HITACHI

株式会社 日立システムズ

平時に対応すべきこと、有事対応で重要なこととは？

日立システムズフェア2025

グローバル＆セキュリティサービス事業グループセキュリティサービス事業部セキュリティサービス本部ＭＳＳ推進第一部

杉本 智

Contents

HITACHI

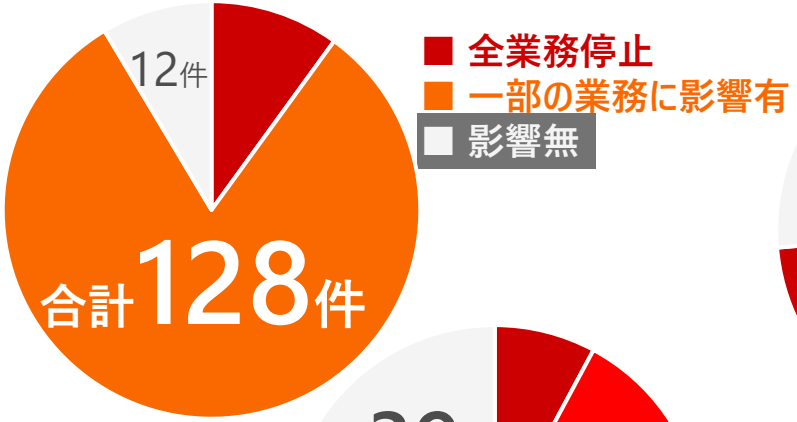
ランサムウェア攻撃の脅威が深刻化しており、業務停止や金銭的損害などの被害が報告されている

情報セキュリティ10大脅威 2025

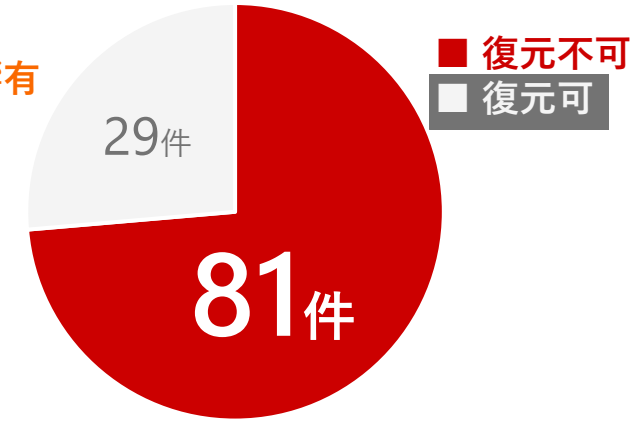
順位	「組織」向け脅威
1	ランサム攻撃による被害
2	サプライチェーンや委託先を狙った攻撃
3	システムのぜい弱性を突いた攻撃
4	内部不正による情報漏えい等
5	機密情報等を狙った標的型攻撃
6	リモートワーク等の環境や仕組みを狙った攻撃
7	地政学的リスクに起因するサイバー攻撃
8	分散型サービス妨害攻撃（DDoS攻撃）
9	ビジネスメール詐欺
10	不注意による情報漏えい等

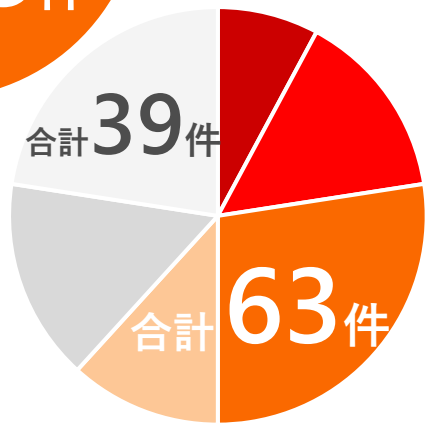
出典：IPA 「情報セキュリティ10大脅威 2025」を日立システムズにて加工
（https://www.ipa.go.jp/security/10threats/10threats2025.html）

ランサムウェア被害が
業務に与えた影響の程度



バックアップからの
復元結果





復旧等に要した調査費用の総額

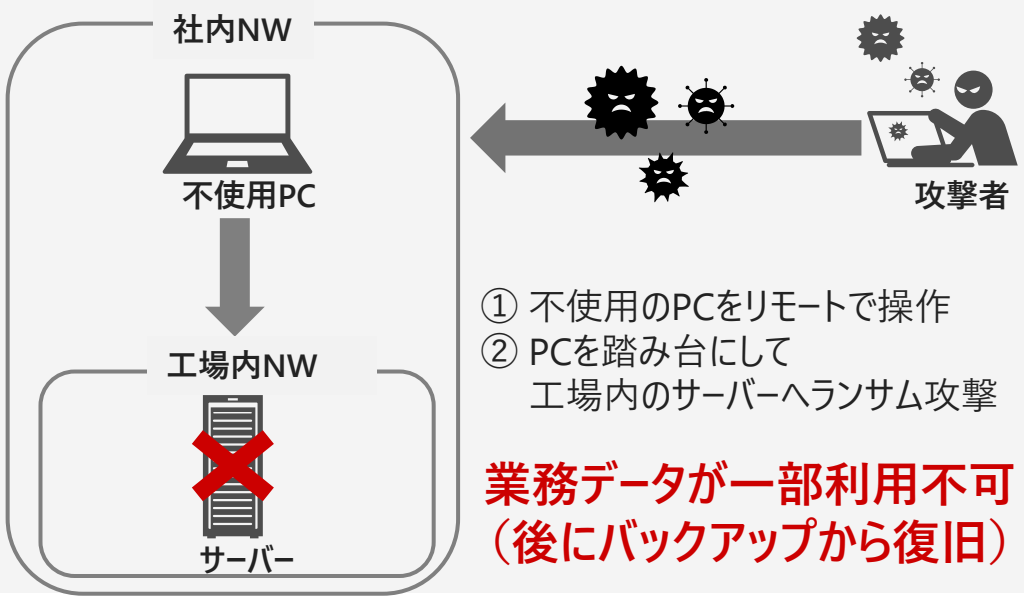
出典：警察庁「令和6年におけるサイバー空間をめぐる脅威の情勢等について」を日立システムズにて加工
（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf）

HITACHI

サイバー攻撃はぜい弱性・設定不備のある機器を媒介に、より重要なIT資産へ被害が拡大する

A社（製造業）

原因　：不使用PCの未管理
　　外部からのリモート操作可否
　　不要なサーバーへのアクセス許可

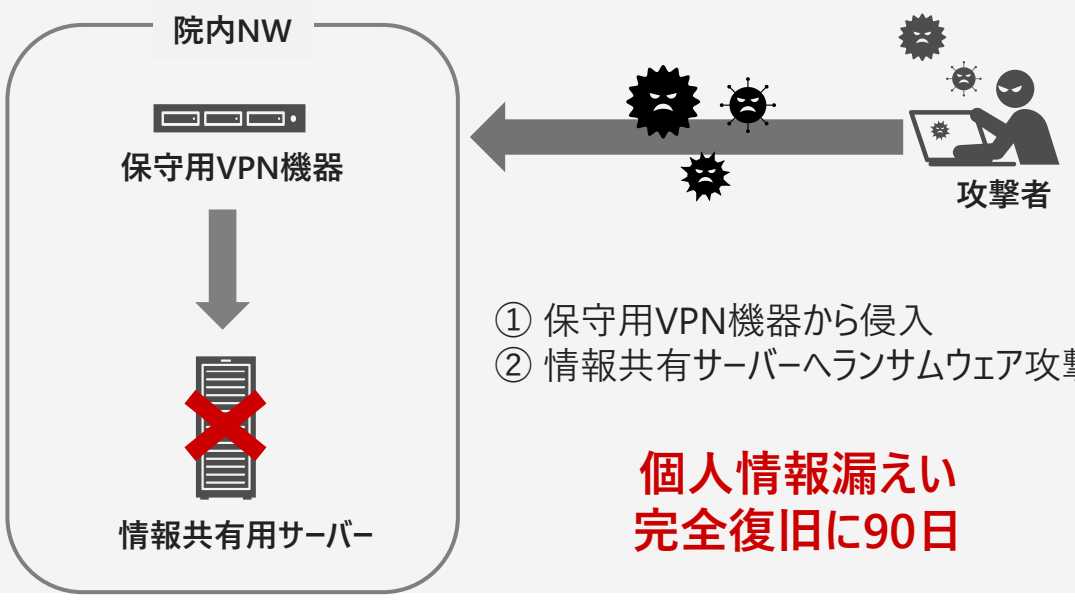


① 不使用のPCをリモートで操作
② PCを踏み台にして
　工場内のサーバーへランサム攻撃

業務データが一部利用不可
（後にバックアップから復旧）

B病院（医療、福祉）

原因　：アカウントの未管理
　　単純なパスワードの使いまわし
　　すべてのユーザーに管理者権限を付与

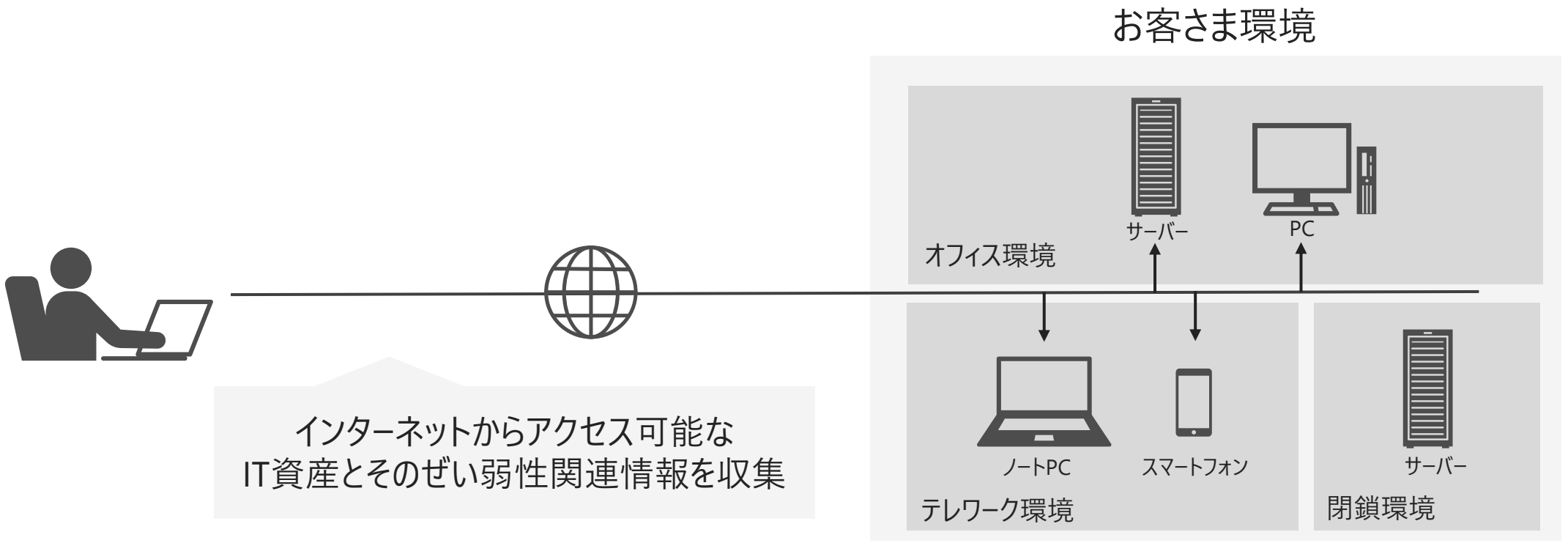


① 保守用VPN機器から侵入
② 情報共有サーバーへランサムウェア攻撃

個人情報漏えい
完全復旧に90日

HITACHI

アタックサーフェスマネジメント（ASM）
組織の外部からアクセス可能なIT資産とそのぜい弱性を継続的に検出・評価するプロセス



確認項目（一例）：ソフトウェアのバージョン/オープンポート/シャドーIT/設定不備等

HITACHI

インターネットからのアクセス可否、把握済か否かによらない包括的なIT資産の管理が必要

インターネットから直接アクセスできるIT資産か否か

自社で把握しているIT資産か否か	アクセス可能	アクセス不可
把握済	社外向けWebサイト メールサーバー ファイアウォール等	業務用のPC、サーバー 従業員のID等
未把握	未管理のサーバー 未管理のWebサイト等	個人の持ち込みデバイス 未管理のサーバー 退職者のID等

資産管理をせずにセキュリティ対策が行える範囲

HITACHI

インターネットからのアクセス可否、把握済か否かによらない包括的なIT資産の管理が必要

インターネットから直接アクセスできるIT資産か否か

自社で把握しているIT資産か否か	アクセス可能	アクセス不可
把握済	社外向けWebサイト メールサーバー ファイアウォール等	業務用のPC、サーバー 従業員のID等
未把握	未管理のサーバー 未管理のWebサイト等	個人の持ち込みデバイス 未管理のサーバー 退職者のID等

資産管理をせずにセキュリティ対策が行える範囲

＋

ASMで検知できる範囲

HITACHI

インターネットからのアクセス可否、把握済か否かによらない包括的なIT資産の管理が必要

インターネットから直接アクセスできるIT資産か否か

自社で把握しているIT資産か否か	アクセス可能	アクセス不可
把握済	社外向けWebサイト メールサーバー ファイアウォール等	業務用のPC、サーバー 従業員のID等
未把握	未管理のサーバー 未管理のWebサイト等	個人の持ち込みデバイス 未管理のサーバー 退職者のID等

資産管理をせずにセキュリティ対策が行える範囲

＋

ASMで検知できる範囲

＋

包括的な資産管理で管理すべき範囲

HITACHI

平時対応（プロアクティブ）と有事対応（リアクティブ）が重要

統治

識 別 ＞ 防 御 ＞ 検 知 ＞ 対 応 ＞ 復 旧

セキュリティ防御

ID管理・アクセス制御	教育・訓練
データセキュリティ	情報保護プロセス
保守	保護技術

Firewall /IDS / IPS / Proxy / DNS
IAM / EDR（XDR） / SWG / CASB 他

導入計画

リスクアセスメント	リスクマネジメント戦略
ビジネス環境	資産管理
ガバナンス	サプライチェーンリスク

評価 / 計画 / 管理 他

NIST (CSF) 2.0

NIST（米国国立標準技術研究所）「Cybersecurity Framework (CSF) 2.0」を参考に日立システムズにて作成
出典：National Institute of Standards and Technology (2024)
The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD),NIST Cybersecurity White Paper (CSWP) NIST CSWP 29.
https://doi.org/10.6028/NIST.CSWP.29

運用

検知	モニタリング
	検知・受付
対応	トリアージ
	分析・低減・改善
	コミュニケーション
	対応計画の作成
復旧	計画検討
	改善・コミュニケーション
	保守

SOC / CSIRT / ITSM / 現場対応 他

HITACHI

「サイバーハイジーン」「サイバーレジリエンス」とは

サイバーハイジーン
Cyber Hygiene

ハイジーンは「衛生」を意味しており、
社内のIT資産を日頃から管理し、
サイバー攻撃を防げる健全な状態を保つ取り組み

サイバーレジリエンス
Cyber Resilience

レジリエンスは「耐久力や回復力」を意味しており、
サイバー攻撃を受けたときその影響を最小化し、
早急に元の状態に戻す仕組みや能力

HITACHI

「サイバーハイジーン」「サイバーレジリエンス」から考えるセキュリティ対策のあり方

サイバーハイジーン

サイバーレジリエンス

統治

識 別	防 御	検 知	対 応	復 旧
・社内IT資産/構成情報の可視化/一元管理 ・IT資産に関わる取引先の契約を管理	・IT資産/アタックサーフェスのぜい弱性情報の収集/迅速適切な対応 ・外部第三者によるアセスメント、リスク最小化	・SOC監視体制の構築・運用 ・早期検知のための可視性の確保およびテクノロジー(AI等)の活用	・CSIRTによるインシデント 対応 ・システム・組織間の連携 ・インシデント対応の自動化	・事業継続性を優先した復旧 ・各種バックアップシステム/自動修復システムによる復旧
			検知アラーム/報告への対応および復旧の指揮	
IT資産・構成管理	ぜい弱性情報収集・管理	クラウド、ネットワーク、エンドポイント 常時監視	初動対応・被害拡大防止	バックアップ＆リストア
ライセンス・保守契約管理	外部第三者機関による定期アセスメント	NW、セキュリティ機器、クラウドサービス ログ監視	被害範囲特定・封じ込め	Disaster Recovery
各種セキュリティ対策		監視検知内容の調査	インシデント調査分析	再発防止策の策定および実施
ASM		社内関連部署(CSIRT)へ連絡	ステークホルダー連絡/連携、監督官庁への報告/届出	
セキュリティオペレーション自動化・オーケストレーションツール				

HITACHI

セキュリティ対応25業務とシステム対応8業務

セキュリティ対応業務

平時

1 リスク分析と評価	2 セキュリティ関連規則と業務の策定	3 セキュリティ関連の基本方針策定	4 セキュリティ関連の組織化
5 情報セキュリティ監査			
6 セキュティ専門組織の運営と評価	8 セキュティリスク対策	11 情報資産の管理	
		12 ぜい弱性ハンドリング	
7 教育、訓練	9 セキュリティでバイスの運用と管理	13 脅威インテリジェンスハンドリング	
		14 サプライチェーン管理	
	10 ぜい弱性評価と対策	15 セキュリティ関連ドキュメントの策定	

A

16 セキュリティイベントインシデント監視	17 インシデント検知・受付

B

有事

18 トリアージ	23 報告・情報公開	24 復旧対処
19 通 知		
20 初動対応・対処		25 コーディネーション
21 解 析		
22 対 策		

システム対応業務

C

1	セキュリティ対応業務用システム構成管理
2	セキュリティ対応業務用システム稼働トレンド管理
3	セキュリティ対応業務用システムおよびドキュメント変更計画
4	セキュリティ対応業務システムおよび関連ドキュメント変更修正対応

D

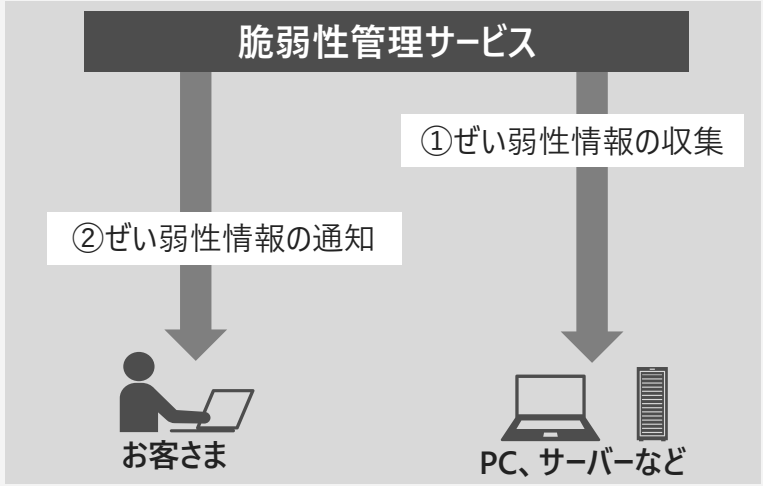
5	セキュリティ対応業務システム基盤システム監視
6	セキュリティ対応業務システム障害対応　（検知/インシデント登録/切り分け）
7	セキュリティ対応業務システム障害対応　（分析/処置/対策/関係者共有）
8	セキュリティインシデントおよびシステムインシデントに関連した修正

HITACHI

日立システムズのブースでは下記のサービスをご紹介しています

脆弱性管理サービス

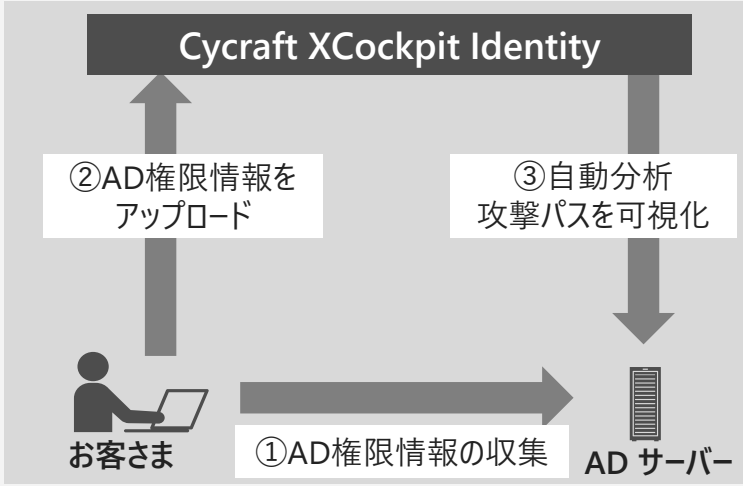
サイバーハイジーン



**お客さま環境のIT資産を自動でスキャンし
ぜい弱性情報を収集**

Cycraft XCockpit Identity

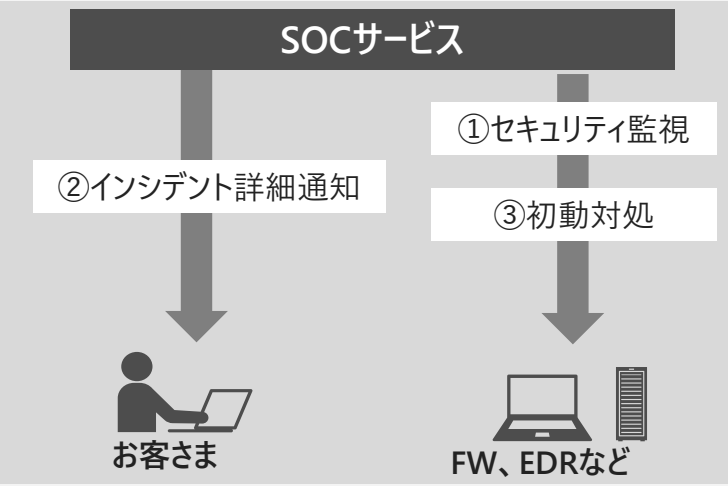
サイバーハイジーン



**Active Directoryの設定を分析し、
権限情報の収集、ぜい弱性を可視化**

SOCサービス

サイバーレジリエンス



**お客さま環境を24時間365日で監視し
有事にお客さまへ通知、
詳細の分析、初動対処を実施**

※Active Directoryは、米国Microsoft Corporationの米国およびその他の国または地域における、登録商標または商標です。
※CyCraft、XCockpit、XCockpit Identityは、台湾CyCraft Technologyの台湾およびその他の国または地域における、登録商標または商標です。

※その他記載の会社名、製品名は、それぞれの会社の登録商標、または商標です。
※ Cycraft XCockpit Identityは台湾CyCraft Technologyの製品「XCockpit IASM」を利用しています。

平時に対応すべきこと、有事対応で重要なこととは？

HITACHI