HITACHI
Inspire the Next

JP1/IT Desktop Management 2 - Manager による生産現場の資産管理

1. JP1/IT Desktop Management 2 - Managerのご紹介
2. 登録事例
   - JP1/IT Desktop Management 2 - Managerによる Edgecross基本ソフトウェアの管理 -

2021年2月

株式会社 日立製作所

HITACHI
Inspire the Next

1. JP1/IT Desktop Management 2 - Managerのご紹介

1−1. 産業、制御システムの資産管理の課題

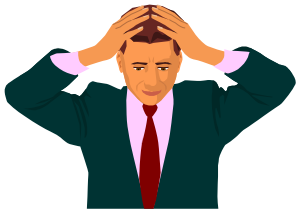
HITACHI
Inspire the Next

標準規格・ガイドラインへの遵守

- EUでは重要インフラ製品セキュリティに関する要件を決定し、2023年までに義務化
- 国内でも総務省がIoT機器セキュリティ技術の基準化を計画しており、**制御システムに対するセキュリティ基準である IEC62443**をベースに、セキュリティ要件に準拠していくことが求められる

	制御システム
組織	ISO 31000（リスクマネジメント ISO 22320（危機管理） ISO 22301（事業継続）
システム	NIST SP 800-82 / IEC 62443 / ISA Secure
装置	IEC 62443 / ISA Secure SSA・EDSA
要素技術	ISO/IEC 29192（軽量暗号）

現場課題



現場には多数の課題が…

工場内・システムにたくさんの装置が存在
資産を把握しきれない

セキュリティ上脆弱な端末の存在
ウイルス感染などのリスク

個人のUSBメモリーやPCの持ち込み
情報漏えいのリスク

JP1/ITDM2 - Managerで解決！

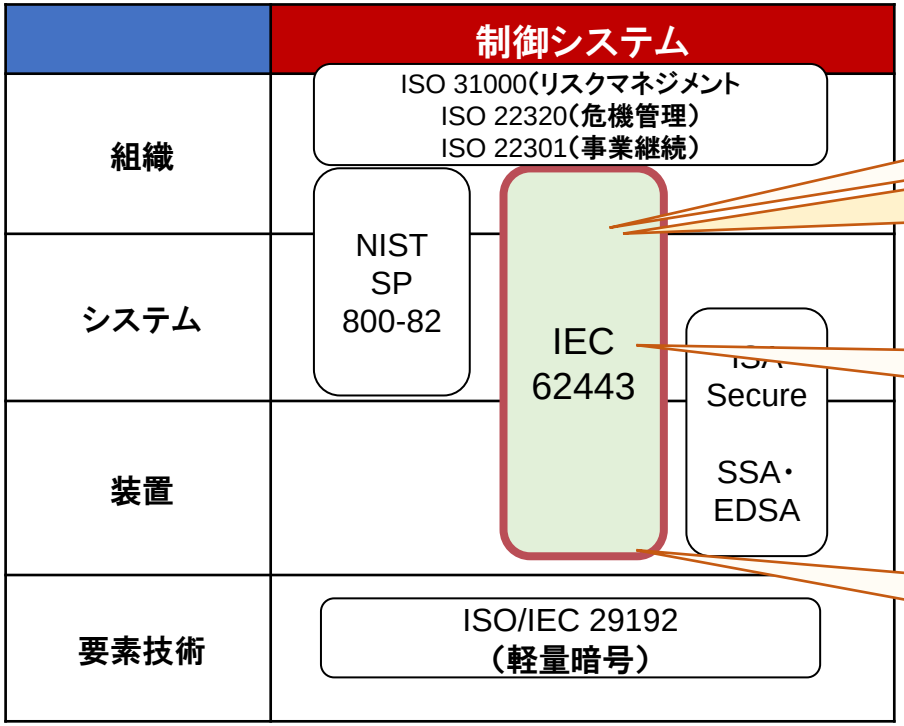
1－2. 制御システムのセキュリティ規格/ガイドライン

HITACHI
Inspire the Next

Point

制御システムをとりまく状況をふまえ、
制御システムに関するセキュリティ規格/ガイドラインが制定されています。

- EUでは重要インフラ製品セキュリティに関する要件を決定し、2023年までに義務化。
- 国内でも総務省がIoT機器セキュリティ技術の基準化を計画しており、制御システムに対するセキュリティ基準であるIEC62443(2013年制定)をベースに、セキュリティ要件に準拠していくことを推奨している。
- IEC62443はPart1からPart4まで分かれ、事業者/立場によって求められる内容が異なる



IEC62443-1
関係者全員が読むべき用語解説、制御システムのセキュリティ動向等が記載されている。

IEC62443-2
工場や設備のオーナーに求められる要件。
マネジメントやセキュリティポリシーの作成、運用など、セキュリティ維持に必要な活動を定義している。

IEC62443-3
複数の機能や製品を組み合わせて運用している制御システムを対象とした規格。

IEC62443-4
制御システムの一部であるデバイスを対象とする規格。

1－3. JP1/ITDM2を使用した資産管理

HITACHI
Inspire the Next

現場課題の解決

- システム内の機器をすべて把握する
- OSとセキュリティソフトを常に最新に保つ
- 未許可PC/USBメモリの接続/使用を制限する

❶ システム内の機器の把握・棚卸

PC・サーバなど**機器の情報を収集し棚卸**します。
・ハードウェア情報(メモリ、CPU)
・ソフトウェア情報、パッチ情報　　など

❷ セキュリティ対策状況のチェックと対策実施

各サーバ/PCの**セキュリティ対策状況をチェックし対策**します。
・古いバージョンのソフトウェアはないか
・Windowsの更新プログラムは最新か
・セキュリティソフト(ウィルス対策製品)が最新か　　など

❸ 未許可PC/USBメモリの制限

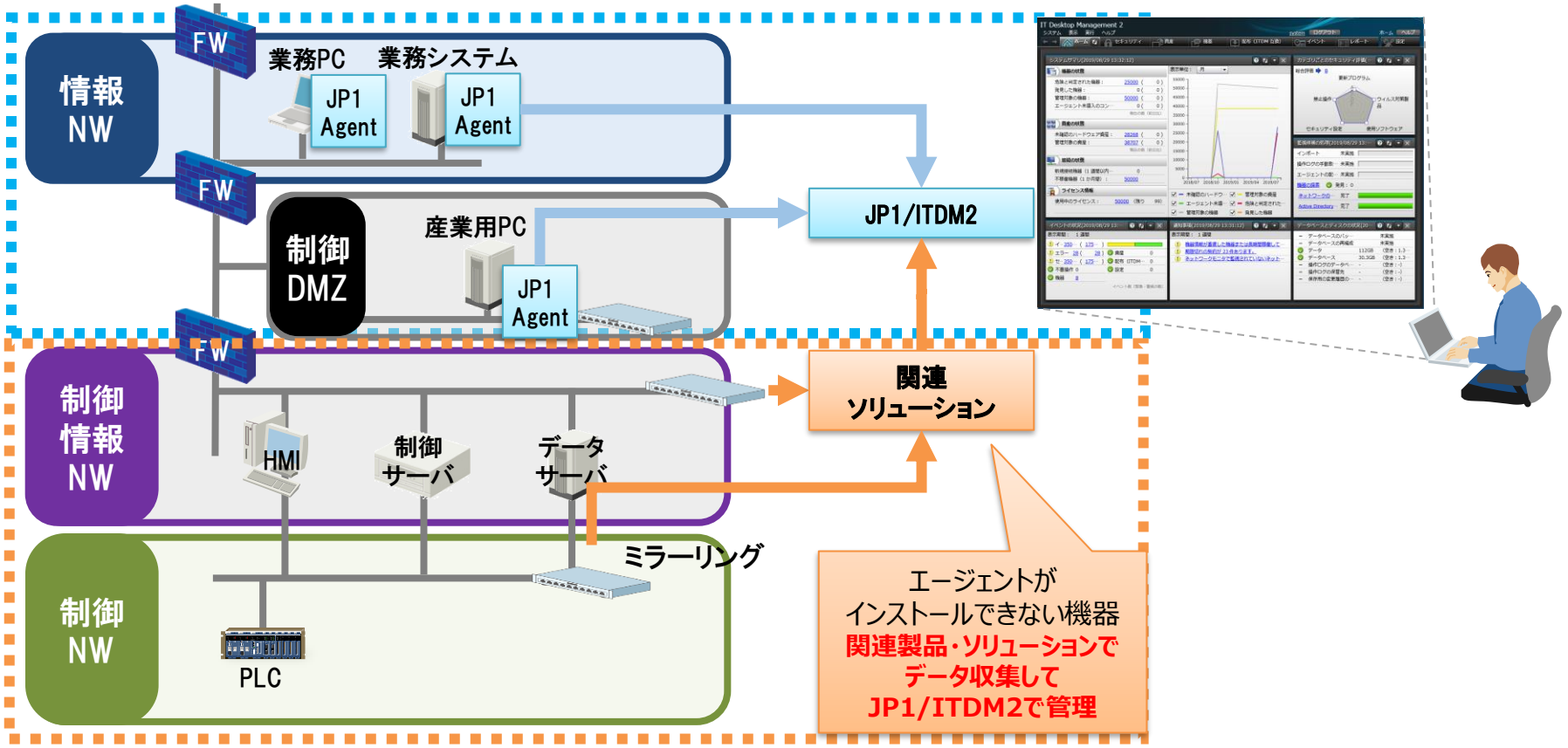
未許可PCやUSBメモリの**接続や使用を制限**します。
・未許可PCのネットワークからの排除
・未許可USBメモリの使用制限　　など

1－4. システム内の機器の把握

HITACHI
Inspire the Next

システム内の機器を漏れなく管理

産業用PCなどシステム内の機器の情報を収集し、一元管理することができます。
JP1/ITDM2のエージェントが導入できない機器(PLCなど)も、関連ソリューション※と連携することで、漏れなく管理できます。



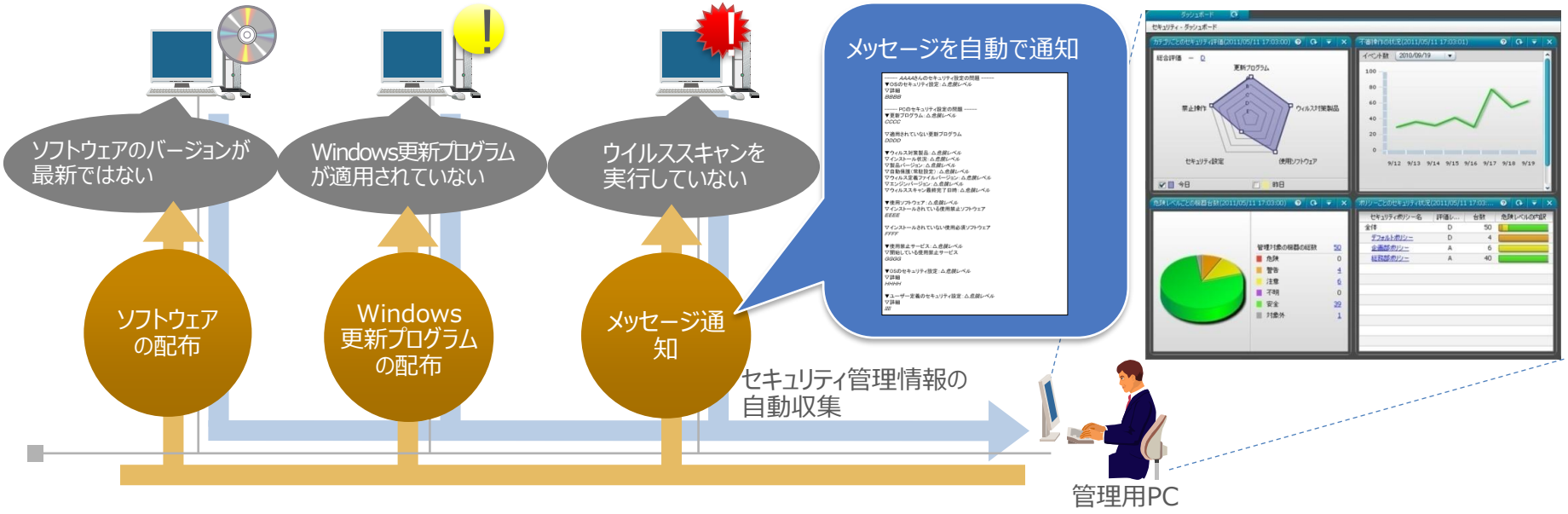
※ 日立エージェントレス資産管理ソリューション

1－6. セキュリティ対策状況のチェックと対策実施

HITACHI
Inspire the Next

セキュリティの問題点を把握し、すばやく対策

管理している機器からセキュリティに関連した情報を収集し、社内のセキュリティ状況をリアルタイムでチェック。摘出された問題点についても自動で対策することで、システムのセキュリティレベル維持・向上をサポート。



セキュリティポリシーとは

セキュリティポリシーとは、組織の情報セキュリティに関する方針です。
セキュリティポリシーを設定し、管理対象のＰＣに適用することで、定期的にセキュリティ状態が適切かチェック(セキュリティ判定※1)できます。
加えて、セキュリティの判定結果にもとづいた対処を自動で行う(自動対策※2)ことによりセキュリティ問題に対する対策が可能です。
初期設定されているデフォルトポリシーには一般的に必要な項目があらかじめ設定されているので、すぐに管理が始められます。
部署単位やＰＣごとに適用するセキュリティポリシーを変更することもできます。

1－7. 未許可PC/USBメモリーの制限（USBメモリー）

HITACHI
Inspire the Next

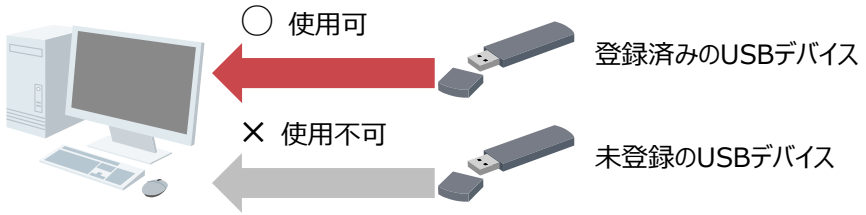
個人持ち込みのUSBメモリーを使わせない

■USBメモリーすべてを使用禁止にする、あるいは、登録済みのUSBメモリーだけ使用を許可することができます。
登録済みのUSBメモリーの使用許可は部署単位、設置場所単位、機器単位で制限することもできます。
使用を許可していないUSBメモリーがPCに接続されたら、管理者側で把握できます。

■使用を許可するUSBメモリーは、一覧で確認して設定を変更することで、すぐに使えるようになります。
社内で許可したUSBメモリーしか使えないように制限して、ウイルス感染や情報漏えいのリスクを低減できます。

セキュリティポリシーの設定例

- ■USBデバイスの読み書きを禁止
- ■登録済みのUSBデバイスは許可
- ■登録済みのUSBデバイスを、部署などの条件付きで許可



セキュリティポリシーをコピーすることでオフラインPCでも利用可能です

＜使用抑止できるデバイス*＞

USB
- •USB接続のCD/DVDドライブ
- •USB接続のFDドライブ
- •USB接続のHDD
- •USB接続のフラッシュメモリー
- •(USB接続のカードリーダ等)

WPD
- ・Windows ポータブルデバイス(スマートフォン/デジカメ/メディアプレイヤー等)

内蔵CD/DVD
- •内蔵CD/DVDドライブ

内蔵FD
- •内蔵FDドライブ

Bluetooth
- ・USB接続のBluetoothデバイス

イメージングデバイス
- ・USB接続のイメージングデバイス(Webカメラ/スキャナ等)

内蔵SDカード
- •内蔵SDリーダ

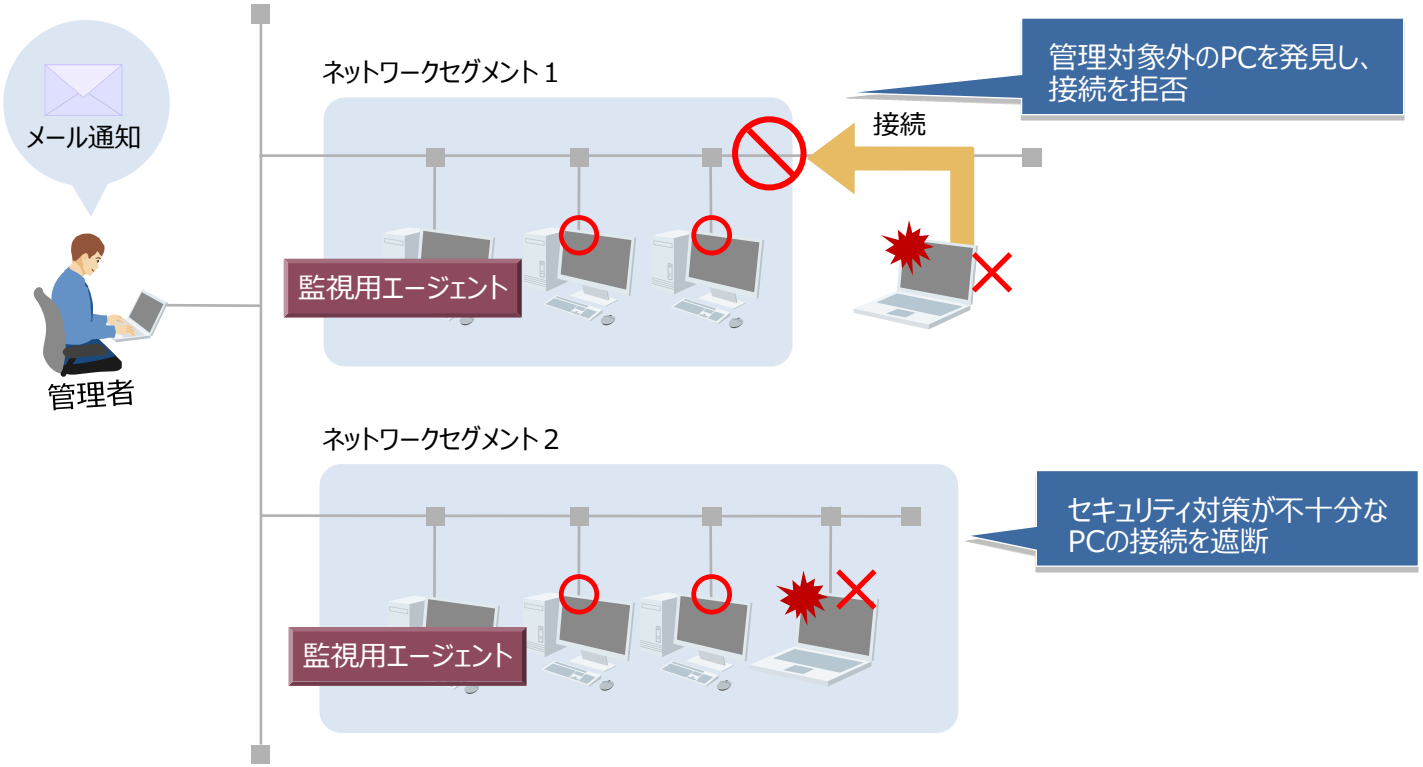
IEEE1394
- •IEEE1394接続のHDD

1－8. 未許可PC/USBメモリーの制限（ネットワーク制御）

HITACHI
Inspire the Next

個人持ち込みの機器をネットワークにつながせない

ネットワーク監視用のエージェントを導入したネットワークセグメントに、管理対象外のPCを接続しようとすると、新しい機器として検知してネットワーク接続を拒否できます。また、セキュリティポリシーで安全でないと判定されたPCがある場合は、ネットワークへの接続を自動的に遮断できます。さらに、ネットワーク接続を拒否・遮断したことをメールで通知することもできます。



HITACHI
Inspire the Next

2.登録事例
- JP1/IT Desktop Management 2 - Managerによる Edgecross基本ソフトウェアの管理 -

2－1. はじめに

HITACHI
Inspire the Next

生産現場でのデータ収集のため、Edgecross 基本ソフトウェアを導入しているシステムは多数存在しますが、導入した時期によりバージョンがバラバラになっているケースも多く見られます。

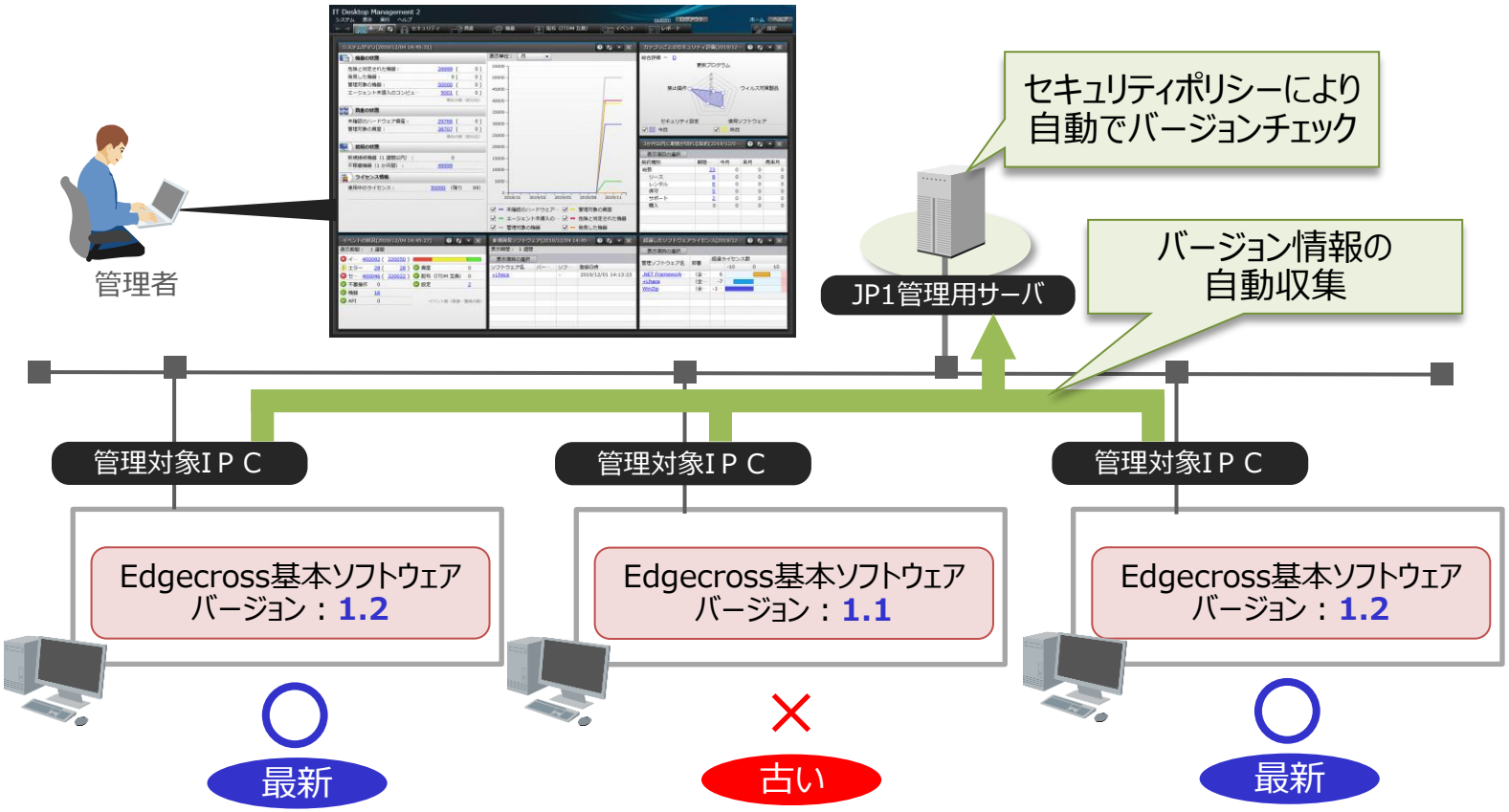
システムのセキュリティを保つ上では、常にEdgecross基本ソフトウェアを最新に保つ必要があります(セキュリティガイドライン 概要編 「4.1 脆弱性対策」)が、大規模なシステムでは、そのバージョン管理も管理者の負担となります。

しかし、JP1/ITDM2を活用することにより、**Edgecross 基本ソフトウェアのバージョン管理を一元的に行い、管理者の負担を低減することができます。**

本章では、JP1/ITDM2により、Edgecross 基本ソフトウェアのバージョン管理を行うためのシステム構築方法や設定例について示します。

2－2. Edgecross 基本ソフトウェアのバージョン管理

JP1/ITDM2では、システム内に導入されたEdgecross 基本ソフトウェアのバージョン情報を収集し、あらかじめ設定したセキュリティポリシーにより、自動的に最新バージョンが導入されているかをチェックすることができます。



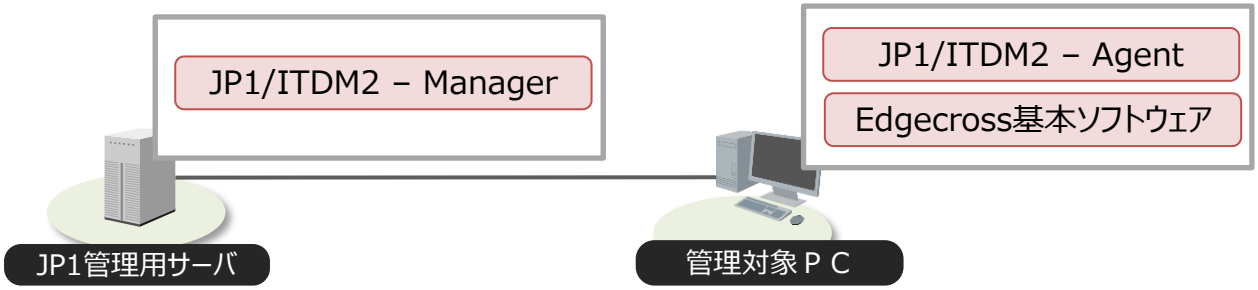
2－3. システム構成例

HITACHI
Inspire the Next

システム構成例を以下に示します。

◆JP1管理用サーバ
OS：Windows Serer 2019　Datacenter Edition
ソフトウェア：JP1/ITDM2 – Manager　12-10

◆管理対象PC
OS：Windows 10 Enterprise
ソフトウェア：JP1/ITDM2 – Agent 12-10
Edgecross基本ソフトウェア 1.22



2－4. インストール・セットアップ手順

HITACHI
Inspire the Next

◆インストール・セットアップ手順
各ソフトウェアのインストール・セットアップ手順は以下のURLを参照してください。

・JP1/ITDM2 – Managerのインストール・セットアップ
http://itdoc.hitachi.co.jp/manuals/3021/30213E1320/DMSK0010.HTM

・JP1/ITDM2 - Agentのインストール・セットアップ
http://itdoc.hitachi.co.jp/manuals/3021/30213E1320/DMSK0028.HTM

・Edgecross基本ソフトウェアのインストール
https://www.marketplace.edgecross.org/file-download?filePath=AQKD3OuYWJuCoRl3%2FOpL2kCC5fZe7qzxLStweg43Bdc%3D&fileName=ECD-MA1-0002-02-JA.pdf&functionId=M01

2－5. 設定例

JP1/ITDM2のセキュリティポリシーを設定し、Edgecross基本ソフトウェアのバージョンが最新かをチェックします。

① Edgecrossコンソーシアムの Webページを開き、Edgecross基本ソフトウェアの最新バージョンを確認します。

②JP1/ITDM2のセキュリティポリシーを編集し、使用必須ソフトウェアにEdgecross基本ソフトウェアを設定します。
ソフトウェア名： Edgecross基本ソフトウェア
バージョン：1.22 (①で確認したバージョン)
http://itdoc.hitachi.co.jp/manuals/3021/30213E1420/DMUY0291.HTM

③JP1/ITDM2で各PCにインストールされているEdgecross基本ソフトウェアが最新かどうかを確認できます。
http://itdoc.hitachi.co.jp/manuals/3021/30213E1420/DMUY0287.HTM

付録

製品略称一覧
商品名、商標等の引用に関する表示

製品略称一覧

略称	正式名称
JP1/ITDM2 - Manager	JP1/IT Desktop Management 2 - Manager

商品名、商標等の引用に関する表示

HITACHI
Inspire the Next

自社商品名の引用に関する表示
• HITACHI、JP1は、株式会社 日立製作所の商標または登録商標です。

他社商品名、商標などの引用に関する表示
• Windows、および Windows Server は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
• その他記載の会社名、製品名などは、それぞれの会社の商標もしくは登録商標です。


HITACHI
Inspire the Next