# Evolving Security

## for changing IoT world.

**日立のセキュリティで**
**スマートな社会を実現するお客さまのビジネスを、さらに前へ。**

### DXがもたらす社会変化と新たなビジネス・価値の創出

事業のグローバル化や業界・企業の垣根を越えたビジネスの創出をもたらすデジタルトランスフォーメーション(DX)。DXの浸透によって人や情報、組織はデジタルでつながり、新たな価値を加速的に創造するスマート社会へと変容を遂げようとしています。

### スマート社会においてますます複雑化するセキュリティ

新たな変化や価値が生まれる一方で、セキュリティの視点では未知の脅威・リスクに即応していくことが必要です。国際機関や国、各業界は、新たな技術や脅威・リスクを前提とした法規制・ガイドラインを定め、企業はそれらをビジネスに適用し、対策することが求められています。代表例として米国のNIST SP800やEUのGDPR、自動車業界でのWP29などがありますが、近年では経済安全保障に関わる機器の管理についても制度化が検討され始め、各企業における課題となっています。また、企業内だけでなくサプライチェーン全体を考慮したルールへの準拠が要求されるなど、セキュリティを取り巻く状況はより複雑さを増しています。

### ビジネスをさらに前へ進めるための日立のセキュリティ

長年の経験を通して蓄積したさまざまな業界の知見とセキュリティ分野における実績を強みとし、お客さまのセキュリティに関するコンセプトづくりから運用までを日立グループで連携し、トータルに提案します。システムの保護といったITの観点に限らず、プロダクトやサプライチェーンなど、広範囲でのセキュリティ確保を実現するための最適なソリューションやサービスを提供することで、お客さまのビジネスをさらに前へ進める環境づくりをご支援します。

NIST：National Institute of Standards and Technology (国立標準技術研究所(米国))、WP29：World Forum for Harmonization of Vehicle Regulations

進化1

# システムセキュリティから お客さまの事業全体を守るセキュリティへ

サイバーセキュリティを検討するうえで最も重要なことは「サイバーセキュリティを経営課題として位置づける」ことです。そのうえで、セキュリティ対策をシステム個別ではなく事業全体で最適化し、継続的かつ着実に実行することが必要です。また、事業活動の関係者すべてを巻き込み、ガバナンスを強化することも大切です。

日立は、さまざまな事業分野でのオンプレミスのIT・OT・IoTシステムはもちろん、クラウドシステムでのセキュリティの実装や日立グループのITインフラの構築、運用を通して得たセキュリティの知見を、過去のランサムウェア事案の教訓も踏まえてお客さまに還元します。長年の実績で蓄積したノウハウとスキルを生かし、個々のお客さまにフィットしたセキュリティをコンセプト作りからご提案することで、システムの先にある「事業」を守ります。ゼロトラスト型のセキュリティや認証基盤などのソリューションのほか、IT部門に留まらないセキュリティガバナンスの醸成などを通じ、安心してお客さまが事業を推進するためのセキュリティエコシステムの構築をお手伝いします。

## 進化2

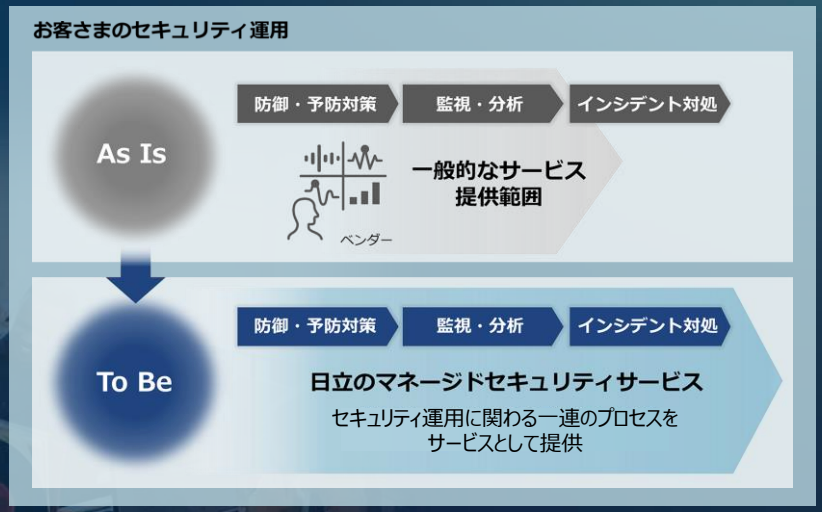
# 検証可能なエビデンス管理や情報共有でサプライチェーン全体の信頼確保

セキュリティに関する各種ガイドラインやルールの整備が進み、技術的にもゼロトラストセキュリティが普及したことで、企業・組織内のセキュリティレベルは向上する傾向にあります。一方で、社外のパートナーやサプライチェーンの脆弱な部分を狙ったサイバー攻撃により、被害を受ける事案が増えています。これは、サプライチェーン全体でセキュリティを確保しなければならない時代の訪れを意味しており、実際にGDPR、WP29といったガイドラインにおいても、説明責任の対象はグローバルなサプライチェーン全体に及んでいます。日立は製造業としての知見をもとに、サプライチェーン全体の工程が手順どおり行われていることの検証や、その検証を第三者へ説明するエビデンス管理、そのような情報を安全に共有するプラットフォーム提供を通じ、サプライチェーンを含めたお客さまの信頼確保とサプライチェーン内の情報のシームレス化を支援し、高度なビジネス推進を実現します。

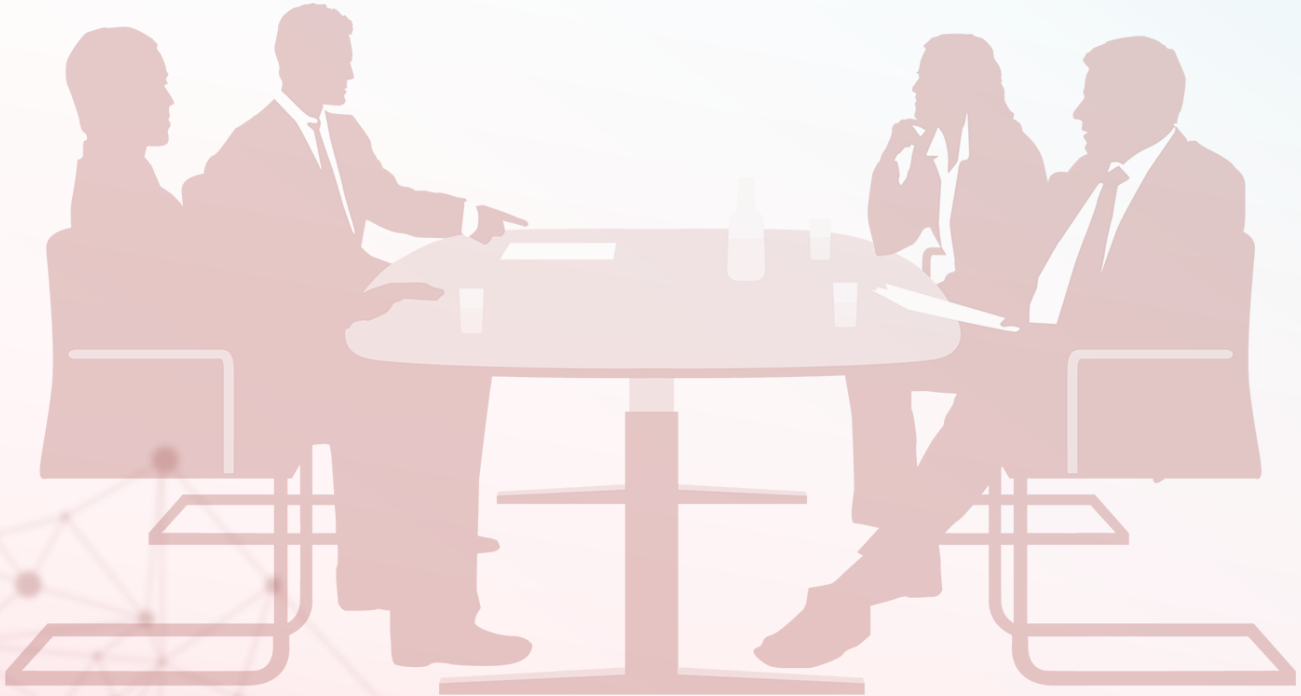

## 進化3

# 高度なセキュリティ運用の実現で安心してビジネスに注力できる環境へ

サイバー攻撃による被害が日常的に報じられる昨今、企業におけるセキュリティ運用は、事業を継続的に守るために、よりいっそう重要視されています。しかし、セキュリティ運用には高度なセキュリティスキルが不可欠です。このため、人財の確保・育成が大きな課題となっています。日立は、このような課題をお持ちのお客さまに向けて、セキュリティ運用を支援するマネージドセキュリティサービスをご提供します。日立のマネージドセキュリティサービスは、セキュリティ監視・分析業務の支援はもちろん、インシデント発生前のプロアクティブな対応やインシデント発生時の速やかな対処や修復など、セキュリティ運用に関わる一連のプロセスをサービスとして提供し、お客さまのセキュリティ運用負荷の軽減を実現。セキュリティを日立にお任せいただくことで、事業の継続性を確保しながら、安心してビジネスに注力できます。



# セキュリティガバナンス



# セキュリティソリューションマップ

| 対象 ＼ セキュリティ分類(*) | | | 特定 | 防御 | 検知 | 対応 | 復旧 |
|---|---|---|---|---|---|---|---|
| セキュリティガバナンス | 規則・ポリシー | | セキュリティプロフェッショナルサービス | | | サイバーインシデント対応<br>BCPコンサルティング | |
| | 組織・体制 | | | | CSIRT構築コンサルティング | | |
| | 教育・人財育成 | | セキュリティ教育 | | | | |
| | セキュリティ分析 | | 診断・<br>ペネトレーションテスト | | | | |
| サイバーセキュリティ対策 | 業務・アプリケーション | | サプライチェーントラスト | | | | |
| | オフィス<br>(IT環境) | 社外・クラウド環境 | ゼロトラスト・セキュリティ | | セキュリティ運用・監視 | | |
| | | オンプレミス環境 | 認証・ID管理/指静脈認証<br>内部不正対策 | | | | |
| | 制御系<br>(OT環境) | 工場・制御システム | 工場セキュリティ | | | | |
| | | 社会インフラ<br>制御システム | 社会インフラ・制御セキュリティ | | | | |
| | 製品・サービス<br>(IoT機器) | 製品セキュリティ | プロダクトセキュリティ | | | | |

(*)NISTサイバーセキュリティフレームワークによる分類

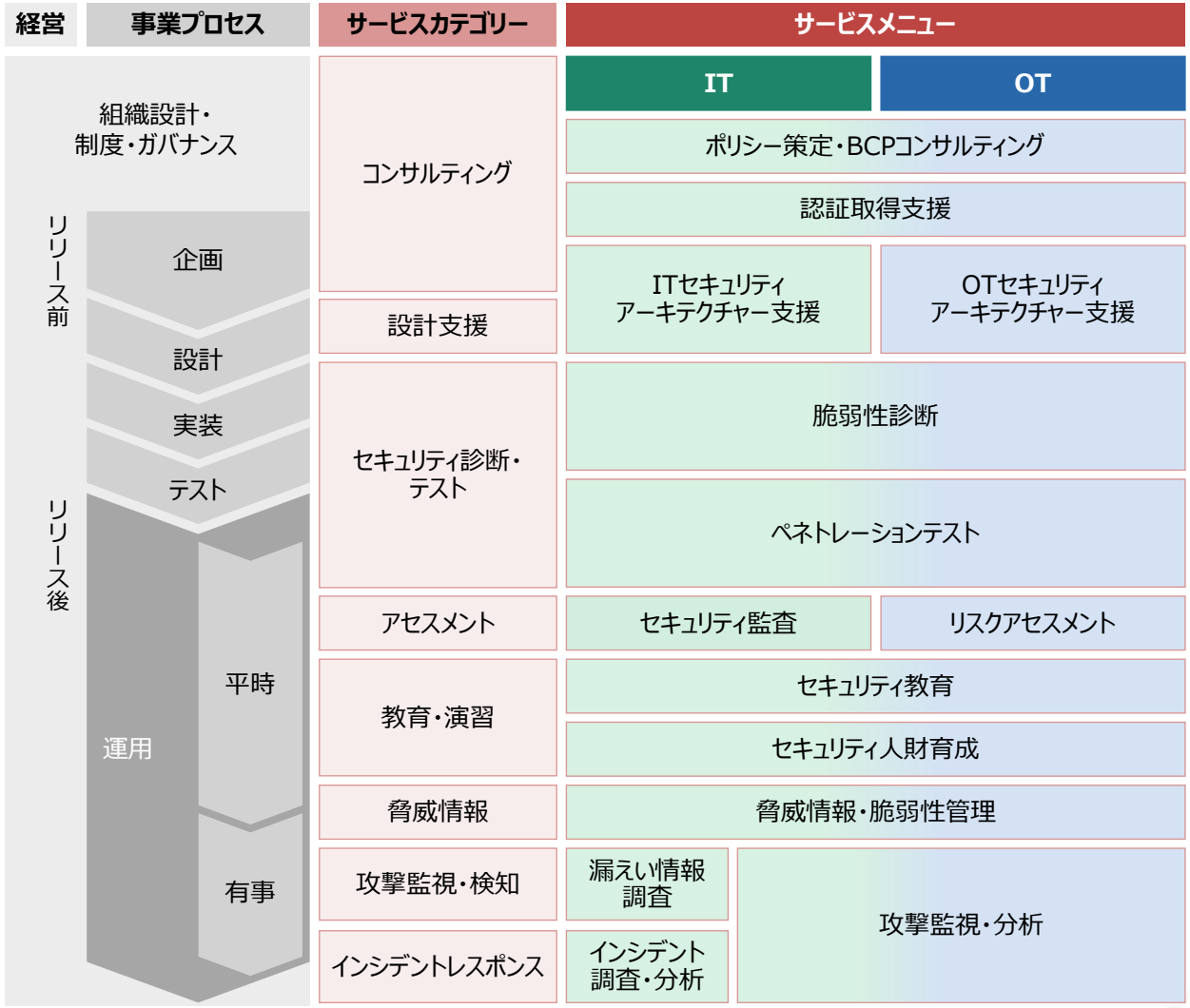
BCP : Business Continuity Plan

# セキュリティプロフェッショナルサービス

IT/OTシステムのライフサイクル全般にわたり、日立グループのサービスメニューから
お客さまの課題に最適なサービスを選択し、セキュリティ施策を実行。
お客さま事業の継続的な運用を可能にします。

**セキュリティガバナンス**
規則・ポリシー 組織・体制
教育・人財育成 セキュリティ分析

セキュリティプロフェッショナルサービス
セキュリティサイト
詳細はこちら




システムライフサイクル全般にわたるサービスメニュー

## 日立の強み

### トータルなサービスを提供

電力・鉄道・金融・製造分野でのセキュリティ対策を施した豊富なシステム構築実績やサービス提供の経験を踏まえ、企画～設計～運用までのシステムライフサイクルに応じたトータルなサービスを提供

### さまざまなセキュリティ施策の実行支援

国内外のセキュリティの法規制・ガイドラインを踏まえて、お客さまの実情に合わせ、日立グループ全体のサービスメニューから課題解決にフィットするサービスを選択し、最適なセキュリティ施策の実行を支援

### 専門知識を有したセキュリティ人財

専門知識や経験を有したセキュリティ人財による、業種・業界の特性や日立グループ内外でのサービス提供実績に基づく豊富なセキュリティノウハウの提供

# サイバーインシデント対応 BCPコンサルティング

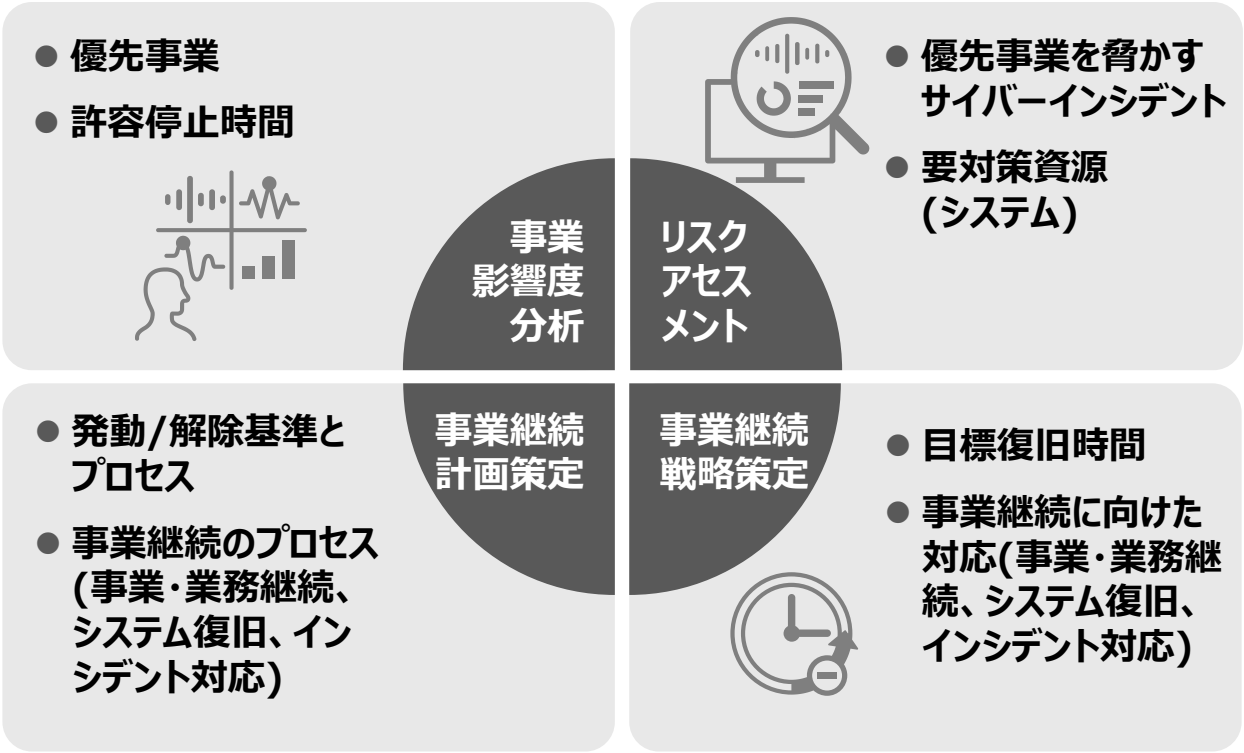
お客さまのサイバーセキュリティリスクに対し、事業・業務、危機管理、およびシステム視点から事業継続策の策定をご支援し、レジリエンスの強化をはかります。

セキュリティガバナンス　規則・ポリシー 組織・体制

サイバーインシデント対応BCPコンサルティング セキュリティサイト
詳細はこちら

## サイバーインシデント対応BCPコンサルティングの全体工程

お客さまの事業の継続、または復旧を有効に機能させるため、サイバーインシデントへの適切な対応や、IT/OTシステムの技術的対応を向上、連携します。




ISO : International Organization for Standardization

## 日立の強み

### サイバー攻撃に特化したBCPの策定支援

高度化するサイバー攻撃に特化したリスク分析や対応計画など、対策から監視運用、復旧までの事業継続計画(BCP)策定をトータルにサポートします。

### 規格やガイドへの対応

ISO 22301:2019などの国際規格・ガイドに対応した支援も可能です。

### さまざまなリスクでの知見・ノウハウの活用

自然災害やパンデミック対応のBCPコンサルティングで得た知見、ノウハウをサイバーインシデント対応BCPにも活用します。

# CSIRT構築コンサルティング

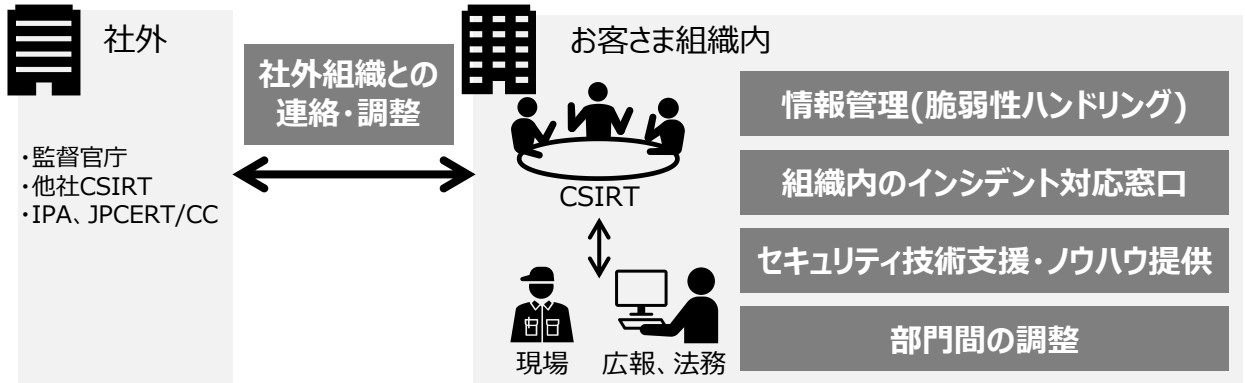
セキュリティガバナンス　組織・体制

日立グループにおけるCSIRT構築・運用のノウハウとともに、これまでの豊富な提案実績から、
お客さまに寄り添った効率的かつ高品質なCSIRT構築コンサルティングをご提供します。

CSIRT構築コンサルティング
セキュリティサイト
詳細はこちら

## CSIRTの役割、CSIRT構築コンサルティングの流れ

### CSIRTの役割




### CSIRT構築コンサルティングの流れ

体制の確保 ▶ CSIRT構築プロジェクトの立ち上げ ▶ 現状分析の実施 ▶ インシデント対応ポリシー策定 ▶ 関連規定整備 ▶ 運用の開始

## 日立の強み

### 豊富な提案実績によるノウハウの活用

規模や業種を問わず、これまでの多くの実績から得られた各種基準やガイドラインに対する知見や、テンプレートの活用により、効率的かつ実運用に即したご提案が可能です。

### 実績とスキルをもつコンサルティング要員

幅広い業種にそれぞれ対応したセキュリティアセスメントの実績豊富なコンサルティング要員が、お客さまに寄り添ってご対応いたします。

### 日立のCSIRT(HIRT)との連携

日立グループにおけるCSIRTであるHIRTと連携し、CSIRTについての社内有識者から後方支援を受けることが可能です。

CSIRT：Computer Security Incident Response Team、IPA：Information-technology Promotion Agency, Japan、
JPCERT/CC：Japan Computer Emergency Response Team/Coordination Center、HIRT：Hitachi Incident Response Team

セキュリティガバナンス

教育・人財育成

# セキュリティ教育

さまざまな業務で必要となるセキュリティの知識について、社員の業務内容やレベルに応じて学習できる教育メニューをご提供します。

セキュリティ教育
セキュリティサイト
詳細はこちら

## 各社員層に合わせて段階的に教育が実施できるメニュー

### 一般社員向けセキュリティ教育

- サイバー攻撃対応基礎
- セキュリティ最新動向 ほか

### 経営層・管理者向けセキュリティ教育

- セキュリティリスク分析 ほか

### 技術職社員向けセキュリティ教育

- ネットワークセキュリティ対策実習
- Certified Ethical Hacker (ホワイトハットハッカー養成)
- サイバー攻撃対応コミュニケーション訓練
- IoT技術解説 －セキュリティ編－ ほか

### サイバー防衛の訓練環境(Nx Security Training Arena: NxSeTA)

現場から経営層まで多様で総合的な訓練を実施

お客さまシステム(IT/OT)を模した訓練環境

## 日立の強み

### 業界をリードする高度なメンバーによる教育

高度な専門性を生かし、優れた人財の育成を通じて社会に寄与するというミッションのもと、多彩な専門家がお客さまの事業に貢献できるさまざまな教育サービスを提供します。

### 日立のIT・OT・プロダクトで培ったノウハウ

日立グループの幅広い環境にまたがる実績と知見をもとにした人財育成メニューを提供し、デジタル時代におけるお客さまのビジネスをサポートします。

### お客さまの実状に合わせた訓練環境

日立の情報・制御システムで培ったノウハウを活用し、お客さまシステムに近い訓練環境(Nx Security Training Arena: NxSeTA)で実態に即した訓練を提供します。

# 診断・ペネトレーションテスト

企業資産の脆弱性を検知する「脆弱性診断」、攻撃者と同じ手口で疑似攻撃を実施する「ペネトレーションテスト」で、セキュリティ課題を網羅的に抽出します。

セキュリティガバナンス | セキュリティ分析

診断・ペネトレーションテスト
セキュリティサイト
詳細はこちら

## 診断・ペネトレーションテストの概要

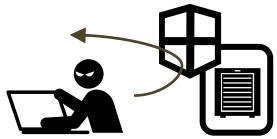
### システム管理者のお悩み

- ✓管理者が把握できていない資産がある
- ✓管理できていない資産が攻撃者に狙われてしまう
- ✓新たな攻撃に既設のセキュリティ対策で対応できるだろうか

**脆弱性診断**

資産の洗い出し → 資産の脆弱性を診断 → リスクへの即時対応

トップドメイン
情報/証明書など



**資産を自動で探索**　**資産の脆弱性を診断**　**ターゲットとなるリスクを低減**

**ペネトレーションテスト**

攻撃者の手口で侵入 → 既設のセキュリティ対策を調査

ホワイトハットハッカー

**攻撃者として侵入**

**既設のセキュリティ対策が破られないかを調査**

## 日立の強み

### ✓企業資産を自動で探索、攻撃者に狙われるリスクを抽出

診断は、攻撃の侵入口となる資産の脆弱性を洗い出します。管理者が把握していない資産についても自動で診断が可能です。

### ✓攻撃者と同じ手口で侵入し、現状を調査

攻撃者と同じ手口を再現して侵入するペネトレーションテストによって、現状の対策の有効性をチェックできます。

### ✓ホワイトハットハッカーによる精度の高い診断が可能

国内外の著名なセキュリティコンテスト＊で好成績をおさめるホワイトハットハッカーが手動または、ツールを駆使し精度の高い診断を実施します。

＊SANS Institute(政府や企業・団体間における研究、およびそれらに所属する人々のITセキュリティ教育を目的としたセキュリティ研究・教育機関)が主催する「SANS 日本NetWars」など

# サイバーセキュリティ対策

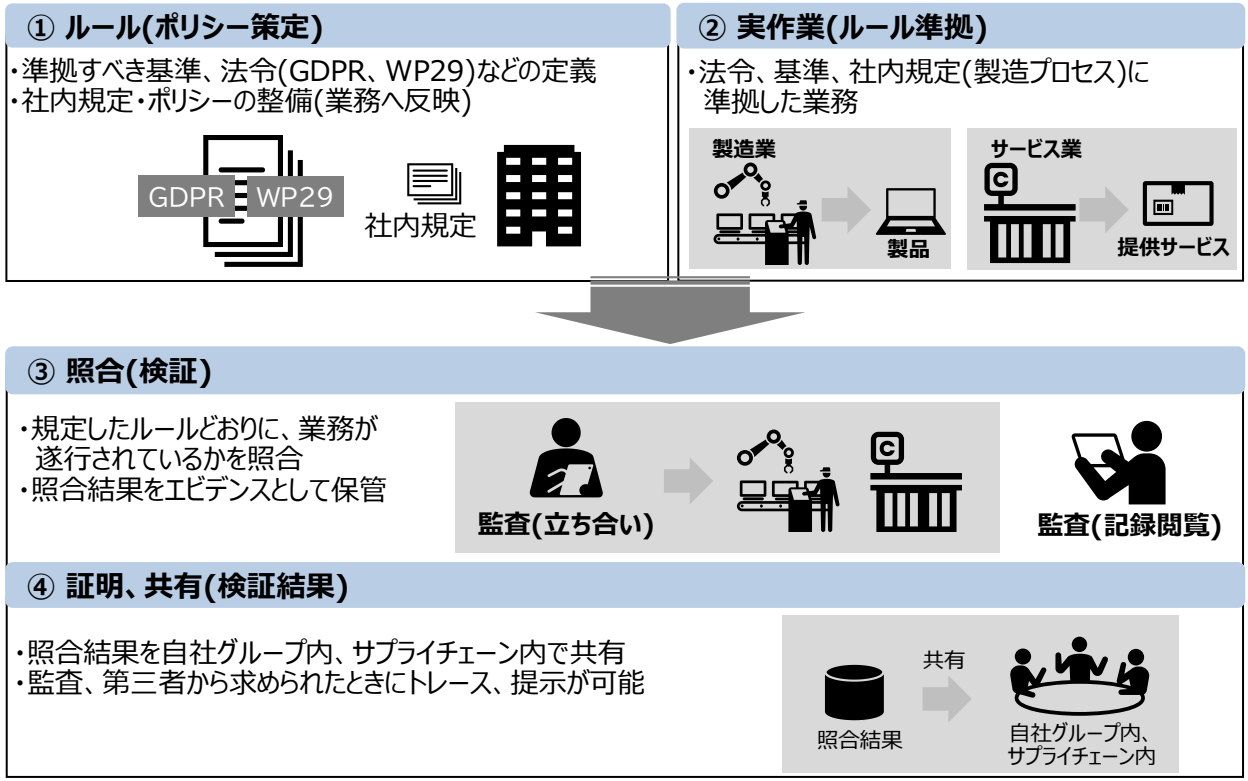
 

# サプライチェーントラスト

お客さまの事業活動をデジタル化の観点から「見える化」して共有し、
業務全体の「正しさ」を証明します。これにより企業・事業の信頼向上に貢献します。

サプライチェーントラスト
セキュリティサイト
詳細はこちら

## サプライチェーントラスト実現の流れ




## 日立の強み

### 事業活動の「正しさ」を証明し、リスクを低減

収集・蓄積したデータの分析・利活用によって、お客さまの事業活動を「見える化」して共有し、事業の正しさを証明することで信頼維持、向上を図ります。これにより、お客さま事業活動の付加価値向上や、リスク低減を支援します。

### 「正しさ」実現のためのさまざまな機能を提供

「見える化」と共有による事業の「正しさ」の実現のため、以下の機能をご提供します
(②はお客さまにて実施)。

① **ルール**(ポリシー策定):正しい規定を備える
② **実作業**(ルール準拠):規定に従い正しく業務実施
③ **照合**(検証):業務が正しく実施されたかを検証
④ **証明、共有**(検証結果):検証結果を示す・共有

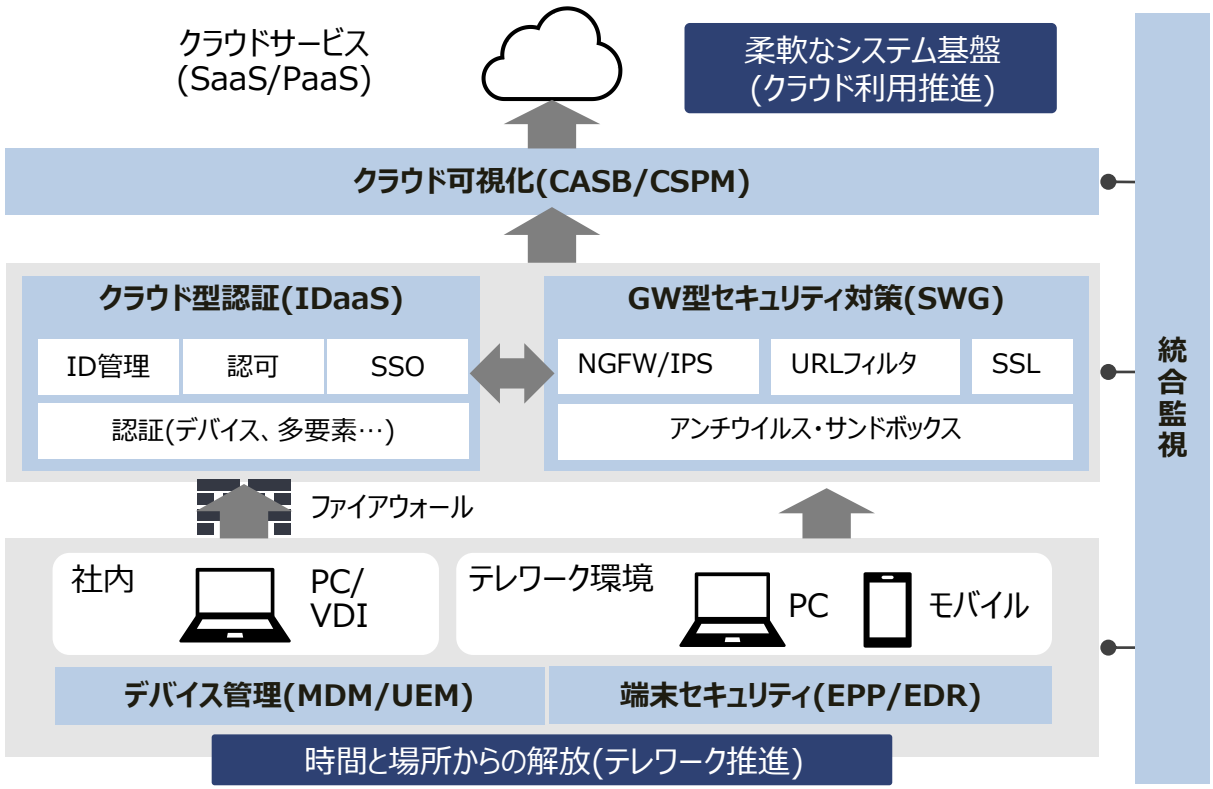
GDPR:General Data Protection Regulation、WP29:World Forum for Harmonization of Vehicle Regulations

# ゼロトラスト・セキュリティ

すべてを信頼しない(ゼロトラスト)というセキュリティアプローチで、
クラウド・インターネット環境に必要な各種セキュリティサービスの導入を支援します。

ゼロトラスト・セキュリティ
セキュリティサイト
詳細はこちら

## ゼロトラスト・セキュリティの要素と構成




## 日立の強み

### 上流コンサルティング、実装、運用まで一貫して支援

サードパーティのSaaS型セキュリティを部品として活用して、お客さまの求めるゼロトラスト環境を設計、具現化し、運用までを一貫して支援します。

### 日立社内のノウハウを最大限に活用

日立社内システムとして構築しているゼロトラスト環境で得られた知見をコンサルティングに活用、計画段階からお客さまの事業に寄り添ったご提案を実施します。

### 日立グループの豊富な商材を活用したご提案

日立製作所をはじめとした日立グループで取り扱う豊富な商材の中から、お客さま環境に最適なものを検討、プロダクトの実装から運用に必要なサービスまですべてご提案します。

SaaS：Software as a Service、PaaS：Platform as a Service、CASB：Cloud Access Security Broker、CSPM：Cloud Security Posture Management、IDaaS：Identity as a Service、
SSO：Single Sign-On、SWG：Secure Web Gateway、NGFW：Next-Generation Firewall、IPS：Intrusion Prevention System、SSL：Secure Sockets Layer、VDI：Virtual Desktop Infrastructure、
MDM：Mobile Device Management、UEM：Unified Endpoint Management、EPP：Endpoint Protection Platform、EDR：Endpoint Detection and Response

サイバーセキュリティ対策

社外・クラウド環境
オンプレミス環境

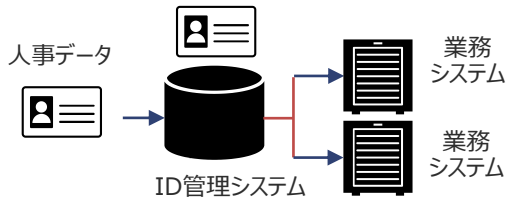
# 認証・ID管理/指静脈認証

クラウド環境にも対応した統合ID管理ソリューション(ID管理、シングルサインオン)と生体認証(指静脈認証)によって、高度な本人認証機能をご提供します。

認証・ID管理/指静脈認証
セキュリティサイト
詳細はこちら

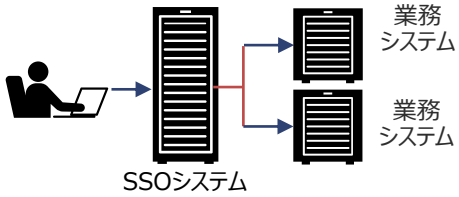
## 統合ID管理の概要

<ID管理>




・ID情報を一元管理し、自動配布
・不要なID削除でセキュリティ強化

<シングルサインオン(SSO)>




・一度の認証で、複数サービスにログイン
・ユーザーの作業効率を向上

## 生体認証(指静脈認証)の概要


・キャッシュレス決済、手ぶらでの入退管理、業務システムの本人確認など、民間や公共機関でグローバルにシステム提供中

・PCのフロントカメラでの認証も可能

SSO：Single Sign-On

## 日立の強み

### 統合ID管理ソリューションを総合的に提案

お客さまの課題に合わせた統合ID管理ソリューション(ID管理、シングルサインオン)をご提案します。
セキュリティに精通した技術者が、豊富な導入経験を生かし、コンサルティングから保守サポートまでワンストップでご提供します。

### 認証強化の枠を超え、世界でも信頼される指静脈認証

日立独自の技術による高セキュアな指静脈での本人認証により、クライアントPCや入退室管理をはじめ、社内システム、勤怠管理など、幅広い分野で業種を問わず生体認証ソリューションをご提供しています。
日立の技術は海外でも認められ、金融機関の本人確認やキャッシュレス対応、各国公的機関での認証でも活用されています。

# 内部不正対策

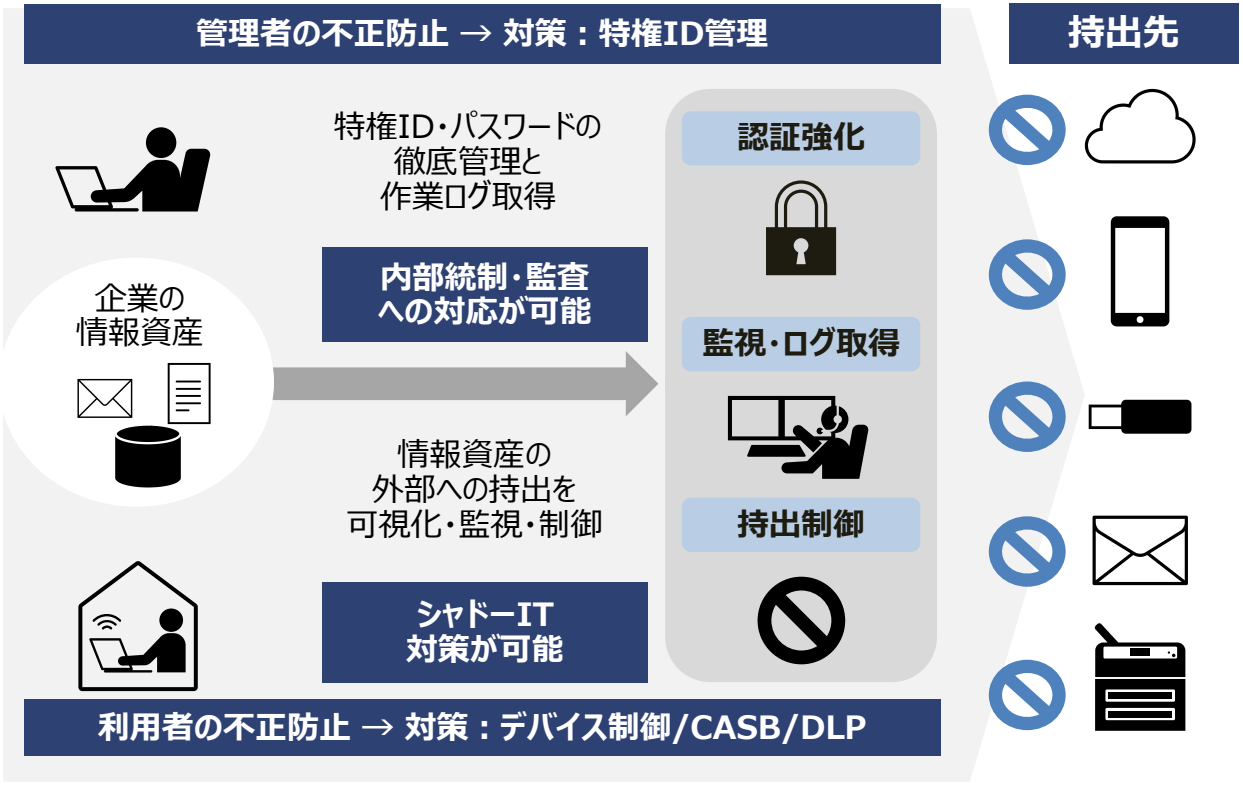
サイバーセキュリティ対策

社外・クラウド環境
オンプレミス環境

認証強化・監視・持ち出し制御などのセキュリティソリューションを組み合わせることで、
管理者や利用者の内部不正による情報漏えいリスクを防止します。

内部不正対策
セキュリティサイト
詳細はこちら

## 内部不正対策ソリューションの概要




## 日立の強み

### さまざまな実現方式の特権ID管理製品が選択可能

- 特権ID管理は、管理者の申請履歴や作業内容をログとして残す対策です。
- 管理者が申請で貸与された特権ID/パスワードで直接サーバーへアクセスする方式や、踏み台サーバーからのアクセスのみを許可する方式を選択可能で、お客さまの要件に合わせてご提案します。

### 情報漏えいの原因となる利用者の持出操作を制御

- クラウドへのファイルアップロードや、スマホ・メディアへのコピー、メール添付、印刷など、情報漏えいの原因となるあらゆる持ち出し操作を制御します。
- クラウド利用状況の可視化・制御を行うCASBなどゼロトラスト・セキュリティを見据えた内部不正対策が可能です。

CASB：Cloud Access Security Broker、DLP：Data Loss Prevention

# セキュリティ運用・監視

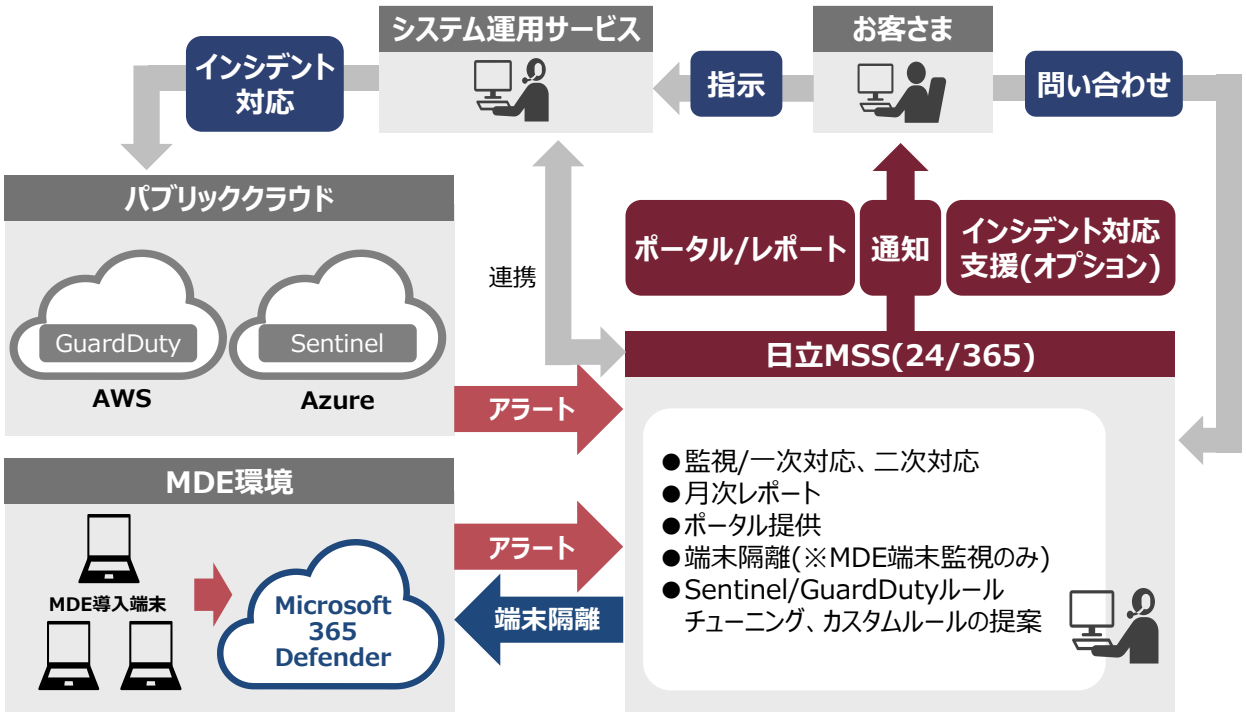
サイバーセキュリティ対策

社外・クラウド環境
オンプレミス環境

お客さまがご契約のパブリッククラウドやEDR環境に対する脅威監視、詳細分析をします。
月次レポートの提供やインシデントレスポンスへの対応支援を実施します。

セキュリティ運用・監視
セキュリティサイト
詳細はこちら

## セキュリティ運用、監視の概要




MSS：Managed Security Service

## 日立の強み

### 豊富な運用実績

大手金融機関や官公庁、大手製造業など150社以上のお客さま向けに、20年以上にわたりセキュリティ監視サービスを提供。

### セキュリティ専門組織による高い監視品質、高度分析

最新の攻撃・脅威情報や当社が保有するインシデント事例の情報を分析し、検知ルールに実装することで、高品質なセキュリティ監視・分析サービスを提供。

### 社内実践ノウハウの活用

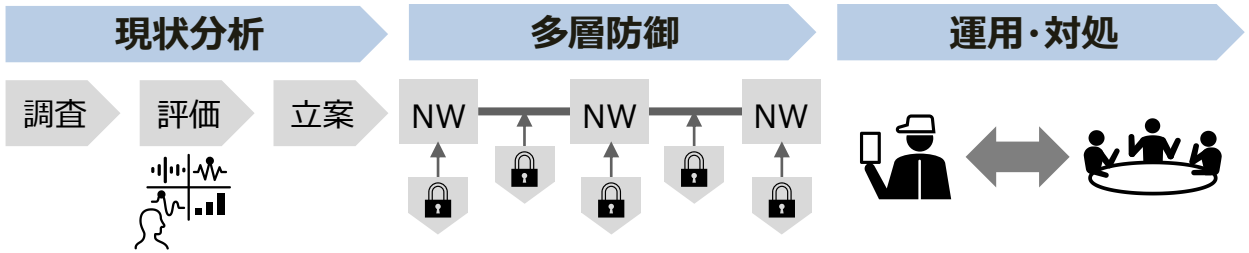
日立グループが利用するIT基盤のセキュリティ監視の実践ノウハウを最大限に活用。

# 工場セキュリティ

日立の工場、生産現場で培ったノウハウを活用し、現場と運用に即した実用的な制御システムセキュリティを現状分析から多層防御の実装、運用までご提案します。

工場・制御セキュリティ
セキュリティサイト
詳細はこちら

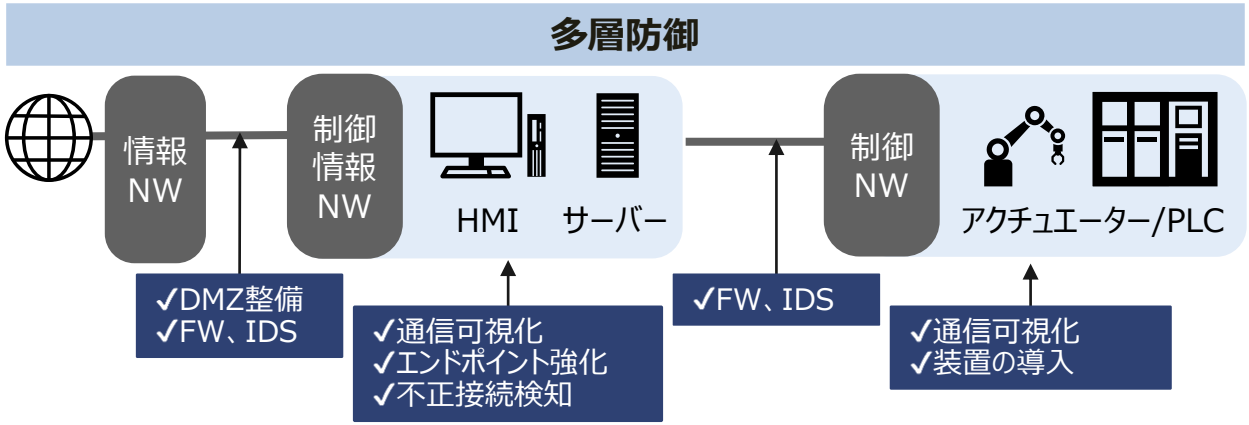
## 工場セキュリティの概要




✓日立の実業でのノウハウ
✓現場に踏み込んだコンサルティング

✓階層化に適した多層防御
✓可用性に重点を置く提案

✓現場とシステム管理者の連携を重視した検知、対応体制




## 日立の強み

### 日立の工場で培ったノウハウを生かした現状分析

日立の工場、生産現場におけるセキュリティノウハウを体得したアナリストによる、現場運用に寄り添った現状分析をいたします。

### 工場セキュリティに特化した多層防御

インストールが可能な機器とそうでないものの管理、工場ネットワークへの影響を加味し、可用性確保が前提の工場現場に特化したセキュリティをご提案します。

### 現場とシステム管理者が連携して運用する体制

インシデント発生時にいち早く現場で検知し、社内の関連部門と連携して対応できる運用体制の構築をご提案します。
シミュレーターおよび総合訓練施設などのご相談も可能です。

DMZ：Demilitarized Zone、FW：Firewall、IDS：Intrusion Detection System、HMI：Human Machine Interface、PLC：Programmable Logic Controller

サイバーセキュリティ対策

社会インフラ
制御システム

# 社会インフラ・制御セキュリティ

社会インフラの制御システムを構築・運用してきたノウハウを生かし、
事業の継続性を重視したトータルセキュリティソリューションをご提供します。

**社会インフラ・制御セキュリティ**
セキュリティサイト
詳細はこちら

## トータルセキュリティソリューション

### セキュリティ コンサルティングサービス

リスク識別　リスク評価　対策立案

### セキュリティ監視 ソリューション

インシデントの見える化　USB管理

### セキュリティ 監視・分析支援サービス

ワンストップで支援　専門チームによる調査・分析

### サイバー防衛訓練サービス

実践的な訓練　組織力強化

**お客さまの組織・運用・システムに合わせたソリューションを提供**

## 日立の強み

### 制御システムを提供し、使用し続けてきた知見

長年にわたり、電力・鉄道・ガス・水などさまざまな社会インフラの制御システムの構築・運用で蓄積し、自社でも利用してきた豊富な知見により、お客さまの事業継続を支援します。

### 日立の工場でのセキュリティの運用実績

日立の工場の制御システムへのセキュリティ機能実装および事業継続対策をとおして得たノウハウを基に、お客さまに合わせたセキュリティをご提案します。

### トータルなセキュリティソリューションの提供

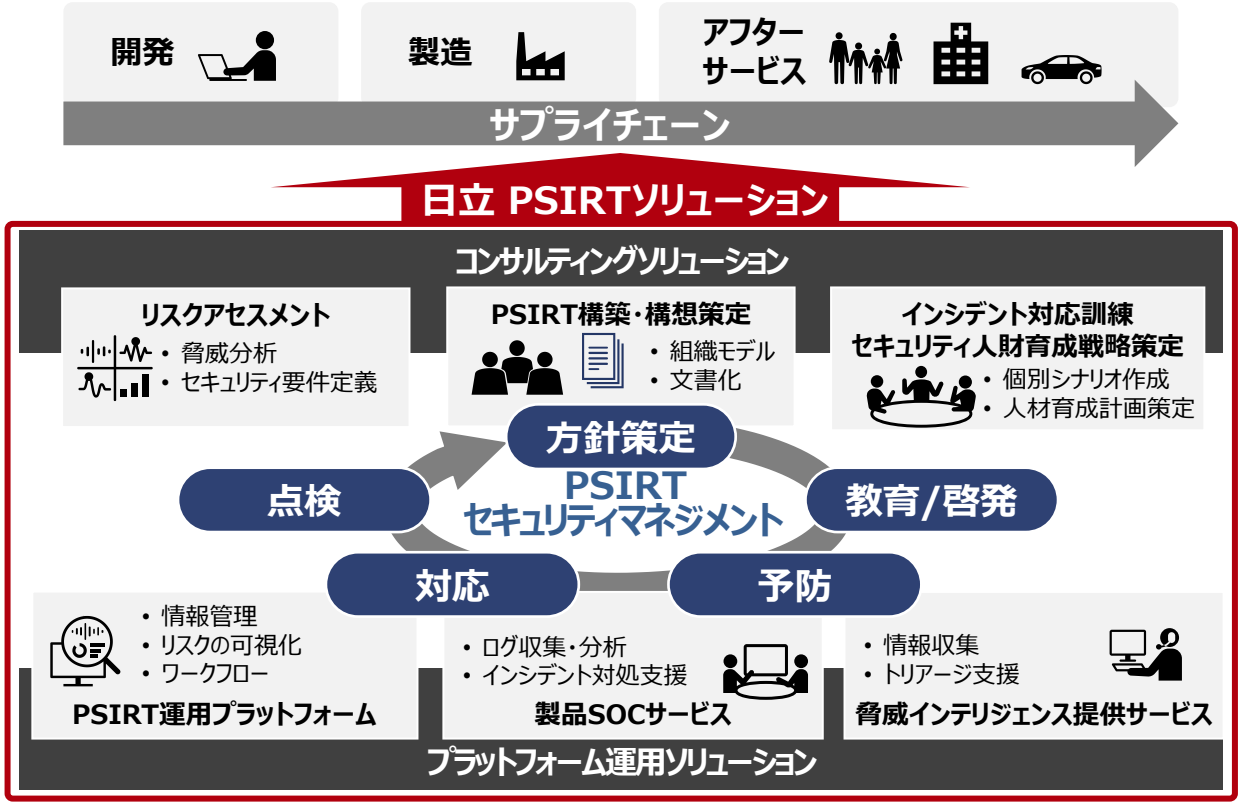
計画立案や現状のリスク把握のコンサルティングから導入・運用支援サービスまでの幅広い製品・サービスを持つ日立が、全面的にお客さまのセキュリティ導入を支援します。

# プロダクトセキュリティ

日立PSIRTソリューションにより、お客さまの製品・サービスのサプライチェーン全体のセキュリティ確保を支援します。

プロダクトセキュリティ
セキュリティサイト
詳細はこちら

## 製品・サービスの安全を守るPSIRT




## 日立の強み

### PSIRTのマネジメントをトータルにご提供

方針策定から点検・アセスメントまで、お客さまの製品・サービスのインシデントマネジメントをトータルにご支援します。

### 最先端の技術活用によるセキュリティ運用

AIやセキュリティ分析ノウハウを元に開発した最先端の技術をご提供し、運用の高度化および自動化を促し、お客さまをサポートします。

### 日立のノウハウを最大限活用

自社のプロダクトセキュリティ運用経験に加え、多数の製造業における実績で培ったノウハウを基に、お客さまに最適なプロダクトセキュリティをご提案します。

PSIRT：Product Security Incident Response Team、SOC：Security Operation Center

## 略称

BCP : Business Continuity Plan
CASB : Cloud Access Security Broker
CSIRT : Computer Security Incident Response Team
CSPM : Cloud Security Posture Management
DLP : Data Loss Prevention
DMZ : Demilitarized Zone
DX : デジタルトランスフォーメーション
EDR : Endpoint Detection and Response
EPP : Endpoint Protection Platform
FW : Firewall
GDPR : General Data Protection Regulation
IDaaS : Identity as a Service
IDS : Intrusion Detection System
IPA : Information-technology Promotion Agency, Japan
IPS : Intrusion Prevention System
ISO : International Organization for Standardization
HIRT : Hitachi Incident Response Team
HMI : Human Machine Interface
JPCERT/CC : Japan Computer Emergency Response Team/Coordination Center
MDM : Mobile Device Management
MSS : Managed Security Service
NGFW : Next-Generation Firewall
NIST : National Institute of Standards and Technology (国立標準技術研究所(米国))
PaaS : Platform as a Service
PLC : Programmable Logic Controller
PSIRT : Product Security Incident Response Team
SaaS : Software as a Service
SOC : Security Operation Center
SSL : Secure Sockets Layer
SSO : Single Sign-On
SWG : Secure Web Gateway
UEM : Unified Endpoint Management
VDI : Virtual Desktop Infrastructure
VMS : Video Management System
WP29 : World Forum for Harmonization of Vehicle Regulations

## 他社商標



●カタログに記載の仕様は、製品の改良などのため予告なく変更することがあります。
●製品の色は印刷されたものですので、実際の製品の色調と異なる場合があります。
●本製品を輸出される場合には、外国為替および外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ、必要な手続きをお取りください。なお、ご不明な場合は、当社担当営業にお問い合わせください。

**製品に関する詳細・お問い合わせは下記へ**

**■製品情報サイト**
**https://www.hitachi.co.jp/security/**

**■インターネットでのお問い合わせ**
**https://www.hitachi.co.jp/security-inq/**

株式会社 日立製作所　クラウドサービスプラットフォームビジネスユニット

2024.03