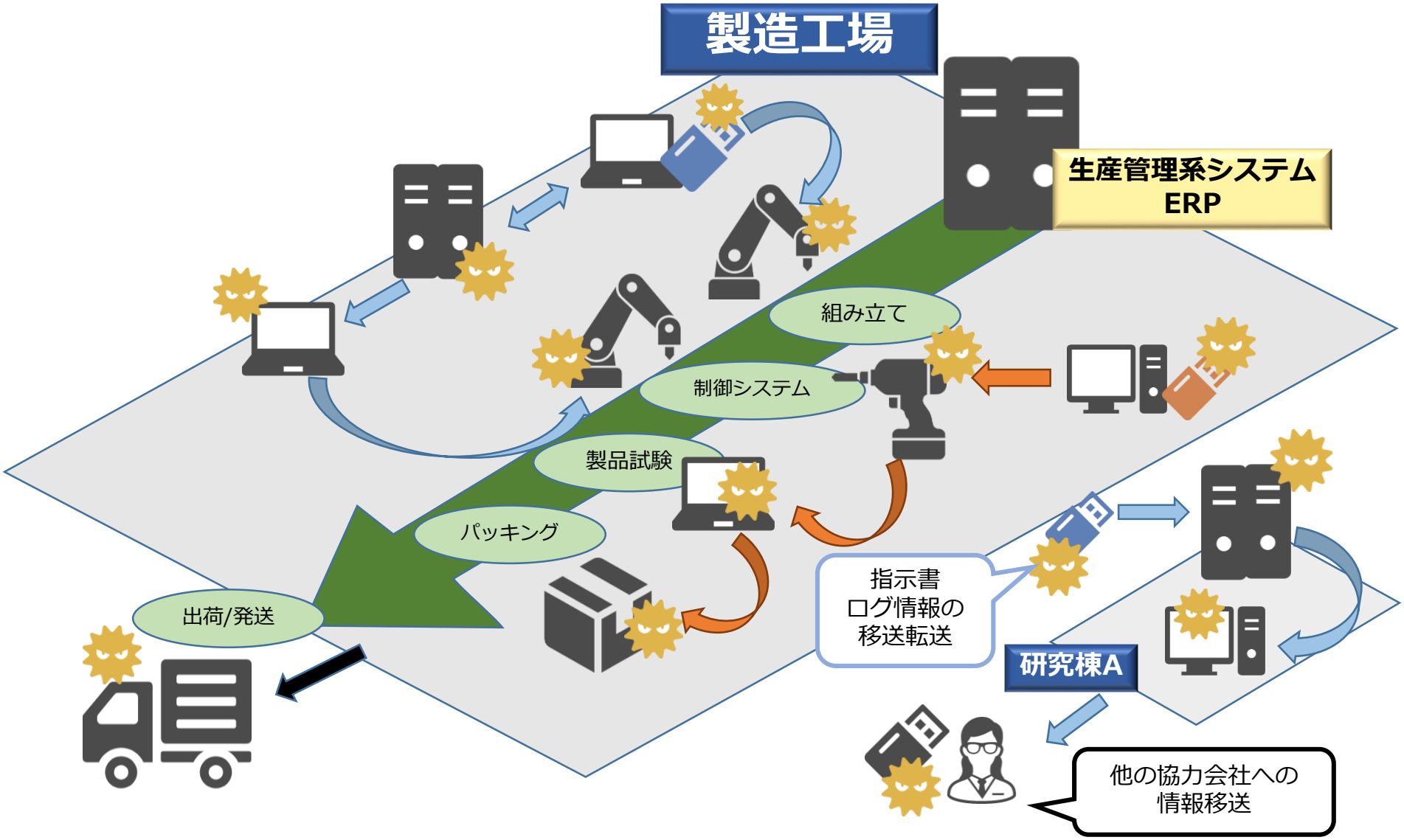
技術と感動をつなぐ
Metro

品質不良を防ぐ！
生産ラインに潜む脅威への対策
～脅威の実態編～

株式会社メトロ
営業本部　セキュリティ営業部
技術本部　セキュリティグループ

生産ラインにおけるマルウェア侵入経路

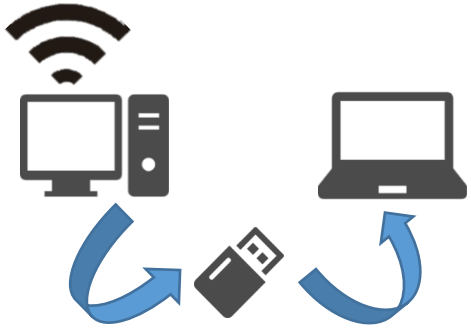


オフライン端末の利用

レガシーOS/Linuxの利用

USBによるデータ移行

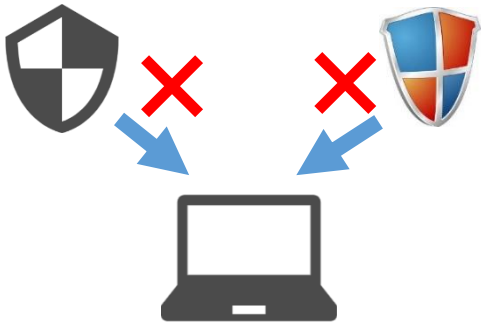
生産ラインにおけるマルウェア侵入経路



①生産記録やログ情報の
やり取りをUSBで行っている

②生産ラインは
オフラインのため、
脅威対策をしていない

③制御用ソフトウェアが
新OSに対応していないため、
レガシーOSを使用



④Linuxに導入できる
脅威対策がない

**どれか一つでも生産ラインに当てはまると、
マルウェアが侵入し、品質不良を起こす原因となります**

マルウェアによる被害

検査端末がマルウェアに
感染することで、生産機器に
誤作動が発生する可能性がある。

出荷物がソフトウェアの製品の場合、
マルウェアが入ったまま出荷することで、
ネットワークを介して他製品に影響を
及ぼす可能性がある。

製品の品質不良

マルウェアが工場PCに入り込み、
顧客情報や設計図などの情報を盗む

機密情報の漏洩

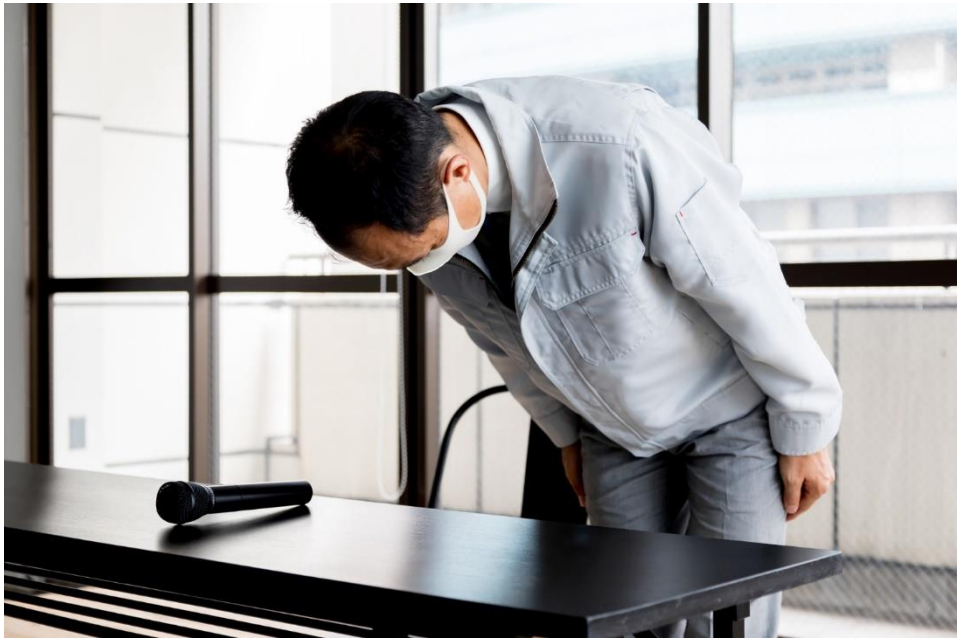
マルウェア被害による影響

問題発生の原因調査に多くの工数がかかる

・不良品がどの範囲まで出荷されてしまったか
・関係各所への連絡
・原因調査
・
・
・

風評被害やブランドイメージの低下

・取引先の減少
・生産ラインの維持が困難になる
・顧客や従業員の不安増加
・
・
・



マルウェア被害による影響　リスク/損失

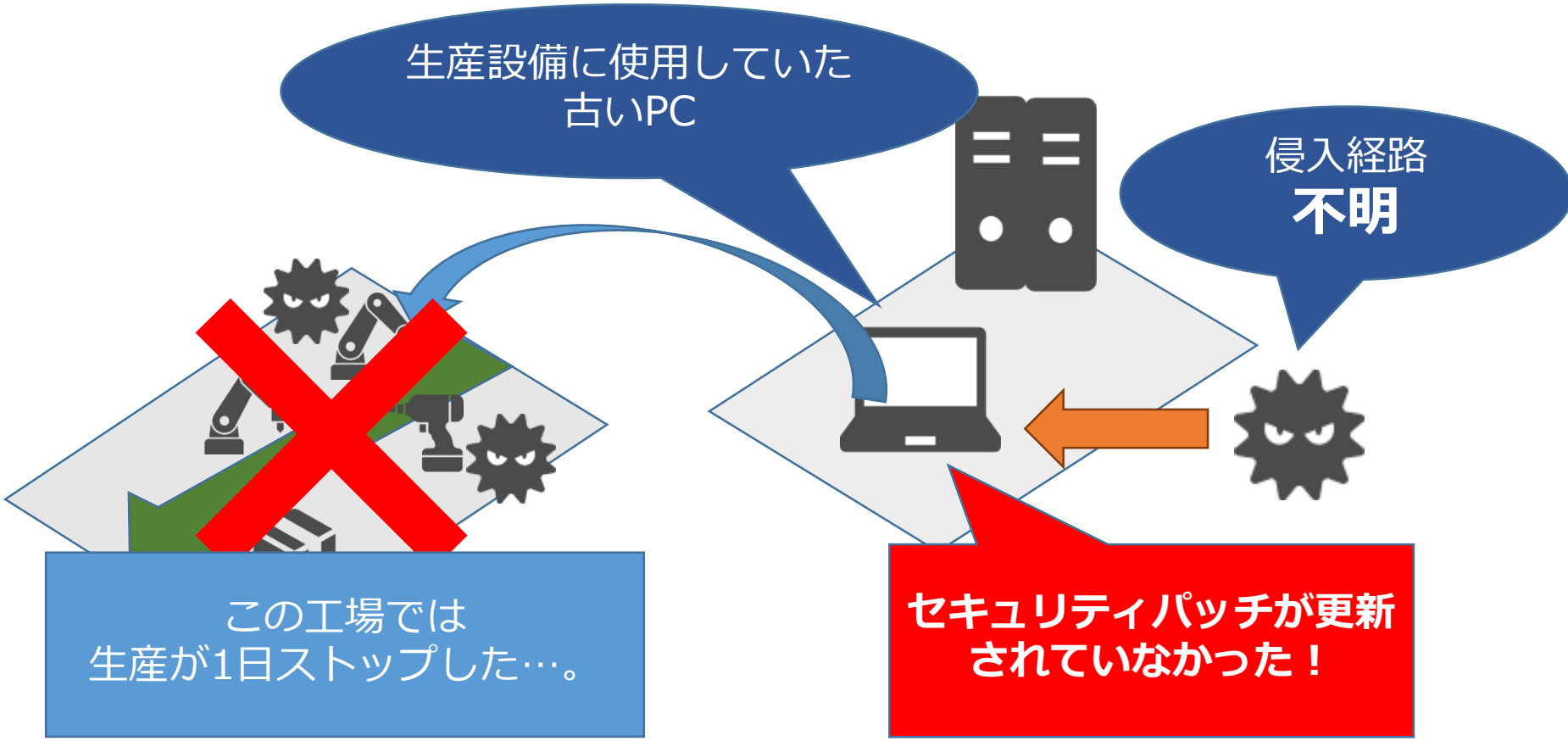
実際に被害にあった企業のニュース記事

引用元：https://www.sbbit.jp/article/cont1/40087

引用元：https://ascii.jp/limit/group/ida/elem/000/004/024/4024075/

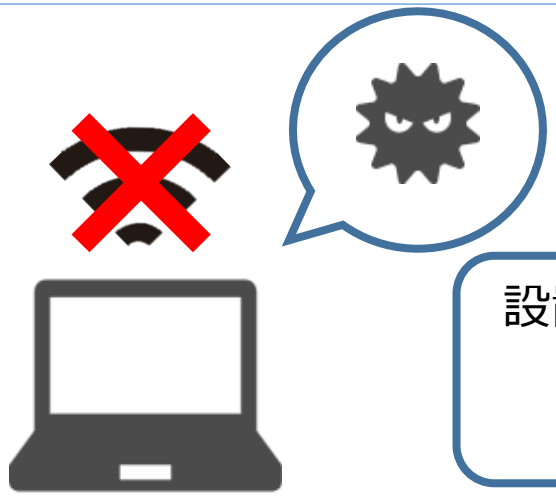
被害総額	
システム部門のトラブル対応コスト	感染台数×人件費
外部ウイルス解析会社への調査費用	ー
損失額	工場停止日数×1日の生産数×費用

実際のマルウェア被害　自動車工場を襲ったランサムウェア



**同様の理由で古いOSを利用していた企業や工場では
ランサムウェアの被害を受けていた。**

実際のマルウェア被害　海外の原子力発電所に潜んでいたマルウェア



設置時から更新等を行っていなかったオフライン端末
（核燃料棒を移動させる装置と連携したもの）
でマルウェアを発見

侵入経路は…

18台のDVD-RやUSBメモリなどの
リムーバブル・メディア上にもマルウェアが発見された。

引用元：https://wired.jp/2016/04/30/german-nuclear-plants-fuel-rod-system-swarming/

今、製造業に求められる対応

対応１

オフライン環境や生産インフラ環境にセキュリティホールを作らない

具体的な対応策がわからない。

対応２

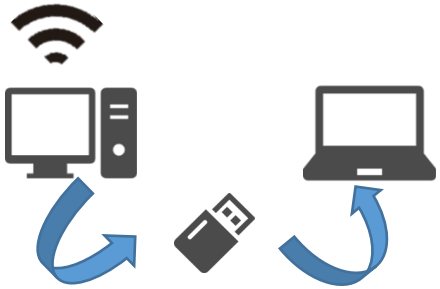
ITセキュリティの知見とOT（※）の両領域に精通する人材の育成

人材育成と言っても時間かかる。

※OT（Operational Technology）

＝ 製造業において工場のハードウェアを制御運用するための技術

製造業のセキュリティ課題と対応策



①生産記録やログ情報の
やり取りをUSBで行っている

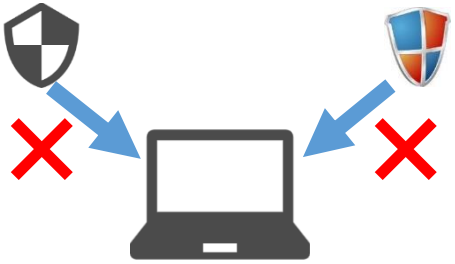
別端末に指す前に
USBのチェックを行う必要がある

②生産ラインはオフライン
のため、脅威対策をしていない

オフライン状態でも
最新のマルウェアを止める対策
を検討する必要がある

③制御用ソフトウェアが
新OSに対応していないため、
レガシーOSを使用

レガシーOS対応のマルウェア対策
製品での対策が必要

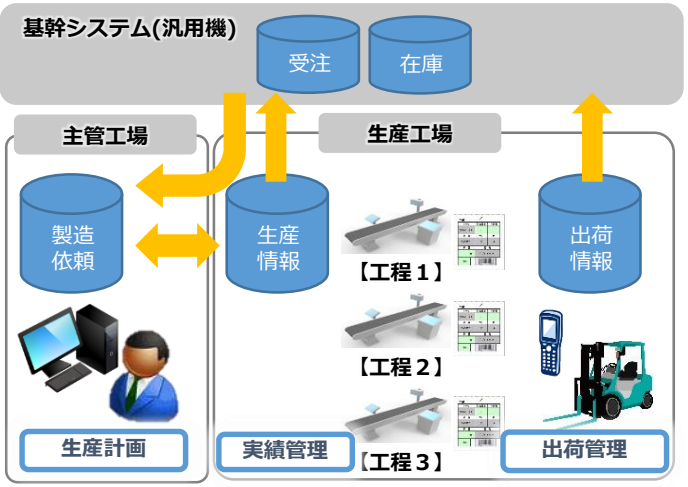


④Linuxに導入できる
脅威対策がない

Linux対応のマルウェア対策製品
での対策が必要

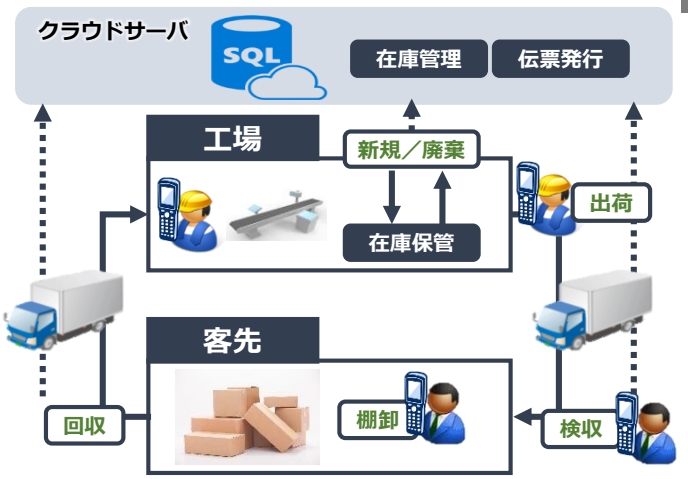
当社メトロのOTに関するノウハウ

工場移管に伴う生産管理システム構築



製品の生産工場移管に伴う生産計画～出荷に至るシステムを構築。新ライン、新運用に沿った計画、生産、出荷業務の効率化。

RFIDを活用した在庫管理改善



工場と客先にある在庫の管理を実現するRFIDを活用したシステムを提案。タイムリーに管理できなかった在庫管理を改善し、リードタイムの削減を実施。

工場セキュリティに関する考慮

Ⅰ.セキュリティソフトを導入できない機器への保護
Ⅱ.どのタイミングでセキュリティ対策を行うか
Ⅲ.ソフトウェアのサポート切れのリスクからどう守るか
Ⅳ.脆弱性の対策をどのように行うか

メトロのIT知見とOT知見で工場を守る

OTの知見
・目的：生産性の維持/向上
・生産管理の知識と経験

1973年～
制御システム開発事業

ITSecurityの知見
・目的：情報の活用/保護
・セキュリティ知識と経験

1990年～
情報セキュリティ事業

製造業様向け
メトロ脅威対策サービス


技術と感動をつなぐ
Metro