制御システムにおけるリモート接続の課題と求められる機能

制御システムセキュリティカンファレンス

Claroty Ltd. Solution Engineer
加藤　俊介

1. リモート接続の現状とメリット
2. リモート接続を取り巻く脅威
3. 各規格・規制における要求事項
4. 求められる機能
5. 導入事例

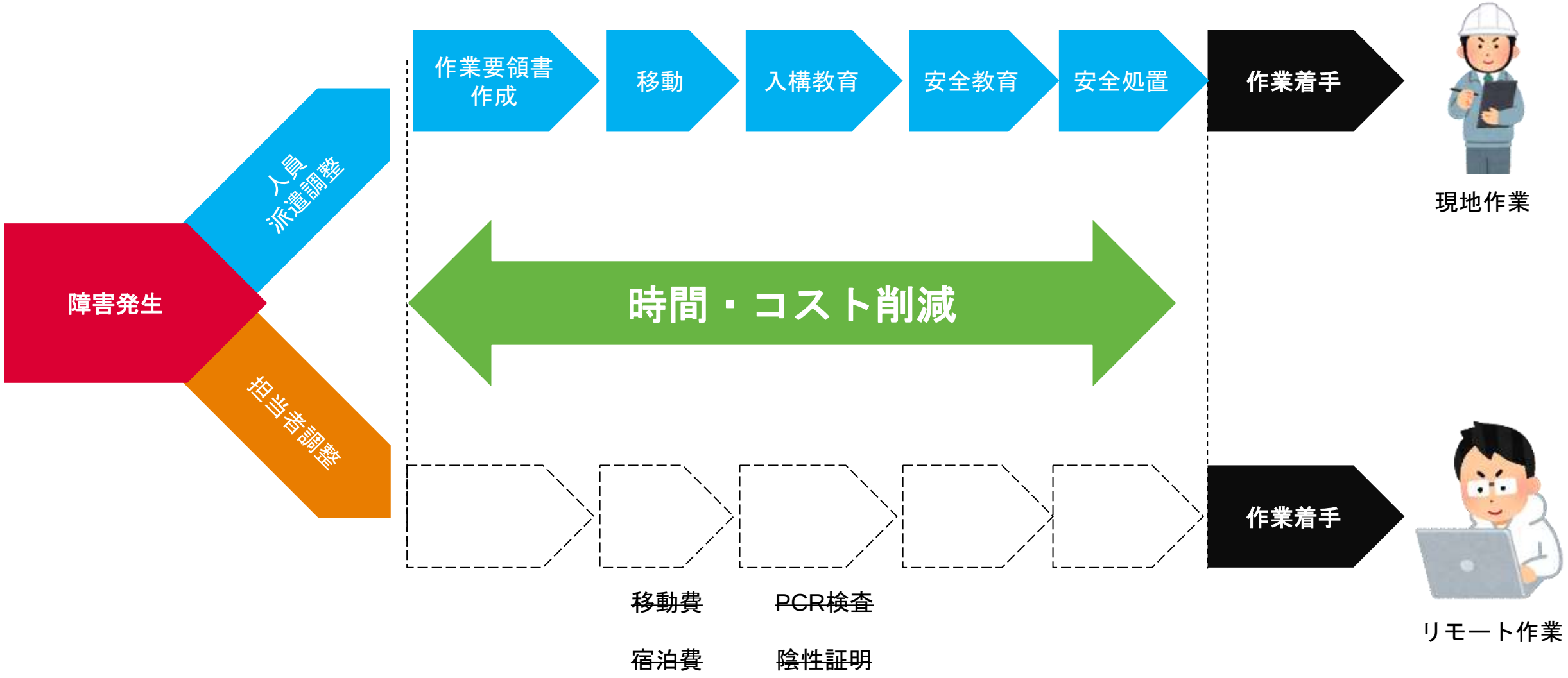
1. リモート接続の現状とメリット

制御システムを取り巻く環境 - 製造業全体での人手不足

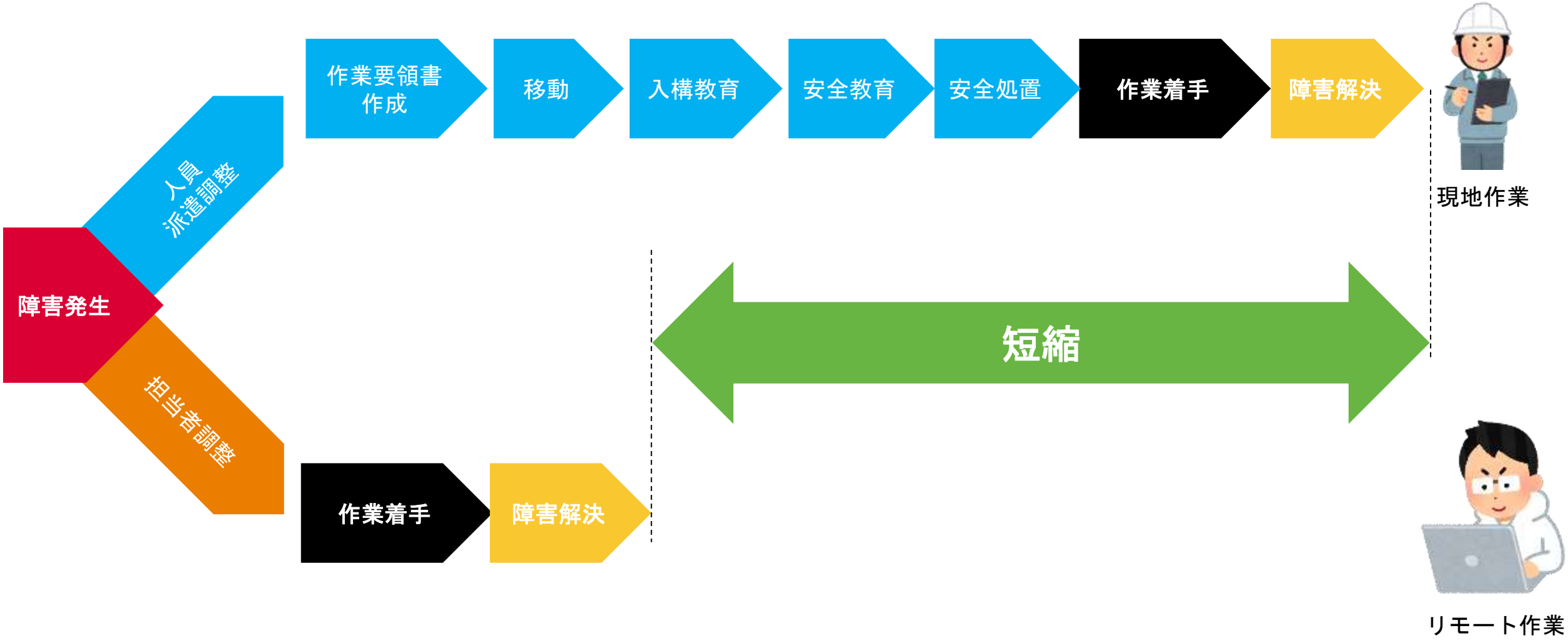
少ない人手で効率的・生産的な制御システム運用・保守が必要

引用元:
2022年版　ものづくり白書（令和３年度 ものづくり基盤技術の振興施策）「概要」
経済産業省「製造業における人手不足の現状および外国人材の活用について」

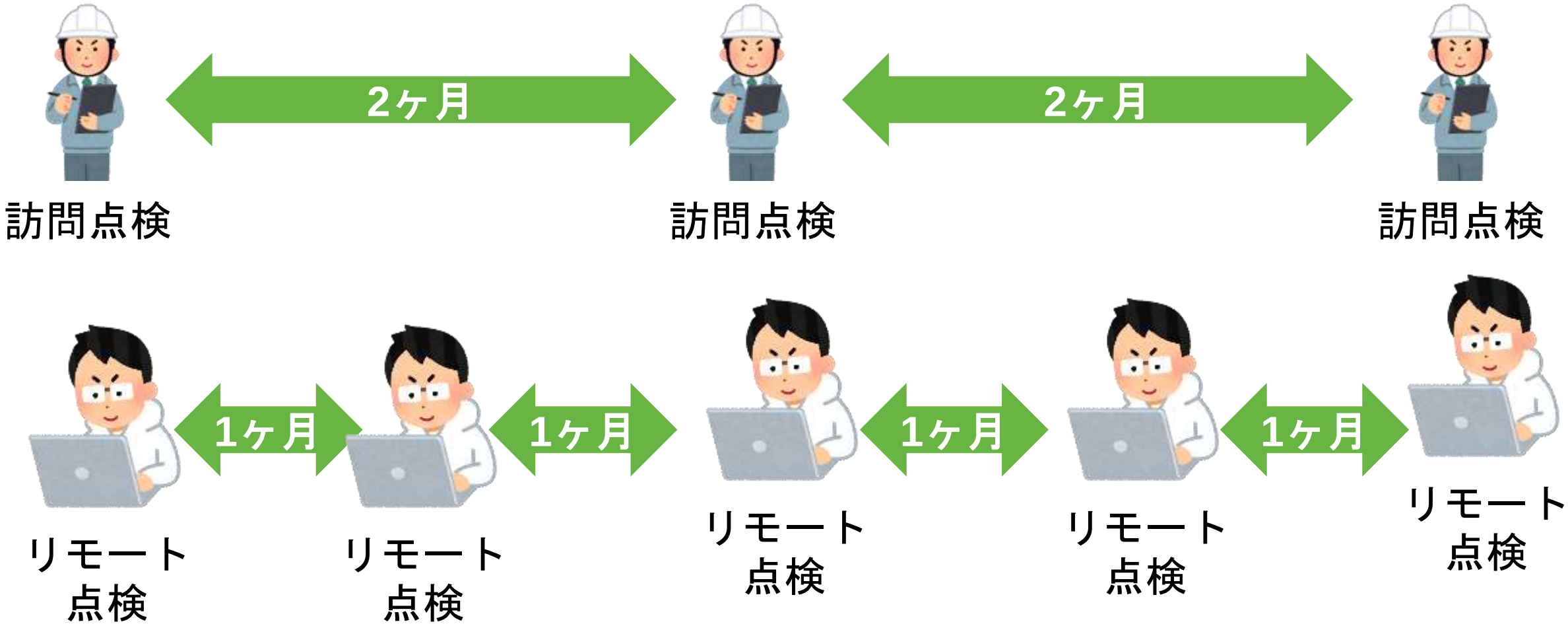
リモート接続による運用メリット - 時間・コスト削減



リモート接続による運用メリット - MTTR短縮



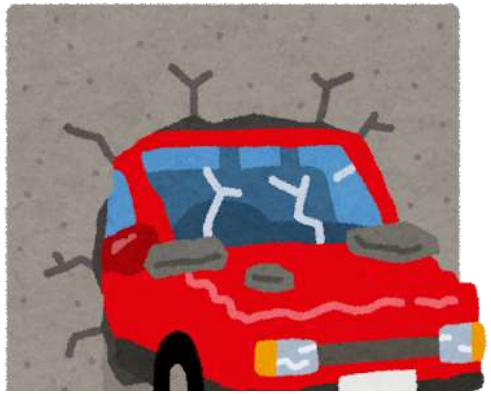
リモート接続による運用メリット - MTBF改善



リモート接続による運用メリット - その他

海外顧客の迅速なサポート

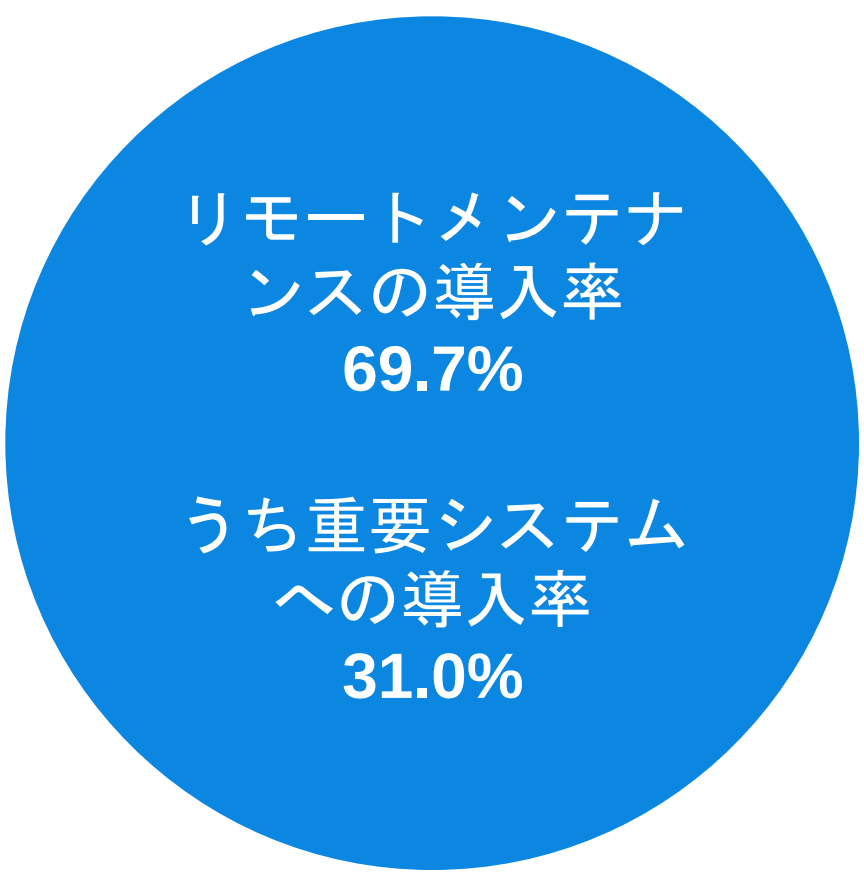
クラスター感染防止



移動リスク低減

柔軟な働き方への対応

リモート接続導入の実態とセキュリティ対策の実情



引用元:
株式会社情報通信総合研究所 次期行動計画の策定に向けた重要インフラ分野におけるIT環境変化及び実態調査報告書
独立行政法人情報処理推進機構　制御システムユーザ企業の実態調査報告書

2. リモート接続を取り巻く脅威

インシデント事例: 下水処理施設への侵入と下水流出

退職者がリモートアクセス経路を不正使用

↓

制御システムに
不正アクセス・不正操作

↓

下水が海洋に流出し、海洋系に多大な被害

退職者のアクセス権限削除忘れ

リモート接続検知機能の欠如

引用元: 制御システムセキュリティの脅威と対策の動向およびCSSCの研究概要について

インシデント事例: 2015年ウクライナ大規模停電

感染したPCを起点として制御システムへのリモート接続

↓

制御システム内のHMIを不正操作

↓

6時間にわたる広域大停電、22万5,000人に影響

認証機能の弱さによるなりすまし

単一障害点により被害波及

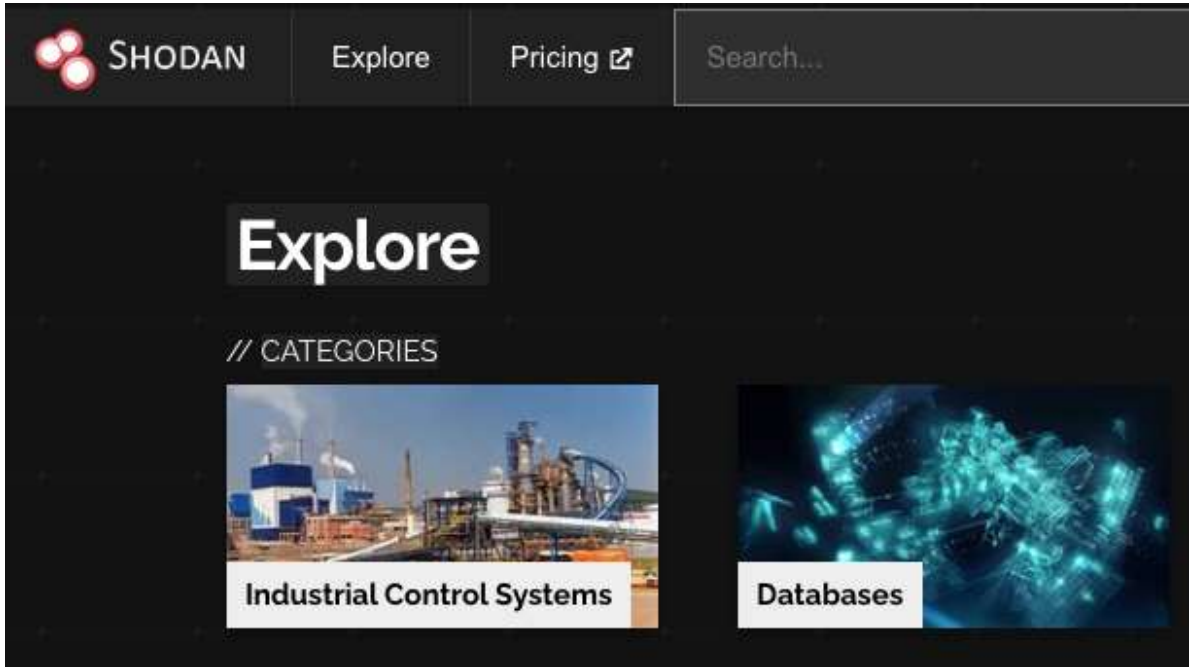
引用元: 制御システムのセキュリティリスク分析ガイド補足資料 制御システム関連のサイバーインシデント事例 1

セキュリティ10大脅威の一つはリモートアクセスからの侵入

10大脅威	2019年からの傾向
リムーバルメディアや外部機器経由のマルウェア感染	
インターネットやイントラネット経由のマルウェア感染	
ヒューマンエラーと妨害行為	
外部ネットワークやクラウドコンポーネントの攻撃	
ソーシャルエンジニアリングとフィッシング	
DoS/DDoS攻撃	
インターネットに接続された制御機器	
リモートアクセスからの侵入	
技術的な不具合と不可抗力	
スマートデバイスへの攻撃	

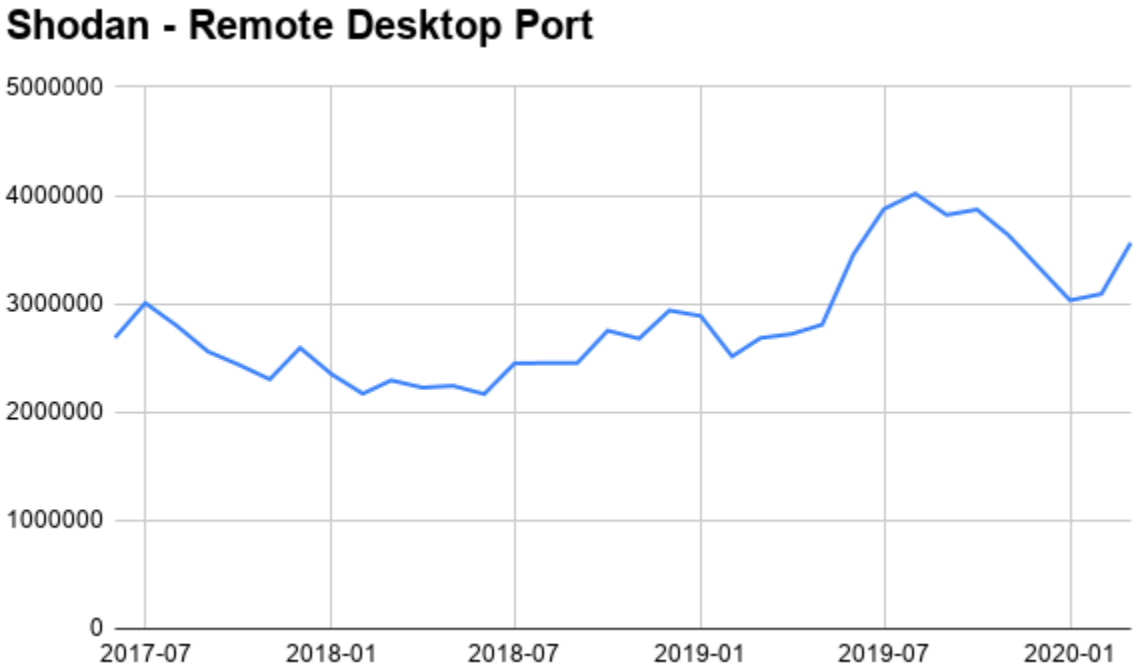
引用元: [ドイツBSI] 産業用制御システム（ICS）のセキュリティ -10大脅威と対策 2022-

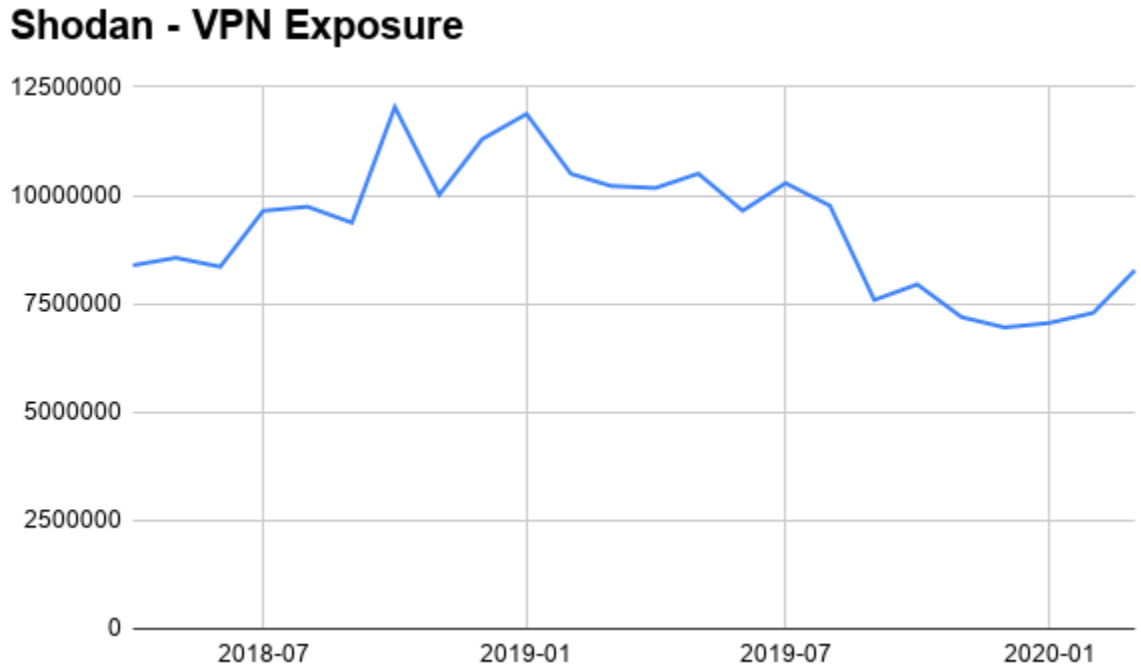
制御システムのインターネット露出は増えている



引用元: リモートワーク拡大に伴うRDPやVPNの使用状況、産業制御システムのネット接続状況の変化が調査で明らかに

リモート接続(RDP, VPN)の使用状況は増えている





引用元: リモートワーク拡大に伴うRDPやVPNの使用状況、産業制御システムのネット接続状況の変化が調査で明らかに

3. 各規格・規制における要求事項

国際規格 IEC62443 3-3 FR1 SR 1.13：識別と認証の制御

制御システムは、**信頼されないネットワーク経由の制御システムへのすべてのアクセス方法を監視し、制御する機能**を提供すること。

引用元: https://www.forescout.com/resources/how-to-effectively-implement-isa-99iec-62443/

NIST SP800-82 5.10.2: リモートアクセス

インターネットやダイアルアップモデムを介して接続するリモートサポート担当者は、一般的な企業ネットワークに接続するために、企業VPN接続クライアント、アプリケーションサーバー、または安全なHTTPアクセスを実行するなど、**暗号化プロトコルを使用し、**

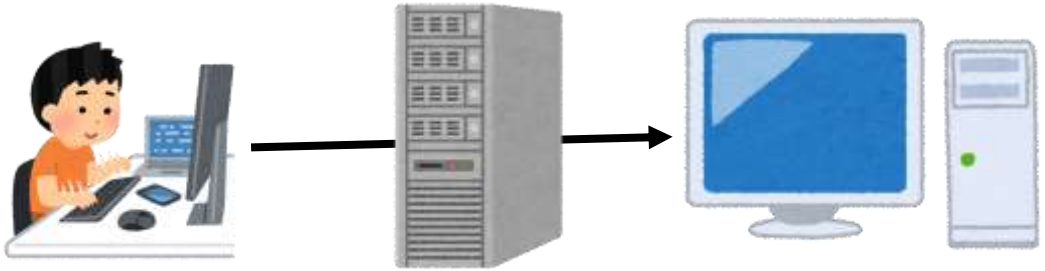
トークンベースの**多要素認証スキーム**などの強力なメカニズムを使用して認証する必要があります。

引用元: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

NIST SP800-82 5.10.2: リモートアクセス

一度接続したら、制御ネットワークにアクセスするために、トークン・ベースの多要素認証スキームなどの強力なメカニズムを使用して、**制御ネットワークのファイアウォールで2回目の認証**を要求する必要があります。

プロキシサーバーは、リモートサポートアクセスを保護するための追加機能を提供することも可能です。



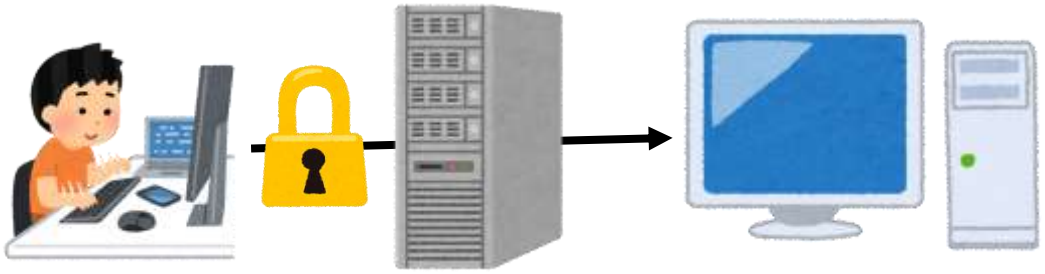
引用元: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

NERC CIP CIP-005 R2: リモートアクセス管理

双方向遠隔アクセスを開始したサイバー資産が該当するサイバー資産に**直接アクセス**しないように、**中間システム**を利用すること。

中間システムを単点とする暗号化を使用すること。

多要素認証を必要とすること。



引用元: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

NERC CIP CIP-005 R2: リモートアクセス管理

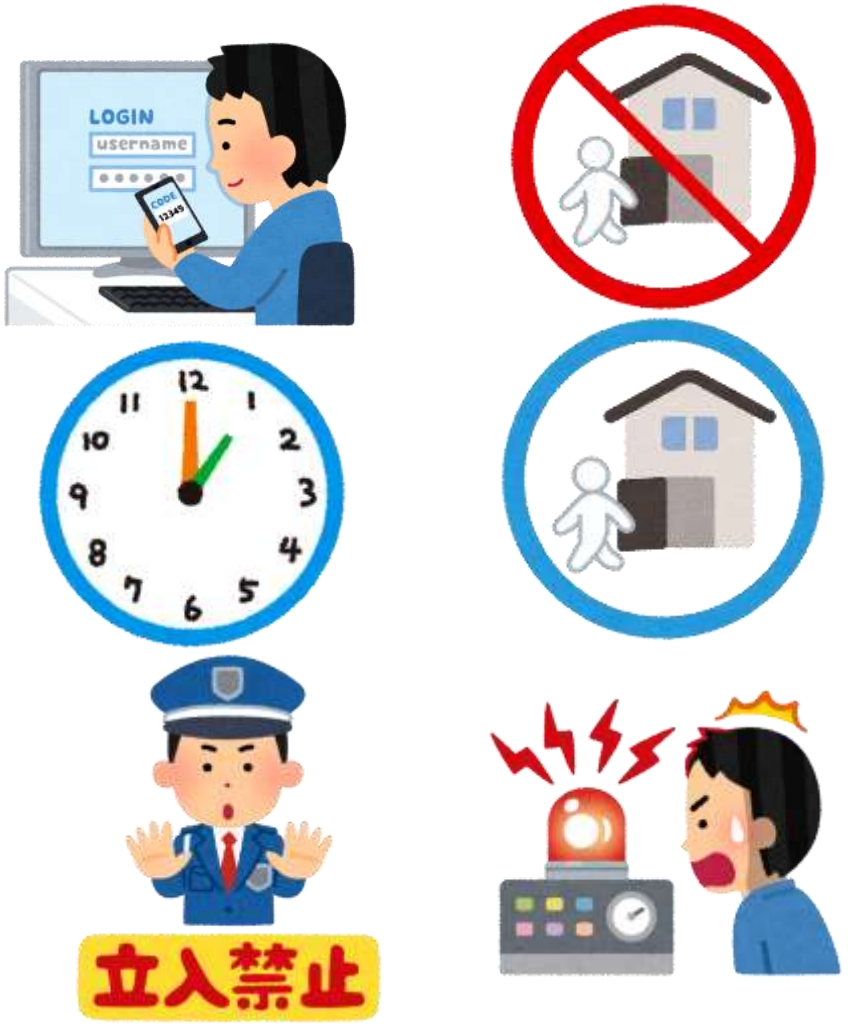
アクティブなリモートアクセスを**特定するための1つ以上の方法**を準備すること。

アクティブなリモートアクセス を**無効にする1つまたは複数の方法**を準備すること。

引用元: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

工場システムにおけるCPS対策ガイドライン Ver 1.0
付録E 3.2.2(1): システム構成面での対策

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。



引用元: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

4. 求められる機能

インシデント・規制から求められる機能

リモート
ユーザー

中間システム

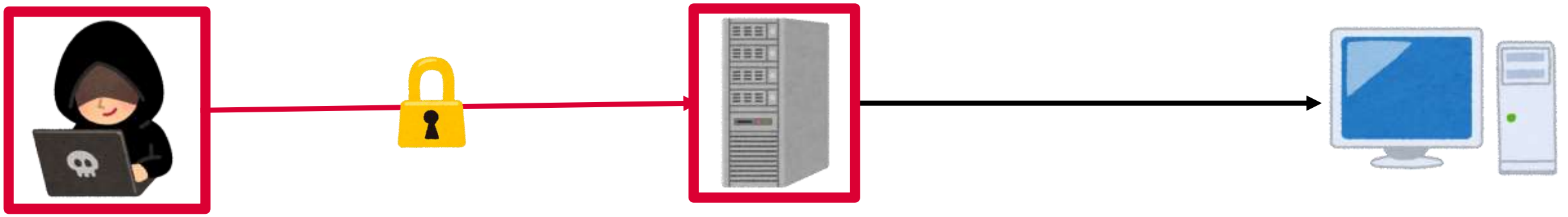
HMI, EWS

接続開始 → 暗号化通信確立 → ユーザー認証(多要素認証) → 対象端末へ接続開始 → 接続確立

管理者

グループ毎に端末接続制限
接続ユーザー特定、接続通知
セッション監視、遮断

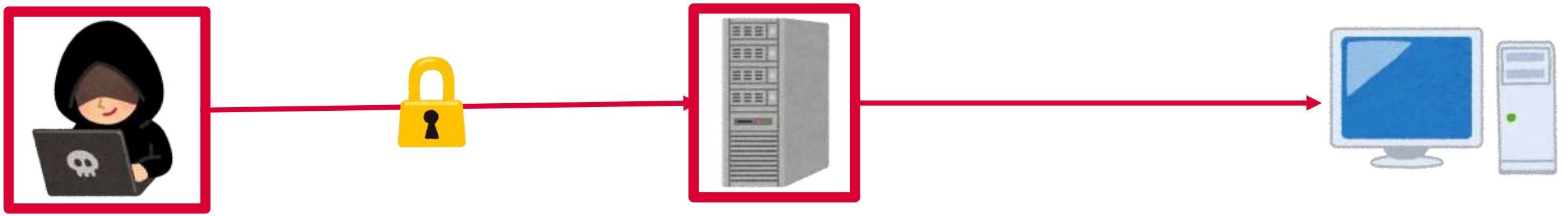
攻撃シナリオ1: なりすまし



接続開始 → 暗号化通信確立 → **ユーザー認証(多要素認証)** → 対象端末へ接続開始 → 接続確立

ユーザーID、パスワード認証が通っても他要素の認証ができず、アクセス不可

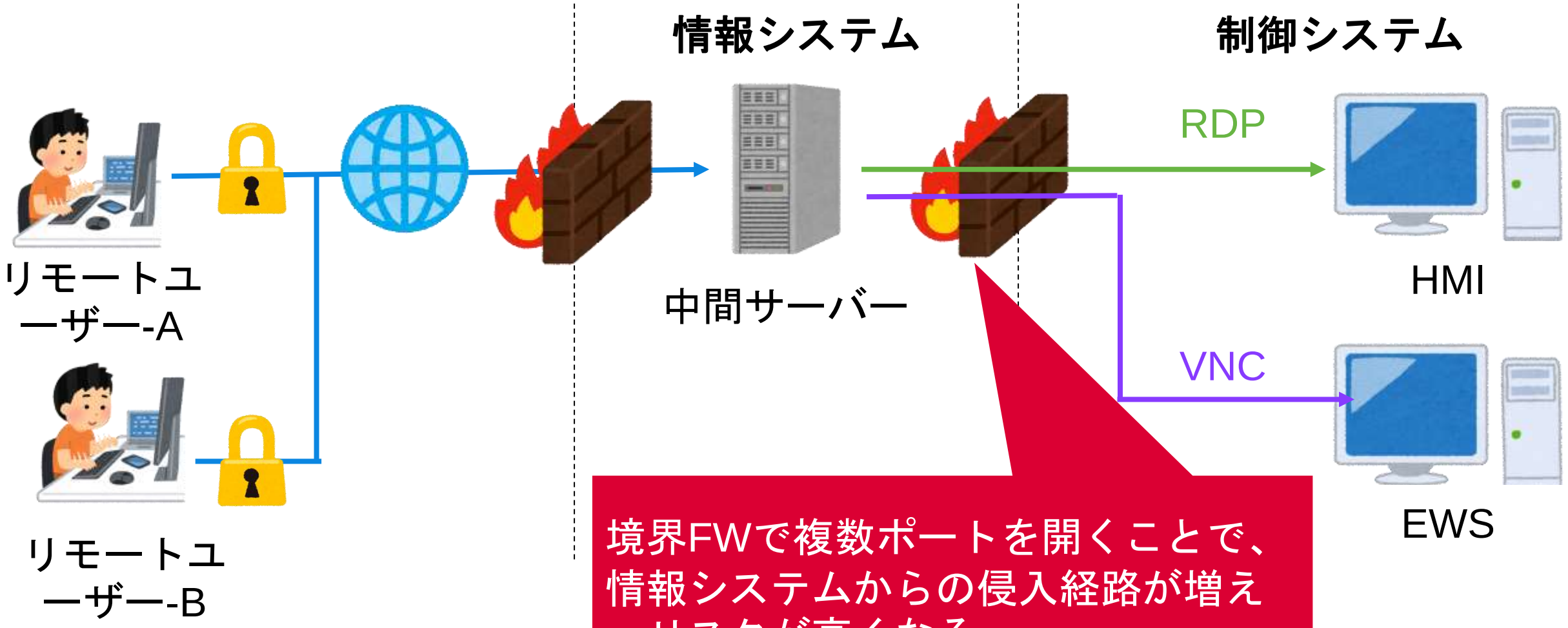
攻撃シナリオ1: 対象端末への不正アクセス



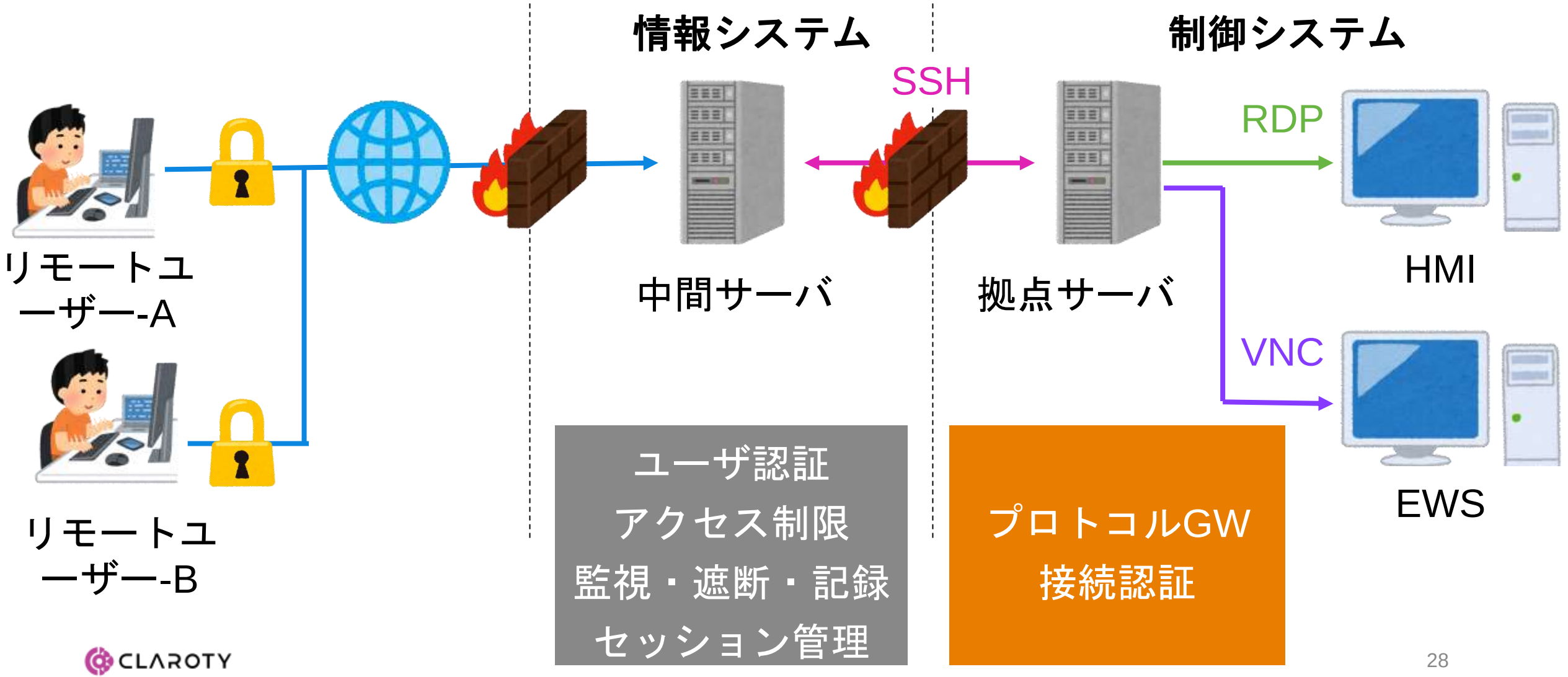
接続開始 → 暗号化通信確立 → ユーザー認証(多要素認証) → 対象端末へ接続開始 → 接続確立

管理者への接続通知
不正な接続のため接続遮断

運用の観点から求められる実装構成

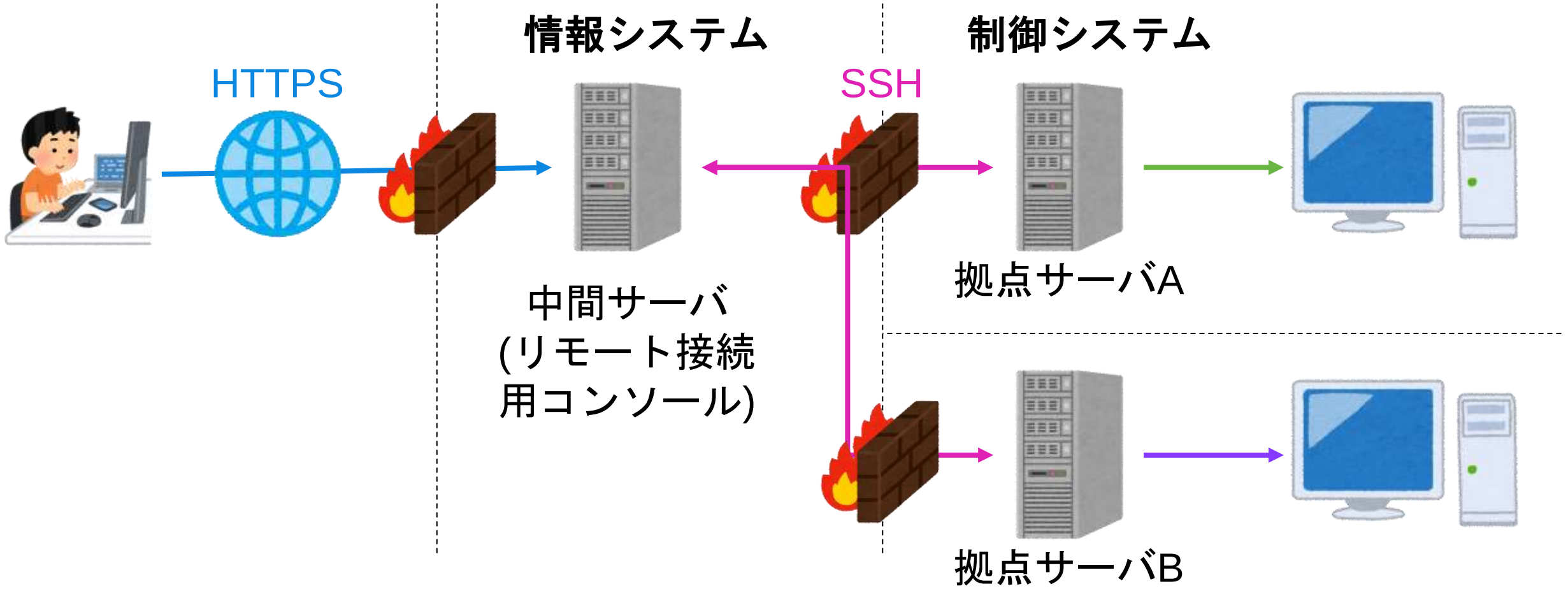


運用の観点から求められる実装構成



5. 導入事例

導入事例 - 実装構成



中間サーバーを経由させることで、全てのリモート接続セッションを集中監視

導入事例 - セキュリティ管理

認証
パスワードポリシーを設定
SAML認証連携
2段階認証

ユーザ管理
社内ユーザはAD連携
保守ベンダー毎にグループ化
ワンタイムユーザは期限付き

アクセス管理
グループ毎に端末制限
重要システムは管理者による承認
接続可能時間の設定

監査
通知・リアルタイム監視・遮断
セッション情報を表示、録画
全てのログはsyslogで保存

導入事例 - セキュリティ管理

~~正規ユーザーへのなりすまし~~	2段階認証により防止
~~権限悪用, 横移動~~	最小権限設定
~~不正な接続~~	接続通知による異常接続を検知
~~不正な操作~~	リアルタイム監視・遮断

導入事例 - 導入による効果

OT担当者の視点

- 人員の最適化
- 遠隔地の早期メンテナンス
- 出張旅費削減

セキュリティ担当者の視点

- リスク軽減
- ゼロトラスト管理
- リモートインシデント対応

まとめ

1. 制御システムに対するリモート接続は、生産性・可用性向上のために必要である。

1. 一方でリモート接続起因でのインシデント、脅威は高まっている。

1. 利用するに当たっては、認証、ユーザ管理、アクセス管理、監査の4つのセキュリティ管理を実装が求められる。

1. セキュリティ管理された接続性が確立されれば、リモート接続によるメンテナンス作業などは生産性・可用性向上に寄与すると考えられる。