークに接続できる機器を制限する。

●運用のポイント：

工場ネットワーク内に新規の機器を導入する場合は、その都度、ファイアウォールの設定を見直すこと。



対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：OAネットワークはDHCPでIPアドレスが管理されているケースが多く、PCのアドレスが一意には決まらないため、ファイアウォールでの制限は、セグメント単位となる（固定IPが付与されているサーバーなどは個別に指定できる）

対策No.07-04	関連する脅威の入口：OAネットワーク

具体的な内容：工場ネットワークの通信内容のモニタリング

●対策内容

工場ネットワーク内の機器とOAネットワーク内の機器との通信もしくはOAネットワークを経由して外部のネットワークと通信する場合、通信内容をモニタリングしてマルウェアの感染拡大等の動きを早期に検知する。

-工場ネットワークとOAネットワークの境界にファイアウォールまたはルータを設置し、OA-工場ネットワーク間の通信プロトコルを必要な(許可された)ものだけに制限する。

-OAネットワーク側に導入されたIPS/IDS、サンドボックスなどからマルウェアを検知する。

●運用のポイント

一般的にファイアウォールやIPS/IDP、サンドボックスなどはOAネットワークの管理であるため、何らかの異常を検知した場合の連携体制を確立しておくこと。

対策の種類：□被害に遭わないための対策　☑被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：検知した結果には誤検知や過検知が含まれるので的確に判別するためには専門知識が必要

対策No.08-01	関連する脅威の入口：インターネット

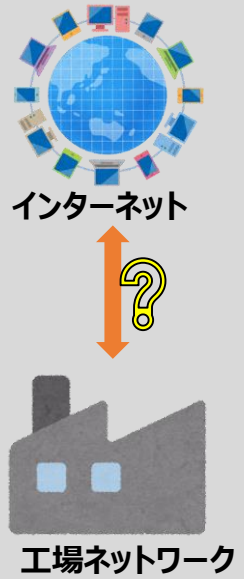
具体的な内容：ネットワークの接続状況の確認

●対策内容

ネットワーク構成図と機器設置状況や配線を目視確認することにより、工場ネットワークがインターネットに直接接続されていないことを確認する。

●運用のポイント：

直接接続されている場合、もしくはOAネットワークを経由してインターネットに接続されている場合は、No.08-02以降の対策を検討する。
遠隔保守のためにVPN接続環境がある場合は、セキュリティ対策の内容をベンダーに確認する。
パソコンにモバイルルーターが接続されているケースもあるので見逃さないように注意する。

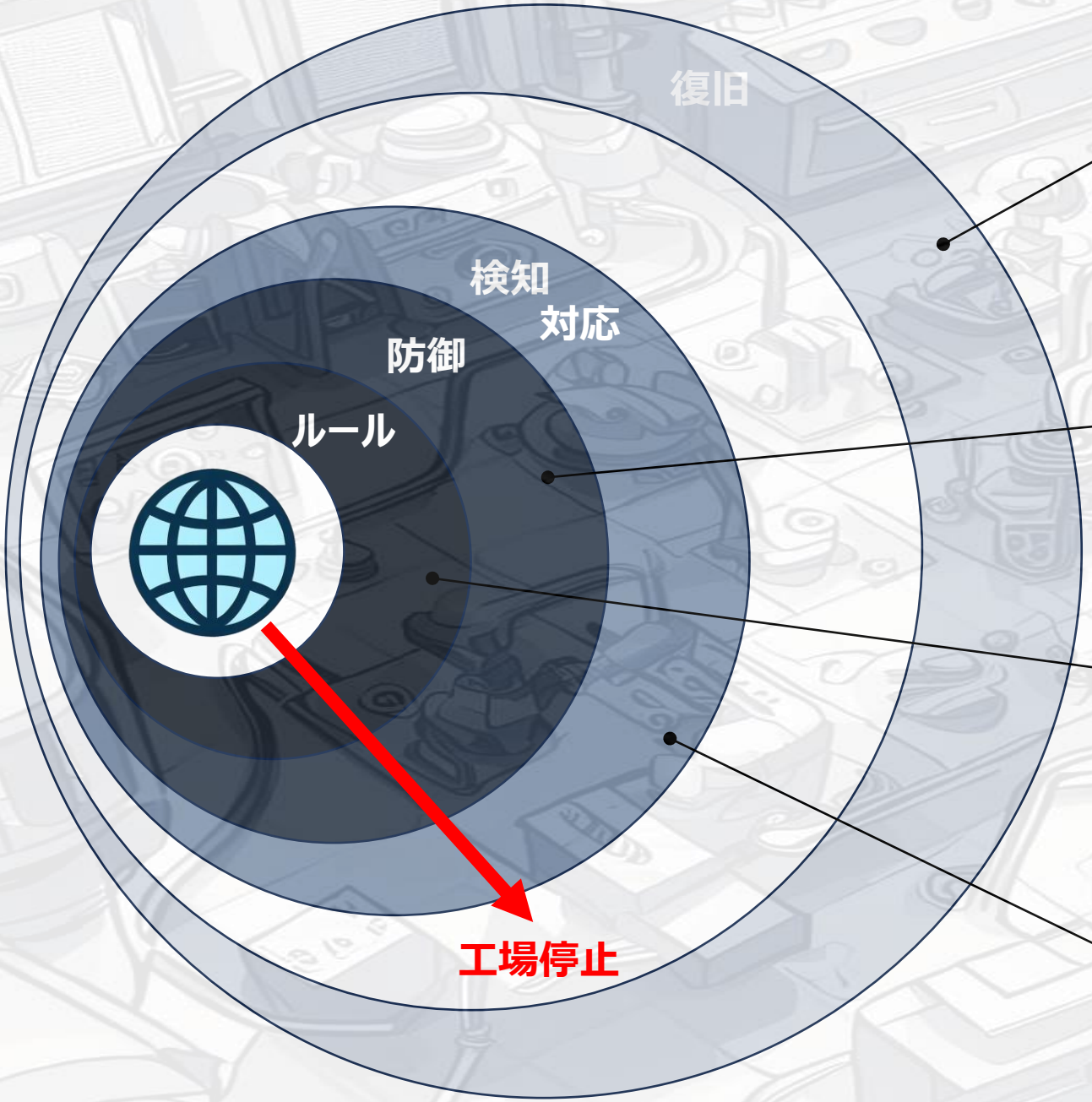


対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：管理外のインターネット接続の有無は経費（プロバイダー利用料）から確認する方法もある。

インターネット



E-02💰,E-03💰
一般的な復旧手段

08-04💰🛡
ネットワーク境界で防御する

08-01🛡,08-02🛡,08-03
利用のルールとその徹底が最重要

08-04🛡,E-01💰
ネットワーク境界の防御が前提

🛡推奨対策 💰投資

対策No.08-02	関連する脅威の入口：インターネット

具体的な内容：インターネット利用用途や使用機器のルール化

●対策内容

工場内からのインターネット利用を許可する用途や使用する機器を明確にしルールや規約を策定する。
（原則としてはWEB閲覧やメールの送受信は許可しない）
インターネット接続にパソコンやサーバーを使用する場合は、パッチ適用やウイルス対策ソフトの導入を行う。
教育等で現場の担当者に周知し、勝手に外部と接続させないように管理する。

●運用のポイント：

ルールだけではなく、業務上、例外的に接続せざるを得ない場合の手順書も用意する。
ルールや規約が遵守されているかを定期的に確認する。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：工場内からのインターネット利用は、機器の保守、他拠点接続、安全なクラウドサービスの利用などに限定することが望ましい。また、実際の接続に際しては、VPNを利用するなどの安全対策を考慮すること。

対策No.08-03	関連する脅威の入口：インターネット

具体的な内容：他拠点や取引先とインターネットで接続する際の接続条件のルール化

●対策内容

インターネットを利用して外部と接続を行う際の条件を明確にしルールや規約を策定する。
（接続方法、接続相手の選定基準、接続相手のセキュリティレベルなど）
教育等で現場の担当者に周知し、無断で接続されないように管理する。

●運用のポイント：

既存の取引先の中には、策定したルールに適合しない状態で接続されている場合も考えられるため、一定の猶予期間内で改善することを求めるなどが必要となる。また、その間はリスクがあることを全社で理解しておくことも重要である。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：接続方法としてはVPNの利用が一般的。インターネットではなく専用線で接続する場合も相手の選定基準やセキュリティレベルの確認は必要。

対策No.08-04	関連する脅威の入口：インターネット

具体的な内容：インターネット接続点のモニタリング（監視）と防御

●対策内容

工場ネットワークから直接インターネットに接続する場合は、ファイアウォールを設置し、通信相手や利用するサービスを制限する。また、外部からの攻撃を防御するための不正侵入防御システム（IPS）の導入も検討する。
OAネットワークを経由してインターネットに接続する場合は、対策No.7のOAネットワークを参照。

●運用のポイント：

ファイアウォールポリシー（通信許可ルール）はできるだけ必要な通信に絞ること。特にインターネットから工場内に向けた通信は基本的に許可しない。（VPN接続による遠隔保守や他拠点接続のための通信のみ許可するなど）
IPSは誤検知が発生することがあるため、検知内容が確認できるスキルを持った人材の確保が必要。外部ベンダーに相談するなども方法のひとつ。

対策の種類：☑被害に遭わないための対策　☑被害を早期発見するための対策　☐被害から早期復旧するための対策

対策の分類：☐物理的対策　☐人的対策　☑技術的対策

備考：インターネットプロバイダーが提供するファイアウォールサービスもある。自前で構築する場合は、機器のみで10万円～。

Wi-Fi（無線AP）

E-03、E-05
情報漏洩は発覚後の対応が重要

C-01、09-02
機器を管理する

09-01
現状確認とリスクの把握が最重要

E-01
定期的なログの確認が有効

推奨対策 投資

対策No.09-01	関連する脅威の入口：Wi-Fi（無線AP）

具体的な内容：工場内LANに接続されている無線機器の把握

●対策内容

工場内LANに接続されている機器の実態を調査し、認識のない無線機器が存在しないことを確認する。
工場内LANに接続する無線機器設置のためのルールを策定（申請・承認フロー）し、確実に管理をする。
（ルールには用途、無線仕様、認証、接続制限方法、管理責任者などを記載する）

●運用のポイント：

無線APを設置する場合、無断で個人のスマートフォンやタブレットが接続されないように制限すること。
敷地外への電波漏洩についても確認し、必要に応じて、無線APの設置場所の変更、出力の調整、電磁波シールドを導入するなどで利用できるエリアを限定する。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　☑技術的対策

備考：無線APに無断で接続されないようにSSID／PWは管理者のみで共有するか、無線APのフィルタリング機能等で接続を許可する端末（MACアドレス）を制限する。

対策No.09-02	関連する脅威の入口：Wi-Fi（無線AP）

具体的な内容：無線APのセキュリティ設定

●対策内容

無線APの管理者ID(変更できない場合もある)、パスワード及びSSID/PW(暗号化キー)はデフォルと値を変更しておく。
WEP、WPAの古い暗号化方式は使用せず、WPA2以降の暗号化方式を使用する。
暗号化アルゴリズムが選択可能な場合はAESを選択する。
MACアドレスの認証機能を使用して、接続を許可する端末を制限する。

●運用のポイント：

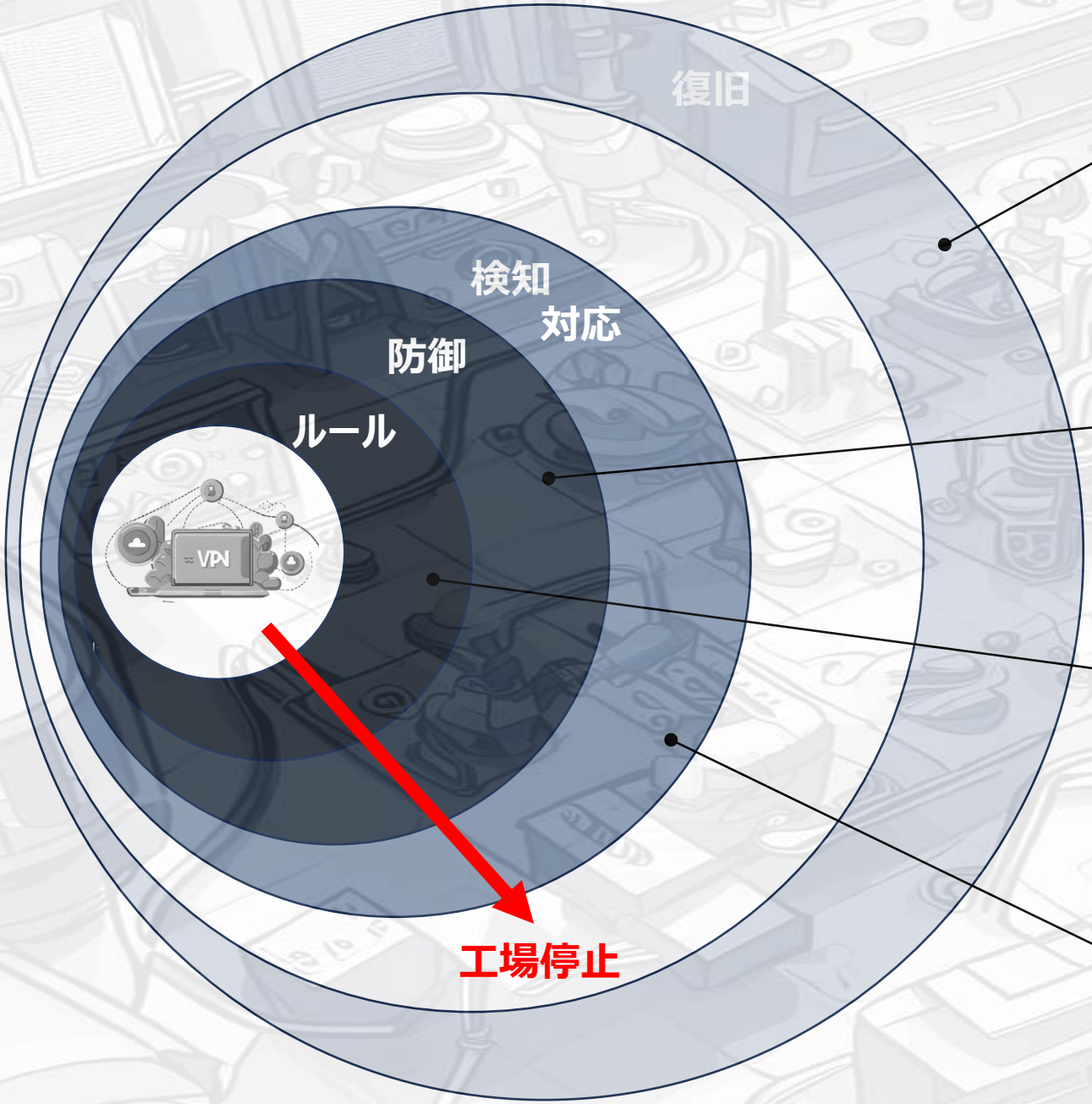
無線APには企業用と個人用がある。企業用の無線APは高価だが、認証サーバとの連携、細かなアクセス制御ができ高度なセキュリティ機能を持っている。重要な情報を扱う場合は、企業用APの使用を検討する。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：無線APに無断で接続されないようにSSID／PWは管理者のみで共有する。

保守用ネットワーク



E-02💰,E-03💰
一般的な復旧手段

10-02💰🛡
OAネットワーク、インターネットを参照

10-01🛡
OAネットワーク、インターネットを参照

E-01💰💰
ネットワーク境界の防御が前提

🛡推奨対策 💰投資

対策No.10-01	関連する脅威の入口：保守用回線

具体的な内容：保守用ネットワークの実態把握と改善

●対策内容

工場内にある製造装置などを遠隔保守するためのネットワークの有無、接続方法を調査する。
インターネットを利用した遠隔保守の場合、
-直接インターネットに接続されている場合は、対策No.08も参照すること。
-OAネットワーク経由でインターネットに接続されている場合は、対策No.07も参照すること。

●運用のポイント

保守用ネットワークは機器ベンダーが設置・管理している場合があるが、任せきりにならないように、セキュリティ対策の状態などを確実に把握しておくこと。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：保守用回線から情報セキュリティの脅威が侵入しないことを保守ベンダーに確認し、懸念がある場合は改善を要求する。（VPN装置の脆弱性対応、アクセス制御、認証情報の管理、ベンダー側のセキュリティ対策など）

対策No.10-02	関連する脅威の入口：保守用回線

具体的な内容：遠隔保守環境の把握と改善

●対策内容

保守用ネットワークを経由して製造装置を保守する場合、通常は工場内に設置したパソコンなどに接続し、ここを踏み台として製造装置にアクセスをするケースが多い。この踏み台パソコンの対策として以下を検討する。

-ウイルス対策ソフトウエアの導入
-OSアップデート（パッチ適用）
-アクセス制御（この踏み台パソコンからアクセスできる先を対象となる製造装置に限定する）

●運用のポイント

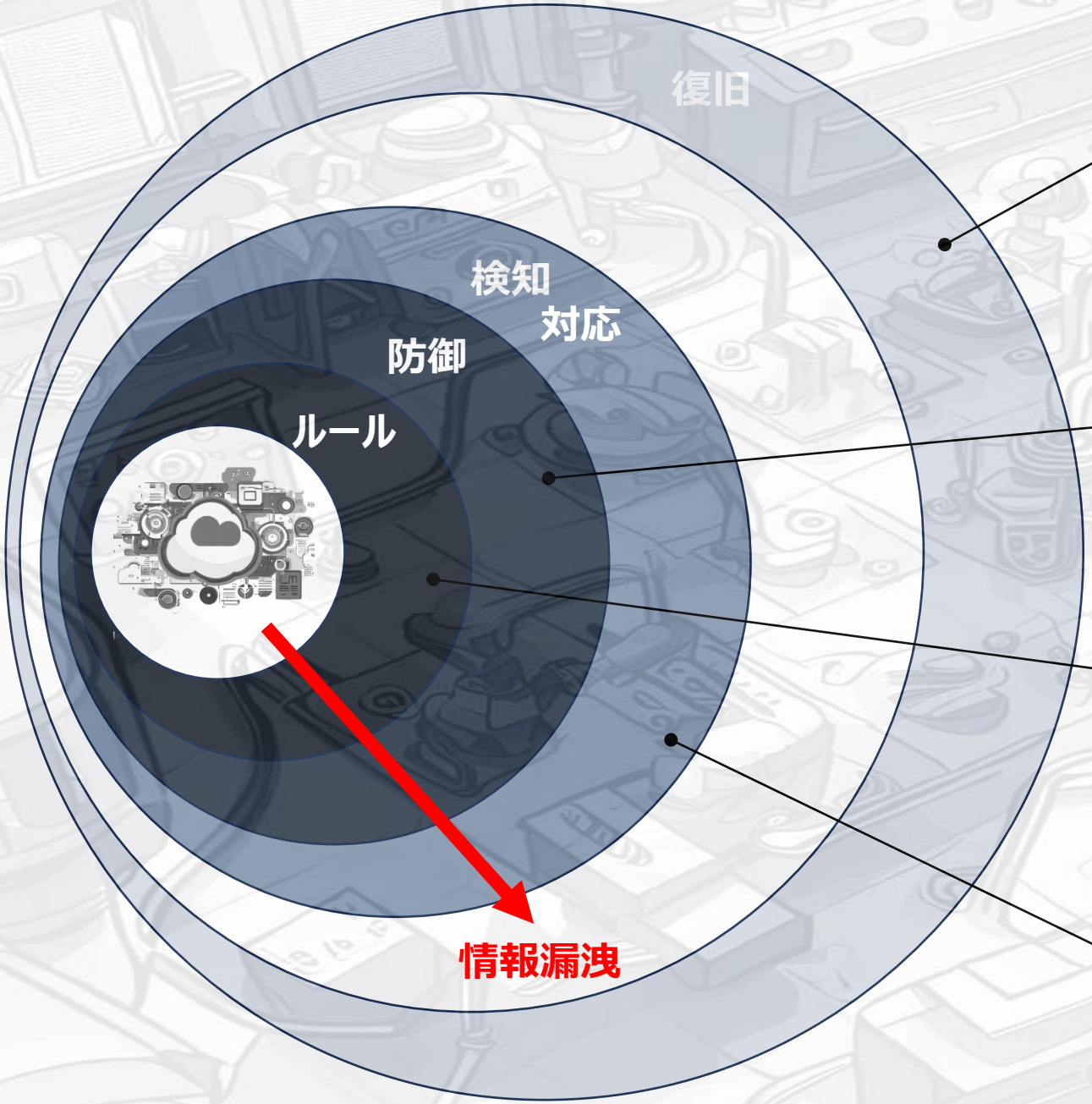
保守用の踏み台パソコンを機器ベンダーが設置している場合は、上記対策を申し入れること。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：ウイルス対策ソフトウエアが導入・アップデートできない場合は、製造装置ベンダーと協議の上、その危険性を認識しておく

クラウドサービス



E-02💰,E-03💰
一般的な復旧手段

個別対策はなし
OAネットワーク、インターネットを参照

11-01🛡
OAネットワーク、インターネットを参照

E-01💰💰
ネットワーク境界の防御が前提

🛡推奨対策 💰投資

対策No.11-01	関連する脅威の入口：クラウドサービス

具体的な内容：クラウドサービス利用のためのルール策定

●対策内容

クラウドサービスを選定、利用する際に意識すべき下記の事項を明確にしたルール、規約を策定する。

-利用目的、サービス事業者の評価、SLA
-アクセス方法、通信保護、認証方式
-利用者管理、データ管理、代替え手段確保の考え方
-直接インターネットに接続されている場合は、対策No.08も参照すること。
-OAネットワーク経由でインターネットに接続されている場合は、対策No.07も参照すること。

●運用のポイント

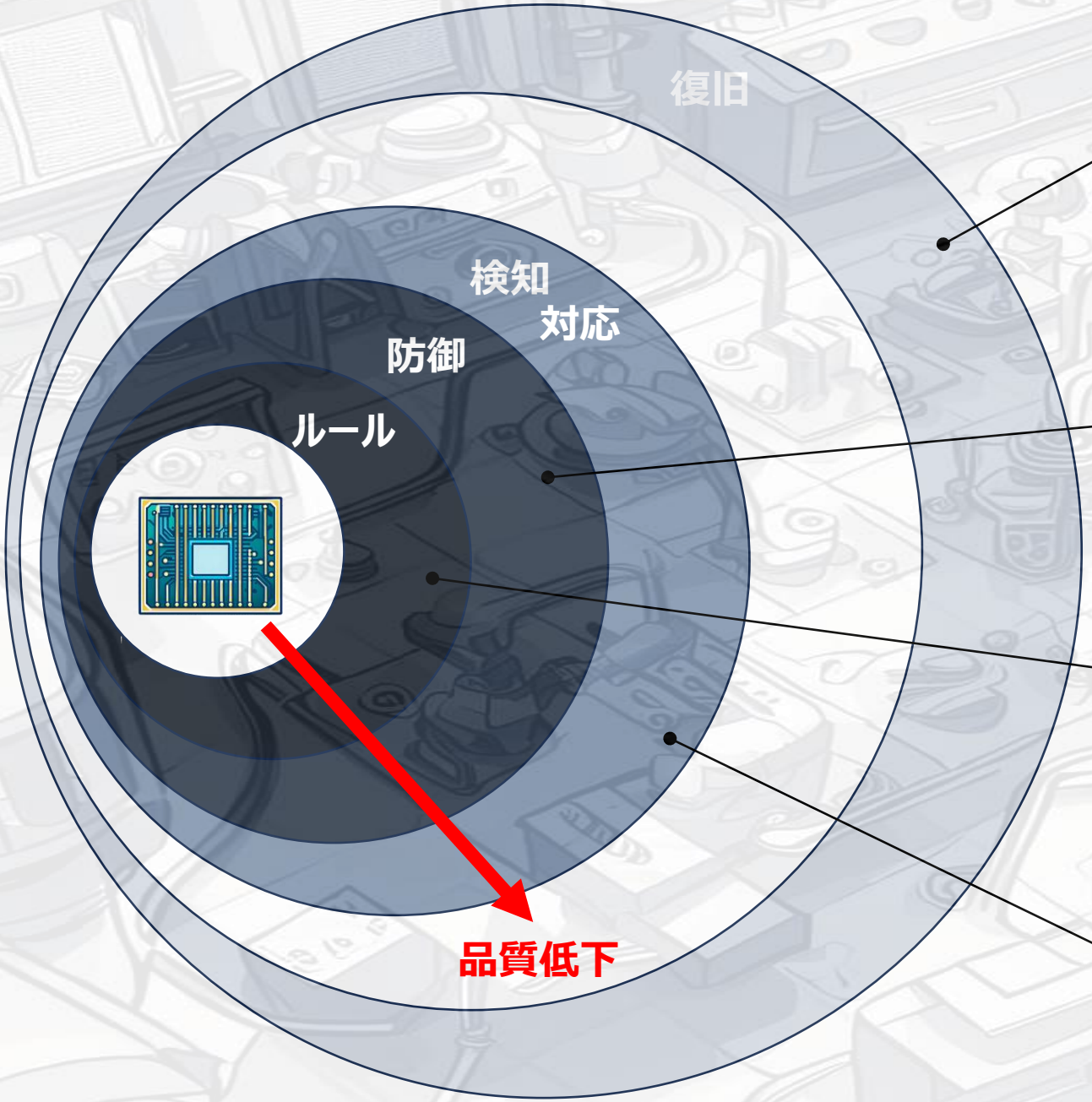
自社に合ったルールを策定すること。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：IPA発行「中小企業の情報セキュリティ対策ガイドライン第3.1版」付録６「中小企業のためのクラウドサービス安全利用の手引き」が参考になる

部品・原材料



12-03
ルールに従う

12-01,12-02,12-03
ルールに従う

12-01,12-02,12-03
ルールの策定とその徹底が最重要

12-02
ルールに従う

推奨対策 投資

対策No.12-01	関連する脅威の入口：部品･原材料

具体的な内容：セキュリティリスクが混入する可能性がある部品･原材料の新規調達ルールの策定

●対策内容

自社取り扱い部品･原材料の内、セキュリティリスクが混入する可能性があるものを明確にする。
部品･原材料の受け入れ基準を明確にし、セキュリティ観点でも受け入れ検査が実施できるようにする。
-セキュリティリスクの混入を検知するためのテスト方法を明確にすること
-業界標準等の基準がある場合は、それに従いテストを実施すること

●運用のポイント

実際には、受け入れ側が部品･原材料のセキュリティチェックを行うことは容易ではないため、部品･現材料の調達先がセキュリティチェック結果を提示し、その結果に責任を持つことを契約事項等に明記する方法が現実的。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：セキュリティリスクは、製品が市場に出てもすぐに影響が出ないこともあるため、できるだけ最初の段階で取り除くことが重要。

対策No.12-02	関連する脅威の入口：部品･原材料

具体的な内容：セキュリティリスクが混入する可能性がある部品･原材料の受入れ後の品質保証ルールの策定

●対策内容

受入れ後の品質保証のルールを定める。主な記載内容は以下の通り。

-部品･原材料に脆弱性があった場合の調達先からの報告方法
-報告受領後の対応方法
-再受入れの手順

●運用のポイント

問題のある部品や原材料が組み込まれた製品が市場に出るまでに対応することが重要であり、平時からの調達先との連携が重要となる。

対策の種類：☑被害に遭わないための対策　☑被害を早期発見するための対策　☐被害から早期復旧するための対策

対策の分類：☐物理的対策　☑人的対策　☐技術的対策

備考：

対策No.12-03	関連する脅威の入口：部品･原材料

具体的な内容：製品出荷後の脆弱性対応ルールの策定

●対策内容

製品出荷後の脆弱性対応のルールを定める。具体的な記載内容は以下の通り。

-所轄官庁、IPA等への報告の必要有無

-ホームページ等での脆弱性の内容、影響範囲の公開

-脆弱性の解消方法

●運用のポイント

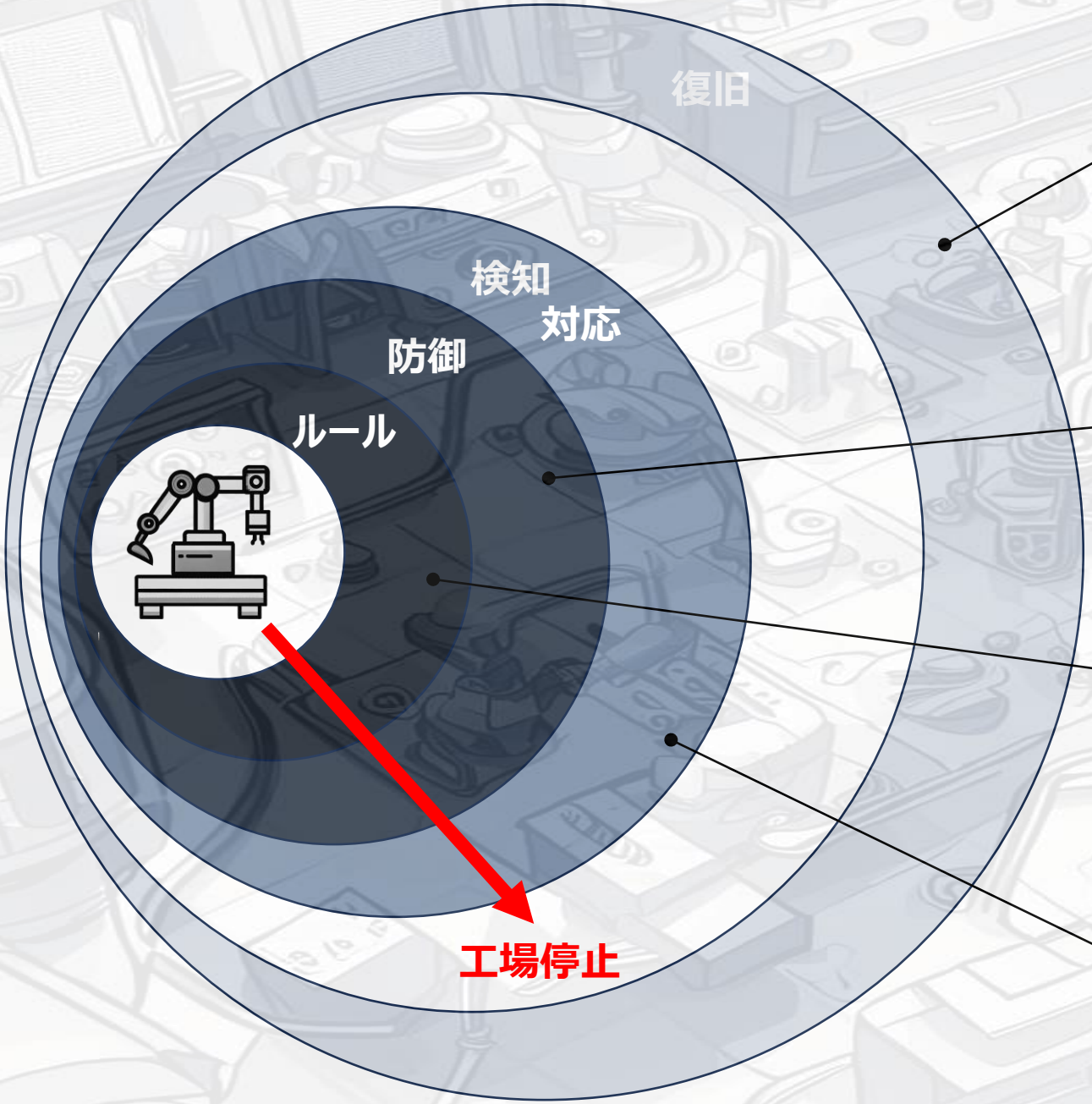
実際に製品に脆弱性があった場合、脆弱性情報の報告、公開、解消方法の見直しを実施する。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：

新規購入機器



13-01
ルールに従う

13-02
水際で防御する

13-01
ルールの策定とその徹底が最重要

13-02
ルールに従う

推奨対策 投資

対策No.13-01	関連する脅威の入口：新規購入機器

具体的な内容：機器の評価ルールの策定

●対策内容

機器を新規購入する場合の評価ルールを定める。具体的な記載内容は以下の通り。

-購入前に、対象となる機器のセキュリティ対策を評価すること。
-機器メーカがセキュリティチェックをしている場合は、評価結果を入手すること。
-USBメモリーを使用する機器の場合は、一度利用したUSBメモリーをウイルスチェックソフトで検査すること。
-ネットワーク接続機能がある場合は、評価用ネットワーク（ハブとネットワークモニタリングツールを導入したPC）に接続し、不正なトラフィック（機器の仕様書にない通信）が流れていないか確認すること。

●運用のポイント

試験期間を設け、期間中は工場内LANには直接接続（ファイアウォール、ルータ等経由）しない。

対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：ネットワークモニタリングツールは無償（フリー）で使用できるものもある。

対策No.13-02	関連する脅威の入口：新規購入機器

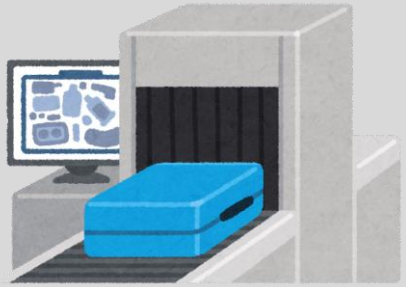
具体的な内容：受入検査

●対策内容

新規に機器を購入し受入れる際に実施している品質検査にセキュリティ観点を加える。具体的には、マルウェアなどの混入がないかを検査する。検査ができない場合は、サプライヤーからセキュリティ検査合格証などを発行してもらう。

●運用のポイント

受入時に検知できなくても、後日、脆弱性が見つかる場合もあるため、
サプライヤーとはセキュリティ観点で情報の連携を継続すること。

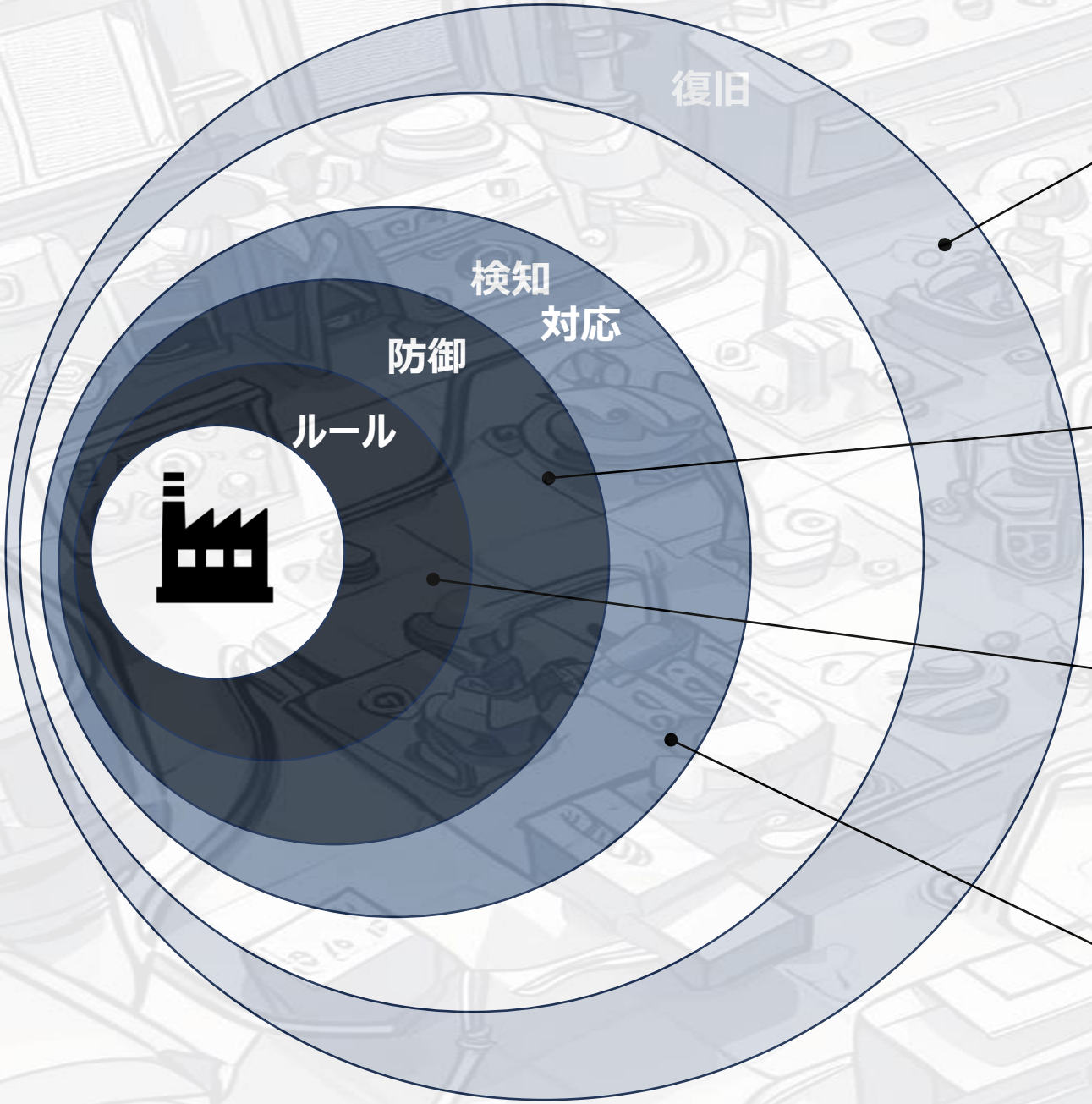


対策の種類：☑被害に遭わないための対策　□被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：□物理的対策　☑人的対策　□技術的対策

備考：

高度な共通対策



E-02 💰🛡️,E-03 💰
確実なバックアップを持つ

E-01 💰💰
ネットワークトラフィックをモニタリングする

🛡️推奨対策 💰投資

対策No.E-01	関連する脅威の入口：共通

具体的な内容：工場ネットワーク内の通信内容のモニタリング

●対策内容

工場ネットワーク内の機器間の通信内容をモニタリングして工場内でのマルウェアの感染拡大等の動きを早期に検知する。具体的には、工場ネットワーク内のネットワーク機器（スイッチなど）からトラフィック情報を収集し、通信量や通信先の変化を監視する。（工場内の通信はある程度、パターン化されている場合が多い）

●運用のポイント

全てのネットワーク機器からトラフィック情報を集めることは困難なため、ポイントを絞って監視すること。

対策の種類：□被害に遭わないための対策　☑被害を早期発見するための対策　□被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

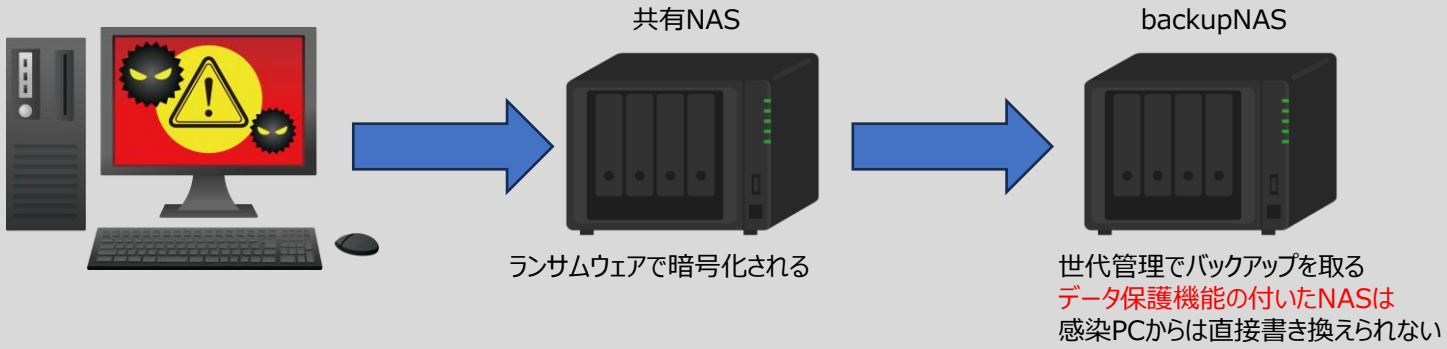
備考：普段と異なる通信量や通信パターンの分析にはある程度のデータの蓄積が必要
ログ収集装置、ログ管理サーバー、分析ソフトウェア、システム構築　300万円～

対策No.E-02	関連する脅威の入口：共通

具体的な内容：バックアップ

●対策内容

守りたい装置のデータを共有NASに保存し、NAS連携機能でBackup NASに世代管理されたデータを保管することで、ランサムウェア感染前のデータを復元できる。



●運用のポイント

バックアップはシステムに変更が加わるなどのタイミングで漏れなく取得すること。
ランサムウェア感染対策に有効なデータ保護機能付(インミュータブル)きNASのファームウェアはセキュリティパッチを適用する。

対策の種類：□被害に遭わないための対策　□被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：NAS×2、システム構築　５０万～

対策No.E-03	関連する脅威の入口：共通

具体的な内容：原因解析のためのログの取得

●対策内容

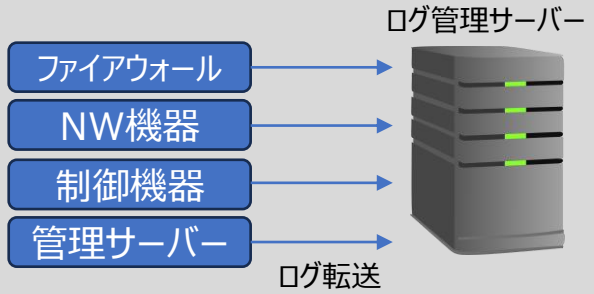
Syslogサーバーを導入し、以下ログを収集する。

-ファイアウォールのアクセスログ

-機器の保守ベンダーに依頼可能な場合は、機器を制御しているコンピュータ（Windows、UNIX、LINUX等）のセキュリティログ

●運用のポイント

問題発生時はすぐにsyslogサーバーをネットワークから切り離し、ログを保全する。



対策の種類：□被害に遭わないための対策　□被害を早期発見するための対策　☑被害から早期復旧するための対策

対策の分類：□物理的対策　□人的対策　☑技術的対策

備考：有償（保存するログ量により必要なリソースが変わる）

用語集①

【アセット管理】
組織が保有する価値のあるもの。情報資産、人的資産、物的資産などを管理すること

【ID/PW】
アカウントの識別番号とパスワード

【マルウェア】
ユーザのデバイスに不利益をもたらす悪意のあるプログラムやソフトウェアの総称。コンピュータウイルスもこの一種

【アンチウイルスソフト】
コンピュータウイルスからコンピュータシステムを守るソフトウェア

【IPアドレス】
ネットワーク上で機器を識別するためのアドレス情報

【MACアドレス】
機器に付与されたユニークなアドレス情報

【ARP要求】
ネットワーク上の機器のIPアドレスとMACアドレスの対応関係を調べるための通信パケット

用語集②

【認証機能】
利用者や機器が正当なものであることを確認するための機能

【IPA】
独立行政法人　情報処理推進機構（経済産業省のIT政策実施機関）

【OS】
オペレーティングシステム。コンピュータを動かすための基本ソフトウェア

【パッチ】
ソフトウェアの脆弱性を修正するためのプログラム

【パスワードロック】
パスワードを複数回間違えるとロックアウト機能が働く機能

【ファイアウォール】
ネットワーク間の不正なアクセスを遮断するための装置

【ファームウェア】
コンピュータのハードウェアに組み込まれたソフトウェア

用語集③

【フィルタリング機能】
不正なアクセスを遮断するための機能

【リモートアクセス】
遠隔地からコンピュータにアクセスすること

【ルータ】
ネットワークを複数のセグメントに分割するための装置

【ログ】
コンピュータの操作履歴や通信内容などを記録したファイル

【VLAN】
仮想的なネットワーク

【脆弱性】
ソフトウェアやシステムのセキュリティ上の欠陥

【IPSec、SSL/TLS】
通信内容を暗号化することにより盗聴を防ぎ、通信内容が改ざんされていないことを担保するためのプロトコル

用語集④

【WPA2/3】
無線LANの暗号化規格

【WEP、WPA】
WPA2/3よりも古い暗号化規格

【TPM】
Trusted Platform Module。コンピュータのセキュリティ機能を強化するためのチップ

【データ誤入力対策】
ハンディターミナルで入力されたデータの誤入力を防ぐための対策

【データ不整合検出】
ハンディターミナルで取り込んだデータに不整合がないかを検知するための対策

【OAネットワーク】
オフィスで使用されるネットワーク

【工場ネットワーク／OTネットワーク】
工場で使用されるネットワーク

用語集⑤

【DHCP】
ネットワークに接続した機器にIPアドレスを自動で割り付けるプロトコル

【IDS】
不正侵入検知システム（Intrusion Detection System）

【IPS】
不正侵入防御システム（Intrusion Prevention System）

【サンドボックス】
外界から隔離された仮想空間でマルウェアの動作などが安全に確認できる

【VPN】
Virtual Private Networkの略。IPSecなどで暗号化された仮想的なトンネルによる安全な通信路

【SSID】
無線APを識別するための名前

この用語集は、あくまでも参考情報としてご利用ください。
用語の意味は、状況によって異なる場合があります。

◇参考◇ 「JNSAソリューションガイド」で検索（https://sg.jnsa.org/）

対策カテゴリー	検索キーワード
基礎的な共通対策	入退室管理、IT資産管理、教育、訓練
USBメモリー	外部接続デバイス制御、ウイルス対策、検疫
持込パソコン	ウイルス対策、検疫、端末接続制御
スマホ・タブレット	ウイルス対策
IoT機器・センサー	IT資産管理
複合機	廃棄機器
ハンディターミナル	ウイルス対策
OAネットワーク	ファイアウォール、IDS、IPS、可視化、アクセス制御
インターネット	ファイアウォール、IDS、IPS、VPN、インターネット
Wi-Fi（無線AP）	無線
保守用ネットワーク	ファイアウォール、VPN
クラウドサービス	ファイアウォール、IDS、IPS、VPN、インターネット
部品・原材料	脆弱性検査
新規購入機器	脆弱性検査
高度な共通対策	モニタリング、可視化、バックアップ、ログ