HITACHI
Inspire the Next

情報セキュリティ報告書 2018

Information Security Report 2018

日立グループ

ごあいさつ

日立グループは、デジタル技術を活用してお客様やパートナーと新たな価値を協創する、社会イノベーション事業に取り組んでいます。その基盤となっているのが人工知能やビッグデータの分析技術を簡単に利用するためのIoTプラットフォーム「Lumada」です。日立グループはLumadaを基軸として社会イノベーション事業を拡大し、日本政府が提唱する安全、安心、快適でサステナブルな次世代デジタル社会「Society5.0」の実現に貢献してまいります。

Society5.0における最大の課題が情報セキュリティであることも広く認識されています。デジタル技術の進化は日々加速しており、これと同期するかのように情報セキュリティに対する脅威もかつてないレベルに増大しています。情報搾取、標的型メール、フェイクニュースやネット世論操作、重要なインフラ設備の被害など、サイバー攻撃の巧妙化と多様化はデジタル社会の信頼を根底から揺るがす深刻な脅威です。

日立グループにおいても、2017年5月にワーム型「ランサムウェア」のサイバー攻撃により、メールシステムをはじめとする社内システムの一部が被害を受けました。日立グループではこの経験をもとに情報セキュリティ体制の更なる強化を図りました。CISO（Chief Information Security Officer）を新たに設置し、CISOを中心とする情報セキュリティのグローバルなガバナンス体制を同年10月に運用開始しています。

2018年3月に日本経済団体連合会が「経団連サイバーセキュリティ経営宣言」を発表しました。本宣言では、価値創造とリスクマネジメントの両面からサイバーセキュリティ対策に努めることが経営の重要課題であると述べています。日立グループもこの理念を共有して情報セキュリティ強化に取り組んでいます。経営視点で策定した「情報セキュリティ方針」のもと、規則と体制の整備、一般従業員やセキュリティ専門職への教育、監査によるモニタリング、IT技術を活用した安全対策など、情報セキュリティのPDCAをグローバルで回しています。

情報セキュリティでは産学官の連携が必須です。日立グループは今回のランサムウェア被害の経緯や教訓といった知見を社外にも発信するよう努めました。今後も日立インシデントレスポンスチームを中心に日立グループ内で対策事例を蓄積するとともに、官民が連携したさまざまな取り組みの中でノウハウの共有を進めます。社会イノベーション事業の柱である協創の精神を情報セキュリティでも発揮し、Society5.0における信頼性の確保に貢献してまいります。

本報告書が日立グループの情報セキュリティ活動をご理解頂く上での一助となり、少しでも皆様のお役に立てば幸いです。

株式会社日立製作所
執行役副社長　CISO
小島 啓二

情報セキュリティ報告書

INDEX

〈本報告書の概要〉

●報告範囲・期間：2017年度までの日立グループにおける情報セキュリティの取り組み
●報告書の発行時期：2018年9月発行

サイバー攻撃事案の教訓と社内堅牢化の取り組み

日立グループでは、2017年5月にWannaCryと呼ばれるワーム型ウイルスによるサイバー攻撃を受け、社内システムが停止し、社内外に影響を与えた。IoT時代を迎え、増加するサイバーセキュリティの脅威へ対応すべく、情報セキュリティガバナンスを最も重要な経営課題として取り組むこととなった。2017年10月からCISOを中心としたセキュリティ統括専門組織を設置し、マネジメント/テクニカル面で社内の堅牢化を推進している。

1.はじめに

日立グループでは、ラピッドサイバー攻撃のような新たな脅威に対し、情報セキュリティを最も重要な経営課題の一つと位置づけガバナンス、テクニカルの両面から、日立グループにおけるサイバー攻撃に対する堅牢化の活動を推進しています。

2.サイバー攻撃事案の振り返り

2.1　サイバー攻撃の概要

2017年5月12日WannaCryと呼ばれるワーム型ランサムウェアが、欧州から世界中へ感染拡大しました。

本ウイルスはWindowsの脆弱性を悪用して、自分自身を他の脆弱なWindowsシステムにネットワークを経由して拡散します。また感染したシステムはファイルを暗号化され、その暗号解除の鍵と引き換えに金銭を要求する脅迫文が表示されます。日立グループでも欧州の現地法人の検査機器から、社内ネットワークのサーバ等に次々と感染しグローバルで被害が及びました。

2.2　影響範囲

影響範囲は、社内ネットワークに接続されている機器である業務システムサーバ、OA用PCなど情報システム部門が管理しているものから、工場にある製造･生産システム、制御装置や倉庫システム、ファシリティの入退管理システムなど多種にわたりました。図1は、5月12日からの社外へのファイヤーウォールにおけるWannaCryの拡散パケットの廃棄数を表したものです。20:00ごろに感染が始まり、2時間後の23:00にはほぼ飽和状態になり、脆弱性が対策されていない機器すべてに対しての拡散が終わりました。その後、アンチウイルスソフトによる検疫やパッチ適用により感染機器が減少し、パケット数は減少しました。

3.本サイバー攻撃事案から得た教訓

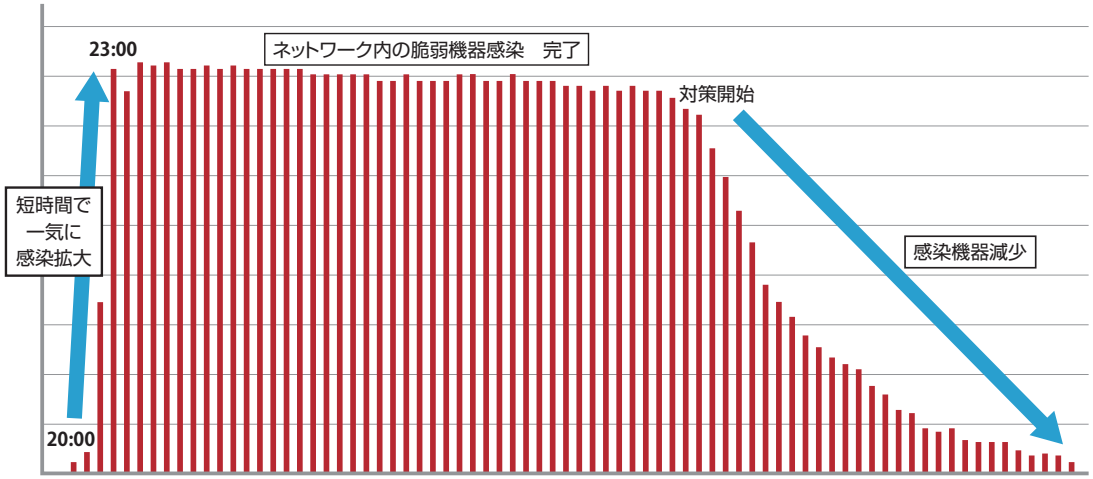
今回のサイバー攻撃事案から得た教訓は、4つあります。

1つめは、ネットワークの構成の在り方です。エンドポイントによるウイルス対策を前提として広域イーサネットによりセグメント化を排除した社内ネットワークは、ワーム型ウイルスに対してはエンドポイントが感染した場合一気に拡散してしまいます。また、エンドポイントのセキュリティ状況も把握できていないままネットワークに接続されていることも拡散の原因となりました。これらを改善するためには、セキュリティ側面と復旧を前提とした監視機能を盛り込んだネットワークとすることが重要です。

2つめは、グローバル化により24時間稼働の各サーバシステムにおいてセキュリティ対策不足が露呈しました。サーバの停止ができないために脆弱性があっても速やかにパッチを適用できない重要なシステムが特に被害を受けました。これはパッチ適用を特に根拠もなく「やらなくても大丈夫」という意識から、「やるのが当然」との意識へ変革し、企業全体のシステム運用において推進することが重要です。

3つめは、IoT機器へのセキュリティ対策の難しさです。今回の事案の感染元である検査機器もそうでしたが、組み込みWindowsであるにもかかわらず、パッチ適用が元々想定されていない機器が大多数であることや、導入する側もシステムをアップデートする意識がないことなど、今後の対応の難しさを改めて認識しました。一般的なOA機器

図1. WannaCryの感染速度 >>



と異なり、アンチウイルスもなくパッチを適用できずにウイルス感染する場合も想定し、予めネットワーク等で対策をすることが必要です。

4つめは、災害に対するIT-BCPとサイバー攻撃に対するIT-BCPは全く異なることです。震災をはじめとする災害対策として、速やかに業務を再開するためのバックアップのため常に遠隔地にデータを同期していますが、ランサムウェア感染により暗号化されたファイルも同期しバックアップデータも破壊されたことで復旧に時間を要しました。ランサムウェアのようなデータ破壊を想定すると、復旧のために必要なバックアップの考え方も見直しが必要です。また、災害時と同様にサイバー攻撃に対する事業継続計画(BCP)においても、人命確保・事業復旧を最優先に考えた行動をとることが必要です。

インシデント対応を行う際には、日頃から最悪のシナリオを考え、大規模な被害につながる可能性を常に念頭において対処しなければなりません。これらに対応するために、想定される攻撃シナリオに則った手順書の整備、トレーニング、現場力の向上が重要です。

これらの教訓から、サイバー攻撃に対する日立グループの堅牢化のため、ガバナンス側面では図2の通り6つの要素に焦点をあて、その推進に当たってはグループ横断での情報セキュリティ専門部門の設置を行い、セキュリティガバナンス体制の強化を図りました。

図2. ガバナンス側面の取り組み >>

1. **サイバー攻撃を想定したBCP設計**
   災害に加え、サイバー観点・グローバル観点を設計
2. **事業リスク分析に基づいたITでの対策**
   情報資産の重み付けを意識したITでの対策
3. **パッチマネジメントにおけるセキュリティパッチ強制適用**
   IoT機器、物理セキュリティほか、現場機器もすべて管理できる体制構築
4. **IT責任者の管理範囲・権限の見直しによる一元管理体制構築**
5. **セキュリティマネジメントのグローバルガバナンス**
   各国のリージョンを含めた体制再検討
6. **IoTセキュリティガイドラインの制定**

➡ **グループ横断での情報セキュリティ専門部門の設置**

4.セキュリティガバナンス体制の強化

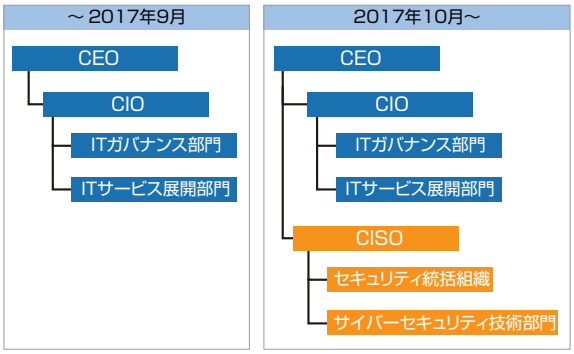
新しいサイバー攻撃等脅威の増加、IoTやクラウド等の事業領域の拡大等から情報セキュリティガバナンスを最も重要な経営課題の一つと位置づけ、2017/10から日立グループ全体の情報セキュリティガバナンスを一括して推進するため、CIOが兼務していた情報セキュリティの責任を分離しCISO(Chief Information Security Officer)を設置し、その配下に日立グループ全体のセキュリティを統括するための専門組織を設置しました。

これによりIT統制の一部であったセキュリティ統制機能を明確に分離し、グループ全体のガバナンス体制を確立しました。

統括組織では、情報・サイバーセキュリティのリスクに対する経営インパクト分析と対策状況の経営会議への答申および実行指示による継続的改善を役割としています。また、有事においては日立グループ全体に影響を及ぼす事案へのシステム停止判断と提言を行います。専門組織内には、SOC(Security Operation Center)による24時間365日のサイバー攻撃の監視、HIRT(Hitachi Incident Response Team)によるインシデント対応の強化を図っています。

図4のように、平時のPDCA活動、有事の緊急体制を整備しました。事業影響があるサイバー攻撃においてはコーポレート全体で緊急対策本部を立ち上げ、各社のサイバーセキュリティ部門と連携し対応を進めます。各コーポレート部門は緊急対策本部として統括組織と一体となってそれぞれ定められた対応を実施します(対策指示・状況把握、警察、マスコミ、省庁等の社外対応など)。

図3. CISOの体制と役割 >>



【CISO/セキュリティ統括組織の役割】

a) サイバー/情報セキュリティマネジメントの継続的実行

b) 日立グループ全体に影響を及ぼす事案へのシステム停止判断と提言

c) 経営インパクト、残存リスクへの対策の日立経営会議へ定期的な答申および実行

5. テクニカル面の強化

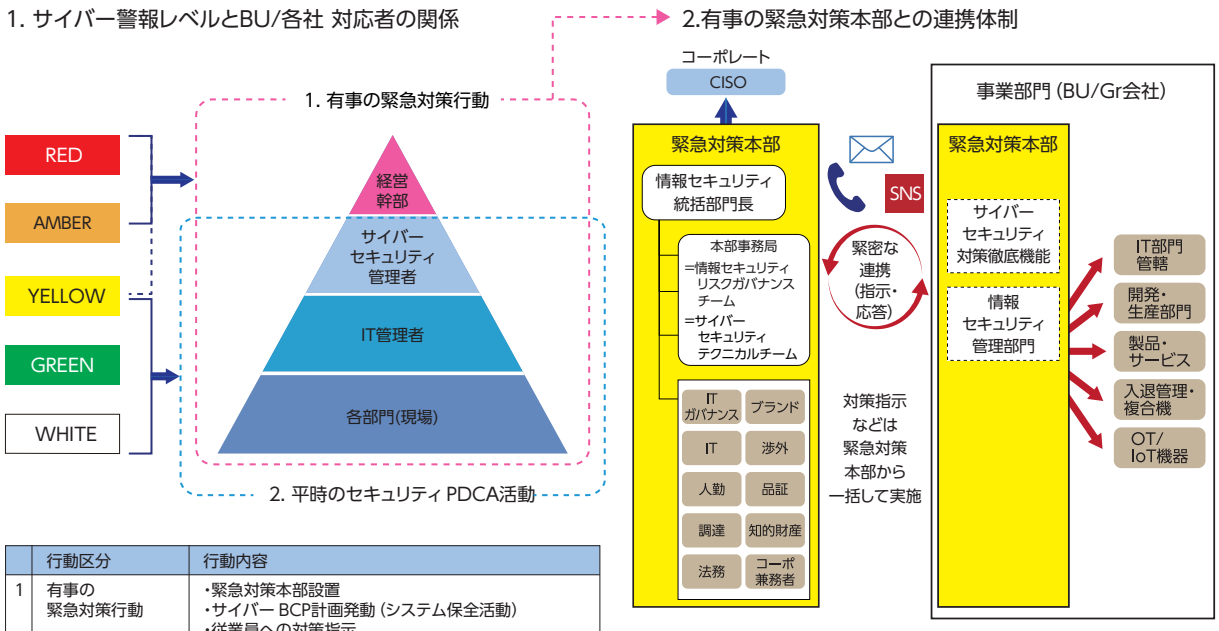
ガバナンス体制の強化と並行し、攻撃の早期検知と迅速な対処の実現に向け、監視およびインシデント対応についてテクニカル面からの強化も進めています。WannaCryの発生以降、亜種による攻撃にも備える必要があり、強化は複数のフェーズに分けて段階的に、かつ着実に進められるよう計画しました。

5.1. 堅牢化Iの取り組み

堅牢化Iでは、即効性のある施策を優先し、既存の運用をベースとして検知の早期化、判断と対処の迅速化に取り組みました。社内ネットワークや業務システムは、それぞれを担当する部署によって自律的に運用管理されてきたため、その構成や詳細について監視側で充分に把握しておらず、運用目的で取得している各種ログについては監視対象外としていました。しかしながら、フラットな構造の社内ネットワークでは監視ポイントを1つでも増やすことが早期検知につながるため、各部署管理の機器やシステムを棚卸しすることで、どこに何があるのか整理し、取得可能なログを確認し、検知に有用なものは新たに監視対象へと加え、検知の早期化を実現しました。また、近年は脅威の変化が激しく、監視業務もそれに合わせて柔軟な対応が求められます。これまでの監視側で準備している運用手順書は、確認や対策の共通項目だけを詳細化した断片的なものであり、対応者の知見を前提とした抽象的なものとなっていました。そうした知見を持った対応者が不在の際にWannaCryのような緊急事態が発生すると、対処までに時間を要し、被害が拡大することが想定されます。そこで、緊急時の対応手順を見直し、一定の前提知識があれば、判断と対処を迷うことなく迅速に進めることのできる手順書を整備しました。

また、従来は国内向けの標的型攻撃に監視の重点を置いていたことから、国内外の対応を区別しました。しかし、今回のWannaCry事案は、国外で発生したインシデントが国内に重大な被害を及ぼすという事象でした。そのため、これまで国内向けに実施してきた対応については国外も想定するものとし、危険度の高い事案については迅速に対応ができるよう、グローバルに24時間365日の受け付けと対応ができる体制を整備しました。

図4. サイバー警報と緊急対策本部の連絡体制 >>



	行動区分	行動内容
1	有事の緊急対策行動	・緊急対策本部設置 ・サイバー BCP計画発動 (システム保全活動) ・従業員への対策指示
2	平時のセキュリティPDCA活動	・製品・サービス、開発・生産、OT/IoT機器に対するセキュリティマネジメントサイクルPDCAの実行 ・脆弱性対策 ・堅牢化計画推進 (堅牢化施策の推進、残存リスク把握、事業インパクトの把握→経営幹部の報告) ・従業員へのセキュリティ向上、啓蒙活動

サイバー BCPの発動が必要となる有事はコーポレート全体で緊急対策本部を立ち上げ、BU/各社のサイバーセキュリティ対策徹底機能と連携し対応を進める。
また各コーポレート部門は緊急対策本部にてそれぞれ定められた対応を実施する。

5.2. 堅牢化Ⅱの取り組み

堅牢化Ⅱではセキュリティ監視の強化に取り組みました。

まず、更なる監視強化のため、監視基盤の拡張について検討しました。従来からある社内独自の監視基盤拡張も検討しましたが、国内だけではなくグローバルでの監視強化を早期にかつコスト面も考慮しながら実現させる必要がありました。そこで、各社のMSS（Managed Security Service）をベースに選定を行った結果、セキュリティ監視だけではなくインシデント発生時のIR（Incident Response）までサービスとして提供可能な日立グループのMSSを採用しました。

次に、グローバルでの監視強化実現に向け、対象とするシステム、およびネットワークの監視ポイントを定め、グローバルの各システムおよびネットワークデバイスのログの連携・監視を実施するための調整を進めました。監視対象拠点としては日本、日立ヨーロッパ社はもちろん日立アメリカ社、日立アジア社、日立中国社等が対象となります。

監視の仕組みとしては、各監視対象拠点のシステムおよびネットワークデバイスのログを、MSSの監視基盤に集約し相関分析を実施します。欧州のGDPR（一般データ保護規則）のように欧州域外に個人情報を含むデータを移転することができないといった規則・法律が拠点ごとにある場合には、相関分析を拠点内に限定し、ログをMSSの監視基盤に集約し分析・監視することで、日立グループへのサイバー攻撃をこれまでよりも早期に検知し、インシデントレスポンスによる対策・復旧をより迅速に行うことが可能となりました。

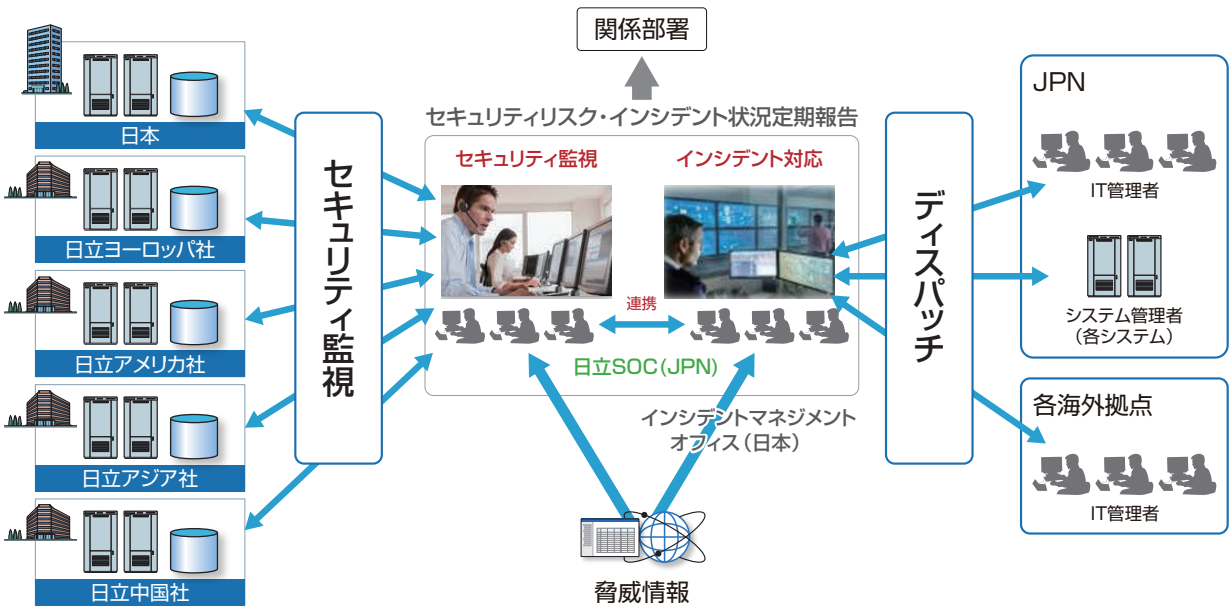
今後の取り組みとして、現在SOCでは24時間365日の監視を実施していますが、拠点ごとにIT責任者やIT管理者の運用が異なったり、24時間365日の対応ができなかったりする拠点もあります。

また、時差によってもグローバルでの対応に遅れやずれが発生する可能性があり、インシデント発生時の初動対応から対策までを迅速に実施することで、サイバー攻撃に対する被害を最小限に抑えるために継続して取り組んでいきます。

5. おわりに

サイバー事案の教訓から社内堅牢化は、着手が容易なOAで利用するIT系から始めていますが、IoT・制御システムも含む社内ネットワーク、クラウド環境あって直接的/間接的に接続するすべての機器を対象とし、製品・サービスの事業領域、開発・生産等の社内設備を含めた(国内・海外)すべてに対する日立グループにおけるすべてのセキュリティリスクのマネジメント活動を拡大していきます。

図5. グローバルでのセキュリティ監視強化 >>



情報セキュリティガバナンスの基本的な考え方

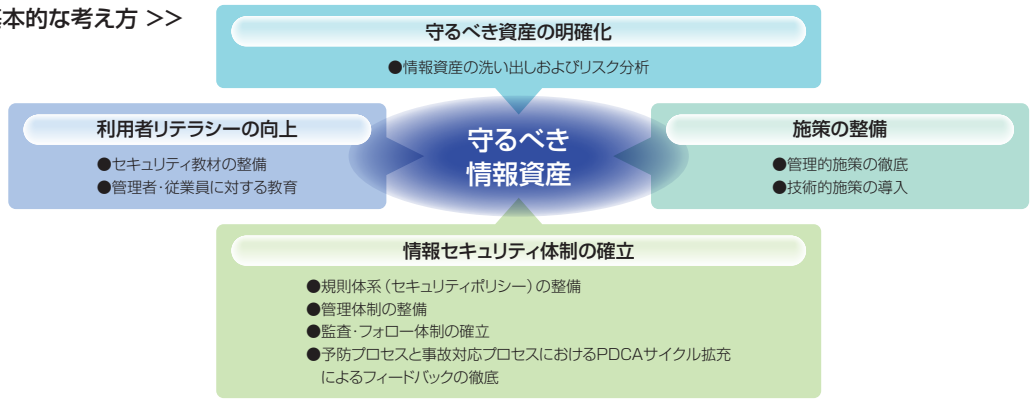
情報セキュリティガバナンスの取り組み方針

日立は、安心・安全な社会インフラシステムを提供する事業運営において、お客様からお預かりした情報資産を安全に管理するため、情報セキュリティへの取り組みを重要視しています。グループ共通の情報セキュリティへの取り組み方針を定め、情報セキュリティ強化活動を推進しています。

情報セキュリティ取り組みの考え方

情報セキュリティへの取り組みの考え方は、①情報セキュリティ体制の確立、②守るべき資産の明確化、③利用者リテラシーの向上、④各種セキュリティ施策の整備の4つの視点からなり、各々に関する実施事項を着実に取り組んでいます。なかでも、予防体制整備と事故発生時の迅速な対応、社員の倫理観とセキュリティ意識の向上、に関しては特に重視して取り組んでいます。また、日立製作所の主導により、情報セキュリティマネジメントのPDCA（継続的改善活動）を推進し、グループ全体でセキュリティレベルの向上に取り組んでいます。

情報資産保護の基本的な考え方 >>



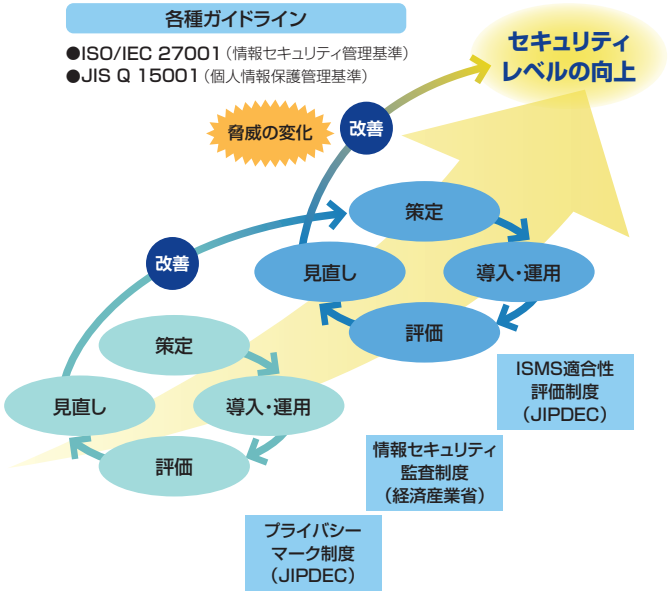
（1）予防体制の整備と事故発生時の迅速な対応

守るべき情報資産を明確にし、脆弱性評価とリスク分析に基づいて情報漏えい防止施策を実施しています。事故は「起きるかもしれない」という考え方を一歩進めて、「必ず起こるものだ」という前提に立って、緊急時のマニュアルを作成し、対応しています。

（2）社員の倫理観とセキュリティ意識の向上

管理者向け、担当者向けなど階層別のカリキュラムを用意し、eラーニングによる全員教育などを通じて倫理観とセキュリティ意識の向上を図るとともに、監査を通じて問題点の早期発見と改善に取り組んでいます。

セキュリティレベル向上のためのPDCAサイクル >>



情報セキュリティマネジメントシステム

情報セキュリティ推進体制とマネジメントサイクル

日立の情報セキュリティに関する方針、情報セキュリティの推進体制、情報セキュリティに関する規則、情報セキュリティマネジメントサイクルなどについて紹介します。

情報セキュリティ方針

日立は、日本を代表するグローバル企業として、サイバーセキュリティリスクを経営リスクの一つとして認識し組織全体の対応方針を組織の内外に宣言できるよう、企業の経営方針と整合を取り、サイバーセキュリティリスクマネジメントを考慮した情報セキュリティ方針および関連規則を定め、情報セキュリティの確保に努めています。

本方針に基づいて、サイバーセキュリティへの対策の強化、ヒューマンエラーによる情報漏えいの防止、マイナンバーなどの個人情報の保護等、あらゆる事業活動の局面に対応する情報セキュリティ施策を実施しています。

情報セキュリティ方針 >>

1. 情報セキュリティ管理規則の策定及び継続的改善
当社は、情報セキュリティの取り組みを、経営並びに事業における重要課題のひとつと認識し、法令及びその他の規範に準拠・適合した情報セキュリティ管理規則を策定する。更に、当社役員を中心とした全社における情報セキュリティ管理体制を確立し、これを着実に実施する。加えて組織的、人的、物理的及び技術的な情報セキュリティを維持し、継続的に改善していく。

2. 情報資産の保護と継続的管理
当社は、当社の扱う情報資産の機密性、完全性及び可用性に対する脅威から情報資産を適切に保護するため、安全な管理策を講じる。また、事業継続のために、適切な管理措置を講じる。

3. 法令・規範の遵守
当社は、情報セキュリティに関する法令及びその他の規範を遵守する。また、当社の情報セキュリティ管理規則を、これらの法令及びその他の規範に適合させる。また、これらに違反した場合には、所員就業規則等に照らして、然るべき処分を行う。

4. 教育・訓練
当社は、当社役員及び従業員へ情報セキュリティの意識向上を図るとともに、情報セキュリティに関する教育・訓練を行う。

5. 事故発生予防と発生時の対応
当社は、情報セキュリティ事故の防止に努めるとともに、万一、事故が発生した場合には、再発防止策を含む適切な対策を速やかに講じる。

6. 企業集団における業務の適正化確保
当社は、前第1項から第5項に従い、当社及び当社グループ会社から成る企業集団における業務の適正を確保するための体制の構築に努める。

情報セキュリティ推進体制

社長が、情報セキュリティについて責任と権限を有する情報セキュリティ統括責任者と、情報セキュリティ監査について責任と権限を有する情報セキュリティ監査責任者を任命します。

情報セキュリティ統括責任者は、情報セキュリティ委員会を組織し、情報セキュリティに関する方針、教育計画、各種施策を決定します。

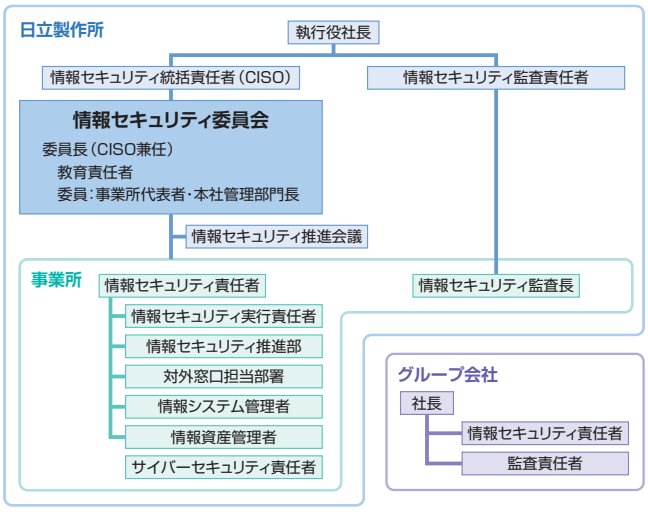
情報セキュリティ委員会の決定事項は、全事業所実務者が出席する情報セキュリティ推進会議を通じて、各事業所に徹底されます。

事業所では、事業所長が情報セキュリティ責任者を務めます。

また情報セキュリティ推進部署を設置し、事業所全体の個人情報保護、情報セキュリティ、機密情報管理、入退管理、外注管理を一元的に処理するとともに、事業所の従業員に対して情報管理意識を徹底する教育を行います。また各部署には情報資産管理者を置き、情報資産の取り扱いに関する責任体制を整えています。

グループ会社においても同様の組織を設け、互いに連携して横断的な情報セキュリティを推進しています。

情報セキュリティ推進体制 >>



CISO：Chief Information Security Officer

情報セキュリティマネジメントシステム

情報セキュリティ規則

情報セキュリティ方針に基づき、下表の規則を定めています。
また、グループ会社も同等の規則を定め、情報セキュリティの推進をしています。

情報セキュリティ関連規則 >>

分類	規則名	内　容
基本規則	情報セキュリティマネジメント総則	「日立製作所企業行動基準」に基づき、情報セキュリティマネジメントシステムの策定、実施、維持、継続的な改善に関する基本的な遵守事項を定め、個人情報を含む当社の情報資産における機密性、完全性、可用性を確保し、保護することを目的としています
	情報及び情報機器の取扱い総則	当社における情報および情報機器の取り扱いと管理に関する基本的な事項を定め、情報の安全な活用を促進するとともに、規則を遵守することによって紙等の媒体や情報システム等で利用される情報全般の漏えい、情報の不正利用による事故を防止することを目的としています
	機密情報管理規則	「日立製作所企業行動基準」に基づき、機密情報の取り扱いに関して必要な事項を定め、機密の保全を図ることを目的としています
個別規則	Webサイト及び情報開示に関する規則	Webサイトにおいて、情報の開示および利用を正しく行うために遵守すべき事項を定め、お客様や従業員等の利用者が安心かつ効率的に情報を利用できる環境を提供することを目的としています
	情報セキュリティシステム管理規則	「情報セキュリティマネジメント総則」に基づき、情報システムに関し管理すべき事項の基本を定め、情報セキュリティの確保を図ることを目的としています
	入退及び立ち入り制限区域管理規則	入退管理に関する原則および構内立入制限、または禁止区域の指定とその管理、運用に関して必要な事項を定め、機密情報の保全を図ることを目的としています
個人情報管理	個人情報管理規則	個人情報の取り扱いに関する法令、国が定める指針その他の規範等に従い、個人情報を適切に保護することに関して遵守する事項を定め、本人の権利・利益の保護を図るとともに、事業上の損失、社会的信用の失墜を防ぐことを目的としています運営管理体制の整備、管理規則の実践・遵守等、個人情報保護に関する責務をまっとうするために必要な事項および手続等について定めています
	個人情報取扱業務委託規準	「個人情報管理規則」に規定する個人情報取扱業務を社外の事業者に委託する場合の具体的な手順を定め、保有する個人情報の外部漏えい、改ざん、紛失、消失の防止を行うことにより、個人情報の適切な管理・保護を図ることを目的としています

●機密情報漏えい防止3原則

日立は機密情報漏えい防止3原則を制定し、自社およびお客様の情報の取り扱いに十分な注意を払い、情報漏えい防止に努めています。

原則1：機密情報については、原則、社外へ持ち出してはならない
原則2：業務の必要性により、機密情報を社外へ持ち出す場合は、必ず情報資産管理者の承認を得なければならない
原則3：業務の必要性により、機密情報を社外へ持ち出す場合は、必要かつ適切な情報漏えい対策を施さなければならない

●基本規則

「情報セキュリティマネジメント総則」は、情報セキュリティマネジメントシステムの策定、実施、維持、継続的な改善に関する基本的な遵守事項を定めています。「情報および情報機器の取扱い総則」は、情報全般の漏えい、情報の不正利用による事故を防止することを目的に、情報および情報機器の取り扱いと管理に関する基本的な事項を定めています。

「機密情報管理規則」は、機密情報の保全に関する取り扱いを定めています。

●個別規則

「Webサイト及び情報開示に関する規則」は、Webサイトにおいて、情報の開示および利用を正しく行うために遵守すべき事項を定めています。

「情報セキュリティシステム管理規則」は、情報システムにおいてセキュリティを確保する手段について定めています。

「入退及び立ち入り制限区域管理規則」は、建物への入退管理に関する規定など、物理的なセキュリティの確保について定めています。

●個人情報の取り扱い

個人情報に関しては、個人情報保護法より一段高いレベルの管理を行うためにJIS規格「個人情報保護マネジメントシステム－要求事項」（JIS Q 15001）相当の規則としています。

●情報セキュリティ監査

情報セキュリティ監査は、社長に任命された情報セキュリティ監査責任者の指揮のもと、年1回実施します。

情報セキュリティ監査では、以下のような事項を確認します。

・情報セキュリティ規則と情報資産の管理および情報セキュリティ対策との合致状況
・個人情報保護法およびJIS Q 15001と個人情報管理体制の合致状況
・個人情報保護マネジメントシステムとJIS Q 15001の合致状況

またグループ会社に対しても年に1度、情報セキュリティ監査を実施するよう要請しています。

情報セキュリティマネジメントシステム

情報セキュリティマネジメントサイクル

情報セキュリティマネジメントは、サイバーセキュリティ対策をPDCA（Plan-Do-Check-Action）として実施するフレームワークを構築することで計画を確実に実施し改善していきます。

Planでは、情報セキュリティ方針、情報セキュリティ施策の策定、情報セキュリティ教育計画、情報セキュリティ監査計画を立案します。

Doでは、セキュリティ施策の社内への展開と運用を行います。

情報セキュリティ教育を実施し、セキュリティ施策の周知徹底を図ります。

情報セキュリティに関する推進会議を開催し、各事業所にセキュリティに関する情報提供と施策の実施状況をフィードバックします。

Checkでは、定期的なセキュリティ運用状況の点検、監査計画に則った監査、経営者によるマネジメントレビューを実施します。

また、経営環境の変化、社内外から寄せられた意見などに基づき、代表者によるマネジメントシステムの見直しを行っています。

Actionでは、監査やマネジメントシステムの見直し、社内外から寄せられた意見などに基づいて是正措置を講じます。

情報セキュリティ監査

情報セキュリティ監査は、社長に任命された情報セキュリティ監査責任者の指揮のもと、年1回実施します。

情報セキュリティ監査では、以下のような事項を確認します。

- 情報セキュリティ規則と情報資産の管理および情報セキュリティ対策との合致状況
- 個人情報保護法およびJIS Q 15001：2006と個人情報管理体制の合致状況
- 個人情報保護マネジメントシステムとJIS Q 15001：2006の合致状況

またグループ会社に対しても年に1度、情報セキュリティ監査を実施するよう要請しています。

事業におけるセキュリティリスクの顕在化

グローバルに事業を展開する日立グループでは、各国/地域に多くの拠点を構えており、本社機能、営業所、サービスや製造拠点などさまざまな事業形態があります。このような環境下において組織内のネットワークの環境や設備、IT機器などの設置や利用環境も多様である一方で、外部とのネットワーク接続やリムーバブルメディア（USBメモリ）などを経由した外部とのコミュニケーションを行うため、標的型攻撃や、マルウェア感染など事業上のセキュリティリスクへの備えが重要となってきます。

日立グループでは、全社共通的なセキュリティ関連規則、基準類を制定し、組織としてのセキュリティポリシーを確立、各拠点で運用しているところです。しかしながら、我々の事業環境を取り巻くセキュリティ上の脅威は時代とともに変化しており、当初は想定されていなかったり、これまで組織が認識できていないセキュリティ上の残存リスクが顕在化しつつあります。組織のセキュリティを維持、底上げするためには以下の課題に対して取り組んでいく必要があります。

① 現場のセキュリティ対策状況の実効性の確認
② 環境の変化に応じた責任分界点の明確化

情報セキュリティマネジメントシステム

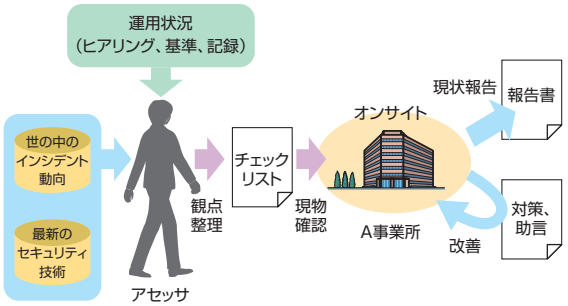
オンサイトセキュリティリスクアセスメントによるリスクベースの対策強化への取り組み

日立グループでは、これまでも機密情報や個人情報等について、高いレベルでのセキュリティ対策、管理を行っていますが、事業環境を取り巻く環境の変化に伴うリスクに対応するために、社内のIT施策を担うIT統括部門から独立したセキュリティ専門家チームによるアセスメント体制を強化しています。具体的には日立グループの各ビジネスユニット、関連する各社の現場を訪問し、次の視点での強化施策に積極的に取り組んでいます。

①日立グループのネットワークにつながるすべての製品や社内設備を対象に、セキュリティ専門家チームが最新動向を踏まえたアセスメントを行う

②セキュリティ上のリスクとなる課題の抽出と解決に向けた現場への有効となる対策の提言

図1 オンサイトリスクアセスメント >>



情報セキュリティに関する教育

●情報セキュリティ教育

情報セキュリティを継続して守っていくためには、一人ひとりが日々の情報を取り扱ううえで必要な知識を身につけ、高い意識をもつことが重要です。

そのため、全従業員に対し、下表に記載の役割に応じた階層別教育を設けて実施しています。

また、より専門的なセキュリティ人財育成するための当事者教育はP22に記載しています。

情報セキュリティに関する教育一覧 >>

	対象者	形　態	内　容
階層別教育（全員）	全員教育	eラーニング	個人情報保護、情報漏えい防止、機密情報管理に関する基礎を授ける教育
	管理職教育	セルフ学習 一部座学形式	個人情報保護、情報セキュリティ、機密情報管理について管理職として必要な知識を授ける教育
	新入社員教育	座学形式	情報セキュリティ、機密情報管理について新入社員として必要な知識を授ける教育
	情報セキュリティ担当者	座学形式 一部演習形式	情報セキュリティ、機密情報管理に関する詳細な知識教育。 事例を踏まえた実践演習
	個人情報保護担当者	座学形式 一部演習形式	個人情報保護（プライバシーマークレベル）に関する知識教育。 事例を踏まえた実践演習
	情報資産管理者	セルフ学習 一部座学形式	各部署で情報資産の管理責任者として行動するために必要な知識教育
当事者教育	情報システム担当者	座学形式 一部演習形式	ネットワークセキュリティ、セキュリティインシデント対応、 Webアプリケーションセキュリティ、社外公開サーバセキュリティに関する 情報システム担当者向けの教育

●標的型攻撃メール訓練教育

標的型攻撃メールによるサイバー攻撃の脅威が強まっていますが、従業員は万一攻撃を受けた場合、適切に対応できるよう一人ひとりの耐性をつけることが欠かせません。

日立では2012年よりグループ会社も含めて全従業員を対象とした標的型攻撃メール訓練教育を実施しています。実際に標的型攻撃メールを装った模擬メールを各人に送付して、不審メールとはどういうものか、受信した際にどのように対応すべきかなどについて、受信体験を通して対応力の強化を図っています。

●その他の支援

「機密情報の適切な管理・取扱い方」の要約版パンフレットを全従業員に配布し、機密情報管理に関する規則の周知を図っています。

サイバーセキュリティに対する脆弱性対策・インシデント対応への取り組み

日立グループにおけるCSIRT活動

日立インシデントレスポンスチーム(Hitachi Incident Response Team:HIRT)は、日立のサイバーセキュリティ対策活動を支援するCSIRT(Cyber security Incident Readiness/Response Team)組織です。セキュリティインシデントの発生を予防し、万一発生した場合は迅速に対処することにより、お客様や社会の安全・安心なネットワーク環境の実現に寄与します。

インシデントレスポンスチームとは

セキュリティインシデント(以下、インシデントと記す)とは、サイバーセキュリティに関係する人為的事象で、不正アクセス、サービス妨害行為、データの破壊などの行為(事象)を示します。

インシデントレスポンスチームは、組織間ならびに国際間の連携によって問題解決にあたるために、「技術的な視点で脅威を推し量り、伝達できること」「技術的な調整活動ができること」「技術面での対外的な協力ができること」という基本的な能力をもち、インシデントの予防(レディネス:事前対処)と解決(レスポンス:事後対処)を通じて、「インシデントオペレーション」を先導する組織です。

HIRTの活動モデル

HIRTの役割は、「脆弱性対策:サイバーセキュリティに脅威となる脆弱性を除去するための活動」と「インシデント対応:発生しているサイバー攻撃を回避ならびに解決するための活動」を通じて、「組織単体活動:自身の企業情報システムを対象とする『情報セキュリティへの取り組み』」と「組織連携活動:お客様の情報システムや制御システムを対象とする『製品・サービスのサイバーセキュリティ確保に向けた取り組み』」の視点から、日立のサイバーセキュリティ対策活動を支援していくことにあります。さらには、「次の脅威をキャッチアップする」過程の中で早期に対策の展開を図ることによって、安全・安心なインターネット社会の実現に寄与することにあります。

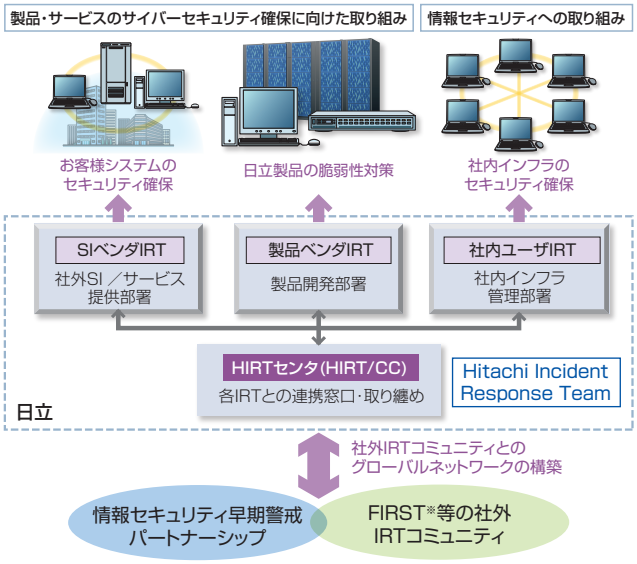
HIRTは、脆弱性対策とインシデント対応とを推進するために、下記のように、4つのIRT(Incident Response Team)という活動モデルを採用しています。4つのIRTとは、

(1)情報システムや制御システム関連製品を開発する側面(製品ベンダIRT)
(2)その製品を用いてシステムの構築やサービスを提供する側面〔SI(System Integration)ベンダIRT〕
(3)インターネットユーザーとして自身の企業情報システムを運用管理する側面(社内ユーザIRT)

の3つとともに、

(4)これらのIRT間の調整業務を行うHIRT/CC(HIRTセンタ)を設け、各IRTの役割を明確にしつつ、IRT間の連携を図る効率的かつ効果的なセキュリティ対策活動を推進するモデルです。

脆弱性対策、インシデント対応活動を支える4つのIRT >>



分　類	役　割
HIRT/CC※	該当部署:HIRTセンタ FIRST、JPCERT/CC※、CERT/CC※などの社外IRT組織との連携、SIベンダ・製品ベンダ・社内ユーザIRT間の連携を通して脆弱性対策とインシデント対応活動を推進する。
SIベンダIRT	該当部署:SI・サービス提供部署 公開された脆弱性について、社内システムと同様にお客様システムのセキュリティを確保するなど、お客様システムを対象とする脆弱性対策とインシデント対応活動を支援する。
製品ベンダIRT	該当部署:製品開発部署 公開された脆弱性について影響の有無を迅速に調査し、該当する問題について、修正プログラムを提供するなど、日立製品の脆弱性対策を支援する。
社内ユーザIRT	該当部署:社内インフラ提供部署 日立サイトが侵害活動の基点とならないよう脆弱性対策とインシデント対応活動の推進を支援する。

※HIRT/CC:HIRT Coordination Center
FIRST:Forum of Incident Response and Security Teams
JPCERT/CC:Japan Computer Emergency Response Team/Coordination Center
CERT/CC:CERT Coordination Center
SI:System Integration

サイバーセキュリティに対する脆弱性対策・インシデント対応への取り組み

HIRTセンタが推進する活動

HIRTセンタの活動には、組織内IRT活動として、制度面を先導する情報セキュリティ統括部門と、品質保証部門との協力による制度・技術両面でのサイバーセキュリティ対策の推進、各事業部・グループ会社への脆弱性対策ならびにインシデント対応の支援があります。また、日立の対外的なIRT窓口として、組織間のIRT連携によるサイバーセキュリティ対策を推進しています。

●組織内IRT活動

組織内IRT活動では、セキュリティ情報の収集や分析を通じて得られたノウハウを注意喚起やアドバイザリとして発行するとともに、各種ガイドラインや支援ツールの形で製品／サービス開発プロセスにフィードバックします。

(1)セキュリティ情報の収集・調査分析・展開

情報セキュリティ早期警戒パートナーシップ※1の推進などを通じて、脆弱性対策ならびにインシデント対応に関する情報やノウハウを組織内に展開しています。

※1 ソフトウェア製品およびWebサイトに関する脆弱性関連情報の円滑な流通、および 対策の普及を図るための、公的ルールに基づく官民の連携体制

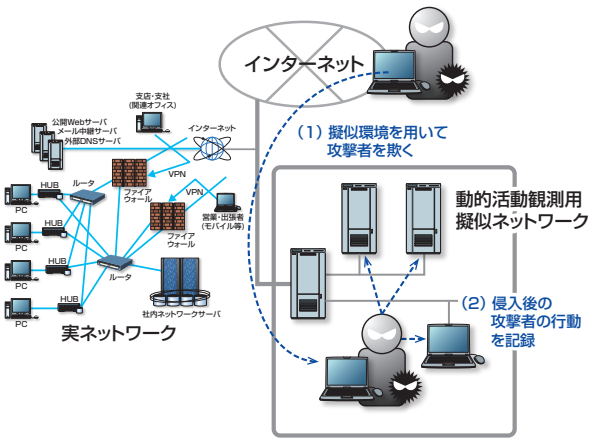
(2)研究活動基盤の整備

「次の脅威のキャッチアップ」と早期に対策展開を図るための技術として「動的活動観測」に取り組んでいます。動的活動観測は、標的型攻撃などのサイバー攻撃を調査するために構築した組織内ネットワークの擬似環境下で、侵入後の攻撃者の行動を記録し分析する観測手法です。

(3)製品・サービスのセキュリティ技術の向上

組織的なIRT活動能力の向上にむけ、情報システムならびに制御システム関連製品に対するセキュリティ施策の具体化、エキスパート人財への技術継承を推進しています。

攻撃者の行動を記録する動的活動観測システム >>



また、実践的な社内セキュリティ啓発の一環として、標的型攻撃やランサムウェアなどのサイバー攻撃の疑似体験演習の開発にも取り組んでいます。

(4)分野別IRT活動の実践

分野ごとの背景や動向を踏まえた対応を具体化していくため、分野に特化したIRT活動の検討と整備を進めています。金融分野における先行的な取り組みとして、2012年10月に、HIRT-FIS※2を設置しました。

※2: HIRT-FIS: Financial Industry Information Systems HIRT

●組織間IRT活動

組織間IRT活動では、複数のIRTが協調して、新たな脅威に立ち向かうための組織間連携、互いのIRT活動の改善に寄与できる協力関係の構築を推進しています。

(1)IRT活動の国内連携の強化

日本シーサート協議会活動を活用して、情報収集において知り得た脆弱性やインシデント情報を他加盟組織のPoC(Point of Contact)に通知するなど、連携網の整備に努めています。また、JPCERTコーディネーションセンターと独立行政法人情報処理推進機構(IPA)が共同運営するJVN※3を用いた情報利活用基盤の整備を支援しています。

※3 JVN:Japan Vulnerability Notes（脆弱性対策情報ポータルサイト）

(2) IRT活動の海外連携の強化

FIRST※4を通じた活動を活用した海外IRT組織ならびに海外製品ベンダIRTとの連携体制の整備、脅威情報構造化記述形式STIX※5、米国国土安全保障省のAIS※6などを用いた情報利活用基盤の整備を推進しています。

※4 FIRST: Forum of Incident Response and Security Teams
※5 STIX: Structured Threat Information Expression
※6 AIS: Automated Indicator Sharing

(3)研究活動基盤の整備

マルウェア対策研究人財育成ワークショップなど学術系研究活動への参画を通じて、人財育成の場の醸成、専門知識を備えた研究者や実務者の育成を推進しています。

参考情報 >>

■Hitachi Incident Response Team

http://www.hitachi.co.jp/hirt/
http://www.hitachi.com/hirt/

情報セキュリティに対する技術面での取り組み

ITによる情報セキュリティ施策

日立は、多発するサイバー攻撃、マルウェア感染、不正アクセス、情報漏えい等の防止に総合的に取り組み、新たな脅威に対して、日々先進的なITセキュリティ施策を追求しています。

安心・安全な日立のITセキュリティ

国内外900社を超える連結会社間で、グループ従業員が安全で安心して情報共有できるセキュアな日立グループ共通ITインフラ環境を構築・管理しています。ITインフラ環境を統一共通化することで、セキュリティ施策の統一および有事の際の迅速な対応を実現しています。

また、日立グループ製品を積極的に導入することで、その結果を製品設計部門にフィードバックし、日立グループの更なる醸成に役立てています。

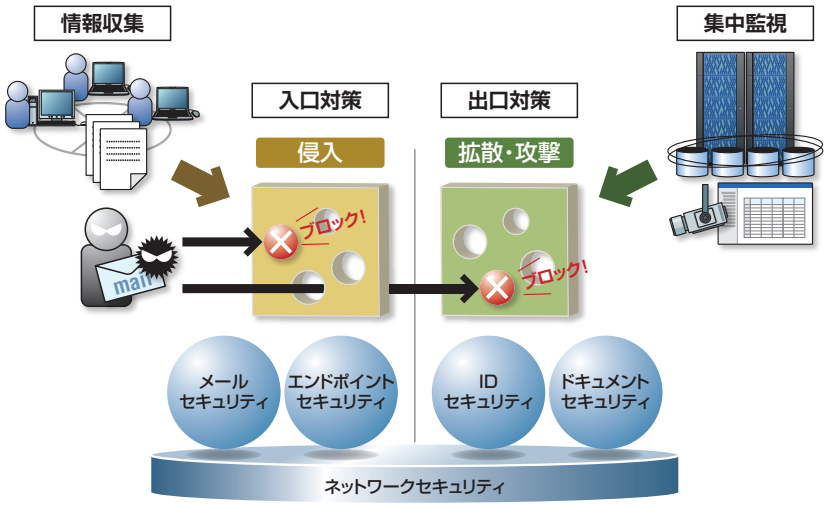
日立のITセキュリティ体系とサイバー攻撃に対応した多層防御

日立のITによるセキュリティ体系は、ネットワークセキュリティ（インターネットなどの社外接続、プロキシ、リモートアクセス）、メールセキュリティ、IDセキュリティなどからなり、それぞれ各種施策を整備し、堅牢な対策を講じています。

また、昨今の標的型攻撃に代表されるサイバー攻撃への対策は、攻撃者の進化に遅れることなく、継続的に実施することが重要です。

これらを実現するため、以下の考え方にのっとり、各種対策に取り組んでいます。

- CSIRT活動によるインシデント情報の収集と活用
- 防御策の多層化（入口・出口対策）と重要情報の防御
- 被害を最小限に抑えるための集中監視による攻撃の把握と分析
- 迅速なインシデントオペレーションの実施
- サイバー攻撃対策の先進研究とセキュリティ対応人材の教育・育成



情報セキュリティに対する技術面での取り組み

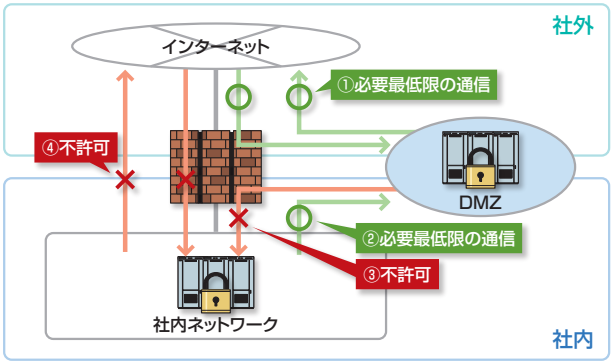
ネットワークセキュリティ

1. 社外接続

社外への情報公開や情報共有を目的に、社外ネットワークと社内ネットワークを接続する際は、その接続点にファイアウォールを設置し、DMZ※1を構成しています。これによって、社内外の直接的な通信を行うことができず、間接的な通信方式をとっています。

インターネット接続点では、IPS※2が不正アクセスを監視・遮断しています。また、社外に公開しているすべてのサーバおよびネットワーク機器に対して定期的にセキュリティ監査を実施し、セキュリティ上の問題がないか確認しています。

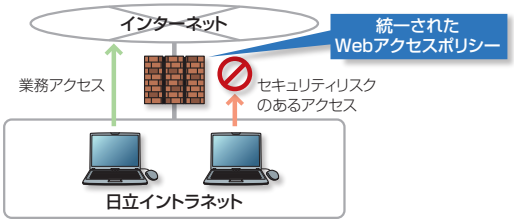
※1：DeMilitarized Zone　※2：Intrusion Prevention System



2. プロキシ

インターネットへの業務アクセスにおけるリスク低減策としてゲートウェイで次の対策を実施しています。

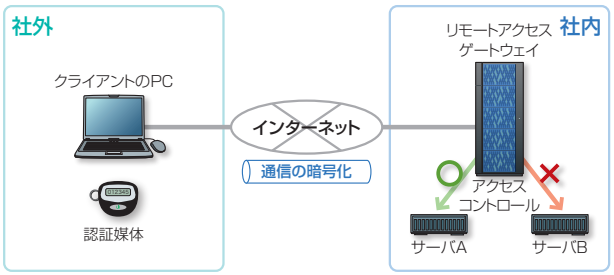
- ID/パスワード認証による、利用者の限定とログ保存およびログ監視
- 画像認証による、ウイルスによる機械的な通信の防止
- 統一されたポリシーによる、URLフィルタリング
- Webウイルスチェック



3. リモートアクセス

ゲートウェイにおける以下の対策により、情報漏えいの防止に取り組んでいます。

- 2要素認証の実施（ID/パスワードに加え、認証媒体などによる認証）
- インターネットなどの区間での通信の暗号化
- サーバへのアクセスコントロール



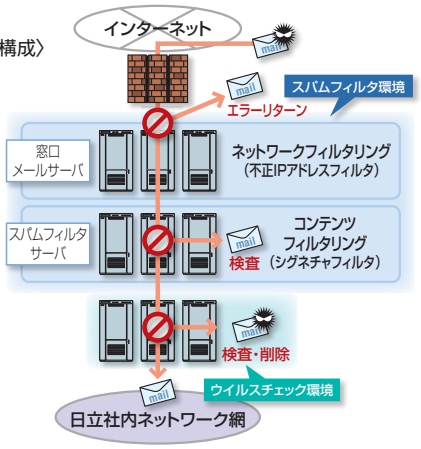
メールセキュリティ

メールについては、外部からの脅威と内部で発生する脅威に備えて対策を講じています。

1.外部からの脅威に対する対策

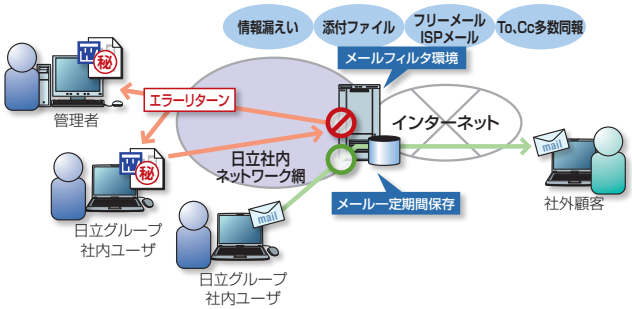
外部からの脅威については、①コンピュータウイルス侵入の脅威、②スパムメールの脅威の2つを考慮したメール配送構成としています。

〈スパムフィルタ、ウイルスチェック構成〉



2. 内部で生じる脅威に対する対策

内部で生じる脅威については、①コンピュータウイルス拡散の脅威、②情報漏えいの脅威を考慮し、メール配送上にメールフィルタサーバを設置し、問題のないメールのみを配送しています。



情報セキュリティに対する技術面での取り組み

サイバーセキュリティ対策

サイバー攻撃や各種セキュリティインシデントへ対応するために、日立では、自社内で運営するセキュリティオペレーションセンター（SOC:Security Operation Center）を設置し、セキュリティ監視およびインシデント対応の強化、推進を図っています。

セキュリティ監視・インシデント対応強化

標的型メール攻撃の高度化やDDoS（Distributed Denial of Service）攻撃など、近年、複雑化かつ巧妙化するサイバー攻撃により、企業や組織のセキュリティリスクが増大しています。このようなサイバー攻撃に対峙するためには、その脅威をいち早く発見し、被害拡大を防止することが重要です。

日立では、マルウェア感染や不正アクセスなどの脅威を早期に検知し、インシデント発生時の初動対応から対策までを迅速に実施し、サイバー攻撃に対する被害を最小限に抑えるための24時間365日体制のセキュリティオペレーションセンター（SOC）を2017年10月より設置し、セキュリティ監視・インシデント対応強化を図っています。

（1）セキュリティ監視

社内ネットワークでは監視ポイントを1つでも増やすことが早期検知につながるため、各部署管理の機器やシステムを棚卸しすることで、どこに何があるのか整理し、取得可能なログを確認し、検知に有用なものは新たに監視対象へと加えることで検知の早期化を実現しています。また、グローバルでの監視強化に向けて、対象とするシステムおよびネットワークの監視ポイントを定め、グローバルの各システムおよびネットワークデバイスのログの連携・監視を実施するログの統合監視・分析基盤の構築を行っています。

（2）インシデントレスポンス

インシデント発生に備えた対応手順、連絡体制を整備しており、発生時には、迅速に原因究明や影響範囲の特定、事態の収束を行います。また、インシデント対応から得られたノウハウを社内の各種セキュリティ施策にフィードバックし、再発防止を図る取り組みも実施しています。

HIRTとの連携による脅威情報の収集・潜在する脅威の発見

昨今のサイバー攻撃は、従来型のセキュリティソリューションでは検知困難、あるいは検知不可能なカスタム・マルウェアや高度な手法を使用しています。セキュリティオペレーションセンターでは、日立グループのCSIRTであるHIRTと連携し、マルウェアによる不正接続先の情報や不正アクセスの攻撃パターンなどの脅威インジケータの収集を行い、各種ログに脅威インジケータが存在するかを検査することによって、潜在する脅威の発見と、情報漏えいなどのリスクの低減につなげています。

情報セキュリティに対する技術面での取り組み

警戒情報の収集・分析・配信

日立製作所では、社内で利用している情報システムおよびお客様へ提供する製品・サービスのセキュリティを確保するための活動として、警戒情報の収集・分析・配信を行っています。

この活動は、グループ会社とも連携して推進しています。

(1) 脅威情報の収集

脅威情報の収集では、以下に示すようなWeb上に公開されている脆弱性情報・脅威情報に加え、日立システムズのSHIELD グローバルインテリジェンスサービスを活用して、国内・海外含めたセキュリティ情報の収集を行っています。

・IPA、JPCERT/CCなどの社外団体の発信サイト
・セキュリティ関連のニュースサイト
・各種セキュリティベンダのブログサイト

(2) 情報分析

収集した脆弱性情報・脅威情報については、情報元が公開している深刻度、CVSS基本値※などから攻撃成功の可能性、社内システムでの利用状況などを考慮し、配信対象の選定・5段階の警戒レベルの判定を行っています。

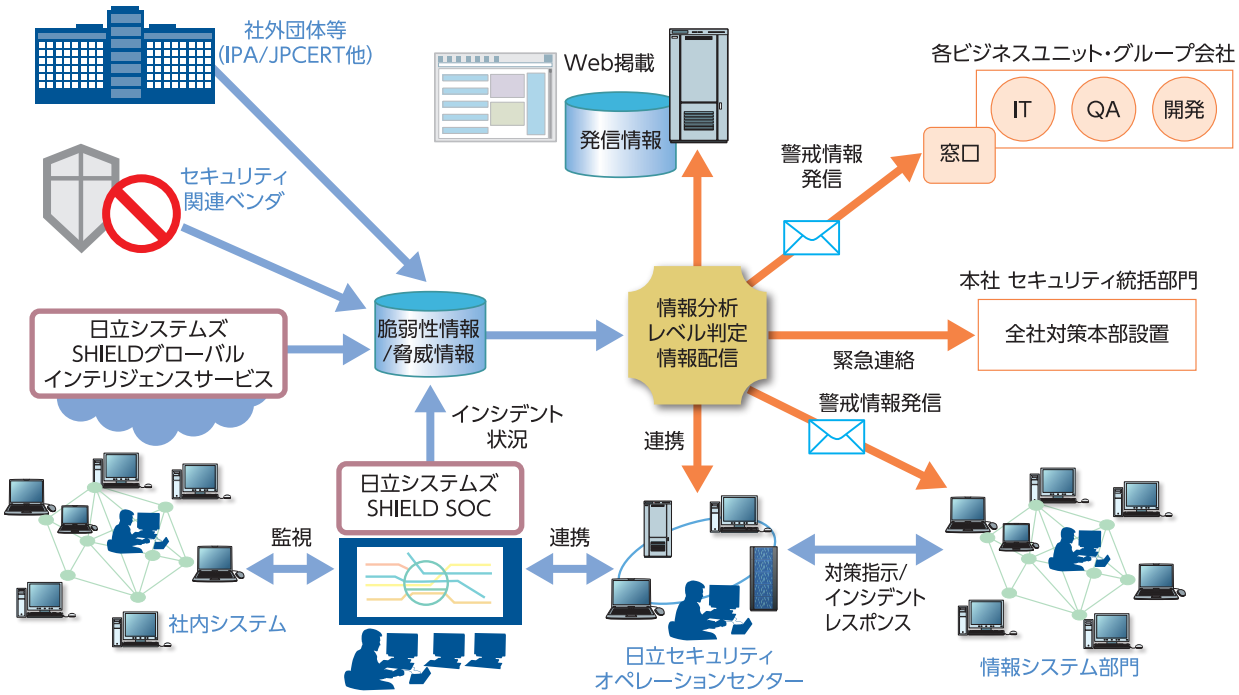
(3) 警戒情報の配信

配信対象の情報は、警戒レベルに応じ、各ビジネスユニット・グループ会社から選出されたサイバーセキュリティ責任者および情報システム部門に対して、即時～週次でのメール配信、社内Web掲載などのコミュニケーション手段を通じて周知を行っています。

(4) 緊急時の際の対応

社内の多数の拠点において重大な業務影響がある場合や、全社レベルで業務継続が不可能な場合には、全社対策本部を設置し、統括したセキュリティ対策指示を行います。

※CVSS基本値:脆弱性そのものの特性を評価する基準であり、情報システムに求められる3つのセキュリティ特性、「機密性」、「完全性」、「可用性」に対する影響を、ネットワークから攻撃可能かどうかといった基準で評価し、算出されます。
(https://www.ipa.go.jp/security/vuln/CVSS.html)



クラウド活用におけるセキュリティへの取り組み

パブリッククラウドの安全な利用の実現

近年、情報システムの実現手段としてパブリッククラウドが注目されています。パブリッククラウドには、情報システムの構築迅速化や運用コスト低減という利点がある一方で、情報漏えいなどのリスクがあります。日立では、パブリッククラウド利用時のリスク対策ガイドラインを定めて、そのようなリスクの低減を図っています。

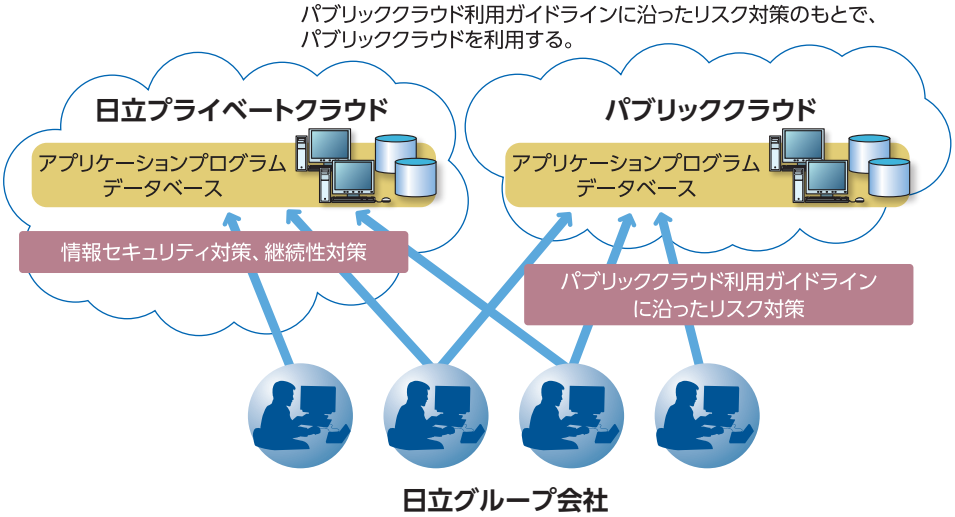
クラウド活用におけるセキュリティへの取り組み

近年、クラウドコンピューティング（以下「クラウド」）に注目が集まっています。一般に、クラウドとは「従来は手元のコンピュータで管理・利用していたようなソフトウェアやデータなどを、インターネットなどのネットワークを通じてサービスの形で必要に応じて利用する方式」※のことです。クラウドには、企業などが自らのIT環境の中でクラウドを実現する「プライベートクラウド」と、専門事業者がクラウドを実現し、インターネットを介してサービスを提供する「パブリッククラウド」があります。

日立では、グループ各社が共通に利用できるプライベートクラウドの整備に取り組んでおり、そこでは前述の「情報セキュリティに対する技術面での取り組み」で述べたようなセキュリティ対策や災害時などのサービス継続性対策を実施しています。一方で、図1に示すように、パブリッククラウドは、そのような取り組みが及ばない領域となるため、パブリッククラウドを利用する際の情報漏えいなどのリスクへの対策指針として、「パブリッククラウド利用ガイドライン」を制定することでリスクの低減を図っています。

※IT用語辞典 e-Words, http://e-words.jp/, 1997-2013

クラウド活用におけるセキュリティ >>



パブリッククラウド利用ガイドラインの制定

パブリッククラウドを利用する際には、図1に示すように、アプリケーションやデータがパブリッククラウドに存在するため、パブリッククラウドへの不正アクセスなどを通じた情報漏えいリスクが存在します。特に、インターネットで提供されているITサービスにおいては、利用者へのなりすましによる不正アクセスなどサイバー攻撃の脅威が高まってきており、パブリッククラウドについても情報漏えいが懸念されます。また、パブリッククラウド事業者の倒産などによる利用者の事業中断やデータ損失といった事業継続性のリスクも存在します。

このようなリスクの低減のために、パブリッククラウド利用ガイドライン(以下「ガイドライン」)を通じて、日立グループ各社がパブリッククラウドを利用するにあたってどのようなリスク対策が必要かを示すことにより、リスクの低減を図っています。

ガイドラインでは、情報漏えいリスクなどに対するリスク低減策として、パブリッククラウドを利用する際に適用すべき認証方法や情報保護方法の指針、パブリッククラウド事業者の運用に関する指針などを定めています。また、ガイドラインの適用を通じたリスク低減の促進のために、パブリッククラウドの利用案件に対して、ガイドラインへの適合性の検証にも取り組んでいます。

物理セキュリティに対する取り組み

物理セキュリティに対する取り組み

情報漏えい対策の一層の強化と防犯対策にはオフィスへの入退管理や防犯カメラ設置などの物理セキュリティ対策の強化が不可欠です。日立グループでは、全社統一方式での物理セキュリティ対策の整備を推進中であり、その概要について紹介します。

物理セキュリティ対策の全社統一化

日立では、従来は物理セキュリティ対策を入退管理を中心に各所が個別方式で対策を行っていましたが、対策強化に向けた整備基本方針を定め、全社統一化を推進しています。

【整備基本方針】

①全社統一対策基準「物理セキュリティ対策基準」による対策方式・管理の均質化

②日立グループ製品・サービスを活用した管理システムの導入

物理セキュリティ整備の概要

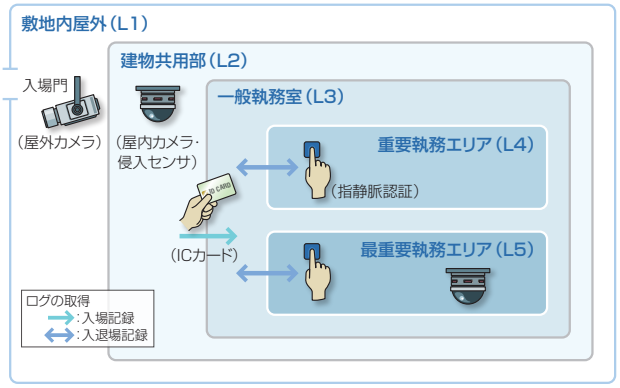
(1) 管理区域のセキュリティレベル設定と対策の統一化

物理セキュリティ対策基準では、管理区域をセキュリティ対策レベルにより5段階に区分し、レベルに応じた入退管理方式、防犯カメラおよび侵入センサの設置基準を定め、これに則して統一した設備により整備しています。

(2) 日立グループ製品と技術の活用

整備する入退管理機器、防犯カメラ、侵入センサは日立グループ製品を活用しています。特に重要区域入場時の、本人確認方式には日立グループの先行技術である「指静脈認証」を導入しています。

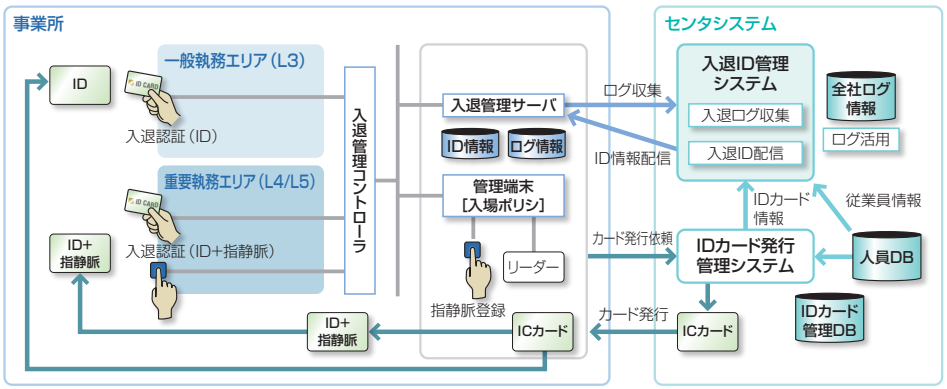
区域のセキュリティ対策レベルと対策方式 >>



(3) センタシステムを活用した運用業務の効率化

事業所における入退管理業務の効率化と標準化のため、全社の人員データベース (社員、資材契約者を含む) を活用したIDカード発行システムとID配信システムを開発し、入場許可対象者の管理業務の効率化を図っています。また、将来的には入退ログ等のフォレンジックデータを一元管理し、有効活用していきます。

入退管理システム全体図 >>



お取引先様と連携した取り組み

お取引先様と連携した情報セキュリティ確保への取り組み

日立は社会イノベーション事業を支える製品・サービスを提供する企業グループとして、お取引先様と連携して情報セキュリティ対策に取り組んでいます。機密情報や個人情報を取り扱う業務を委託する場合は、あらかじめ情報漏えい防止に関する契約書を締結します。また、お取引先様にも日立社内と同じセキュリティレベルでの情報管理を実施していただき、情報セキュリティ事故の予防、再発防止に取り組んでいただいています。

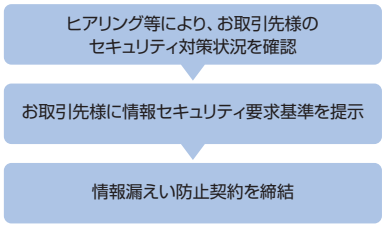
お取引先様との情報セキュリティ確保

日立では、社会イノベーション事業を支える企業グループとして、お取引先様も日立と同じレベルの管理を実施していただき、情報セキュリティ事故の予防、再発防止に向けた取り組みを行っています。

(1) お取引先様の選定

機密情報や個人情報を取り扱う業務を委託する際には、あらかじめ日立が定めた情報セキュリティ要求基準に基づき、お取引先様の情報セキュリティに関する対策状況を確認、審査します。

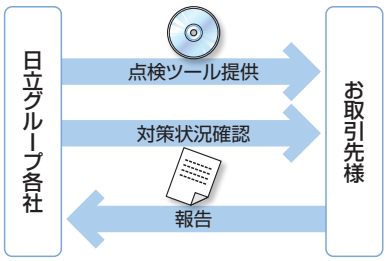
日立では、日立が求めるセキュリティレベルを満たしたお取引先様と情報漏えい防止に関する契約を締結したうえで取り引きを開始します。なお、個人情報を取り扱う業務を委託するにあたっては、別途個人情報の取り扱いに特化した内容の確認を行います。確認の結果、審査に合格したお取引先様に対し、業務を委託します。



(2) 情報セキュリティ事故予防策

ファイル交換ソフトによるインターネットからの情報流出等を防止するため、情報セキュリティツールを提供し、個人のPC等から業務情報を削除するため点検作業を実施しています。

また、お取引先様との契約に基づき、情報セキュリティ対策の状況を確認し、確認結果に応じて適切な改善指導を行っています。



(3) 情報セキュリティ事故への対応と再発防止策

情報セキュリティ事故が発生した場合は、お取引先様を含めて関係部署とともに漏えい情報の影響調査を行い、速やかな問題解決に向け、お取引先様と連携して対策に取り組むとともに、原因を究明して再発の防止に努めます。

なお、重大事故が発生した場合やお取引先様において一向に改善が見られない場合は、取り引きの継続について見直しを行います。

(4) 今後の取り組み

情報セキュリティ事故の防止に向け、お取引先様の情報セキュリティに関する対策状況を絶えず確認するとともに、より一層の連携強化を図り、確実な予防策を講じていきます。

グローバル情報セキュリティの取り組み

グローバル情報セキュリティの推進

情報セキュリティの強化は、企業の社会的信用を確保する上で、全世界の日立グループ会社においても取り組む必要があります。日立は、国際規格であるISO/IEC 27001に則ったグローバル情報セキュリティ管理規程を定め、PDCAサイクルを推進し取り組んでいます。

グローバル情報セキュリティ管理体制

グローバル情報セキュリティの推進において、最も重要な要素であるコミュニケーションチャネルは、ビジネスチャネルとリージョナルチャネルの二つのガバナンス・チャネルを活用しています。この二つのチャネルを効果的に利用することにより、各地域や国で発生する固有の課題を効率的に解決できる体制としています。また、「セキュリティシェアドサービス」の活用を積極的に展開し、セキュリティ施策整備の均質化とIT投資の効率化をめざしています。

国際規格に準拠したグローバル情報セキュリティ管理規程の制定

日立グループがグローバル事業の拡大を図っていくためには、事業基盤としてのITを有効活用することは不可欠であり、このため「ユニバーサルITポリシー」を策定しています。

セキュリティガバナンスを推進するために、「ユニバーサルITポリシー」と情報セキュリティマネジメントシステムの国際規格（ISO/IEC 27001）に準拠した「グローバル情報セキュリティ管理規程」を定めています。この管理規程や関連ドキュメントは、成長著しい新興国も視野に入れ海外会社の成熟度なども考慮した上で、グローバル事業を展開する競争力を維持しつつ、セキュリティリスク対策が確実に実施できる内容としています。

グローバル情報セキュリティレベル向上のためのPDCAサイクル

「グローバル情報セキュリティ管理規程」に基づいたセキュリティレベル向上のため、情報セキュリティ対策の継続的な運用、維持・改善といったPDCAサイクル（継続的改善活動）を推進しています。各海外会社のセキュリティ推進状況把握は、セルフチェックにより行っています。その結果を「見える化」～「分析」することで、各地域・海外会社の状況を把握し、今後、全社的に取り組むべきグローバルセキュリティ施策の方向性の立案に活用しています。

情報セキュリティ人財育成の取り組み

情報セキュリティ人財育成の取り組み

日立グループでは、お客様に安心して製品・サービスをご利用いただくために、セキュリティに関わるスキル・キャリア評価と技術研修・管理教育を通して、高度セキュリティ人財とお客様にセキュリティ技術を橋渡しできる人財を育成しています。

情報セキュリティ人財育成の活動概要

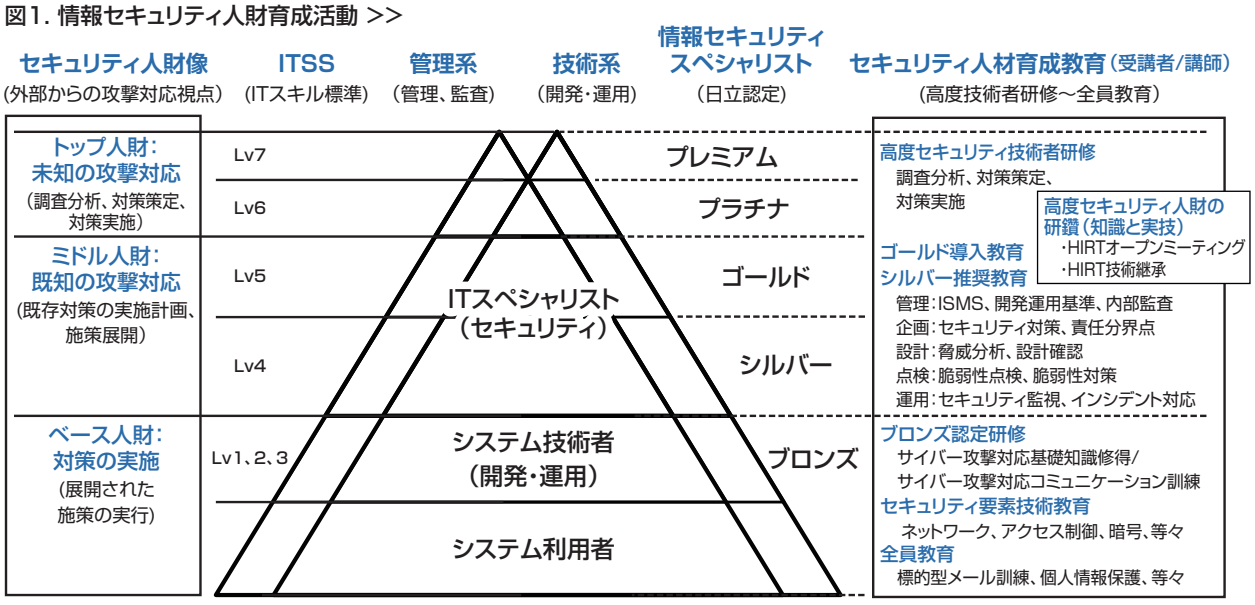
社会インフラへのサイバー攻撃の激化に伴い、日立グループではそれに対応できるセキュリティ人財の①発掘と評価、②育成と活用、③情報共有と組織連携を行い、社会インフラのセキュリティ確保に寄与することを目的に、情報セキュリティ人財育成活動を進めています。

この中で、情報セキュリティの高度な専門家だけでなく、現場のシステム開発運用に携わる技術者や社内インフラの利用者も情報セキュリティ人財の対象として進めています。この活動では、組織的にサイバー攻撃に対応する人財像を、経済産業省が定めているIT関連能力を職種や専門分野ごとに明確化、体系化したITスキル標準（ITSS）をベースに、次の3つのグループで構成しています。また、それぞれの層に必要な教育と演習として、高度セキュリティ人財の研鑽からサイバー攻撃対応の基礎知識修得eラーニングやコミュニケーション訓練を実施しています。

① 高度セキュリティ人財
未知の攻撃に対して調査分析、対策を策定し、ミドル人財やベース人財を指導できるトップ人財
② システム開発運用をまとめるセキュリティ人財
情報システムの開発運用で、既知の攻撃に対して既存対策の実施計画、施策を展開できるミドル人財
③ 展開されたセキュリティ対策を実施する人財
トップ人財の注意喚起やミドル人財の指示にもとづき担当システムの調査や対策を実施するベース人財

日立グループでは、2014年8月より一般社団法人情報処理学会「認定情報技術制度」の企業認定に準拠した日立ITプロフェッショナル認定制度(Hitachi Certified IT Professional)を創設しました。この制度の下、スキル(教育受講等)とキャリア(業務実績等)を兼ね備えた情報セキュリティ人財を発掘・育成・評価し、情報セキュリティスペシャリスト（プレミアム～ブロンズ）として認定しています。

図1. 情報セキュリティ人財育成活動 >>



※ITSS：IT スキル標準（Information Technology Skill Standard）, HIRT：Hitachi Incident Response Team, ISMS: Information Security Management System

情報セキュリティ人財育成の取り組み

日立グループ全体への情報セキュリティ人財育成の展開

サイバー攻撃に迅速に対応するには、セキュリティ専門家・専門組織と現場のITインフラ・システムの利用者や運用担当者が組織の垣根を越え、一体となって対策にあたる必要があります。

まず職場の担当者が、現場での異変・違和感に気付き、速やかにセキュリティ専門家に報告・連絡・相談し、専門家の指示に従って適切に初期対応できることが求められます。さらに、サイバー攻撃対応を担う関係者間で円滑に情報共有し、組織としての対応方針を迅速に決断する必要があります。

このようなサイバー攻撃対応体制の基盤を担うベース人財を育成するために、2016年度下期から「サイバー攻撃対応基礎知識修得eラーニング」教育と「サイバー攻撃対応コミュニケーション訓練」教育を開始し、両教育の受講修了者を情報セキュリティスペシャリスト「ブロンズ」クラスと定義し、その育成と認定を推進しています。

当初、首都圏のIT事業部門から教育を開始し、現在は首都圏以外・IT事業以外の部門へも拡大しており両教育を年間2,000名超が受講修了、ブロンズ認定されています。今後も継続して日立グループ全体へ向けて教育を展開し、サイバー攻撃対応を支えるセキュリティ人財育成を進めていきます。

図2. サイバー攻撃対応体制を支えるベース人財 >>

図3. サイバー攻撃対応教育 >>

■ サイバー攻撃対応基礎知識修得eラーニング

サイバー攻撃を受けた際の動きや影響を修得する研修

【基礎知識】
①日常業務での注意点、②サイバー攻撃への対処、③開発時の注意点、④ぜい弱性情報の収集と対策検討、⑤インシデント発生時の備え

【体験学習】
①標的型攻撃による情報流出、②ランサムウェア感染による業務妨害、③Webアプリケーションの脆弱性による被害、④マルウェア被害

■ サイバー攻撃対応コミュニケーション訓練

インシデント発生時の状況把握、対応内容決定の訓練

【OODA】
①Observe(観察)、②Orient(方向付け)、③Decide(意思決定)、④Act(対応・対策)に要求される迅速性、正確性の体験

【報・連・相】
①報告、②連絡、③相談において、役割分担の重要性や出来事を5W1Hで正確に伝えることの重要性の理解

個人情報保護に対する取り組み

安心と信頼を保証する個人情報保護

日立では、2007年3月に、個人情報の安全管理・保護措置を適切に講じているとして「プライバシーマーク」を付与されました。個人情報保護の仕組みである「個人情報保護マネジメントシステム」を運用し、従業員およびステークホルダーの皆様の個人情報保護と適切な取り扱いに、継続的に取り組んでいます。

個人情報保護

日立では、個人情報保護に関する理念と方針を定めた「日立製作所 個人情報保護方針」に基づいて、ご本人様の大切な個人情報を守るために、個人情報保護法以上に厳しい管理水準を定めている、日本工業規格「個人情報保護マネジメントシステム−要求事項(JIS Q 15001:2006)」に対応する個人情報管理規則を制定しています。

2007年3月、適切に個人情報の安全管理・保護措置を講じていると認められた事業者に付与される、第三者認証「プライバシーマーク」(付与機関:一般財団法人日本情報経済社会推進協会)を取得し、2019年3月の7回目の認定に向け、取り組んでいます。

ステークホルダーの皆様が、日立に安心して個人情報をご提供していただけるよう、「プライバシーマーク認定事業者」としての「自覚」と「責任」をもって、個人情報の保護に努めています。

日立製作所　プライバシーマーク >>

個人情報保護推進体制

日立では、2009年4月に、「個人情報保護推進体制」と「情報セキュリティ推進体制」を統合し、新たに「情報セキュリティ推進体制」を発足させました。個人情報を含む重要な情報および情報セキュリティに関する管理体制を一元化することにより、実効性の高い管理体制の実現を目的としています。この統合により、「個人情報保護法」等で求められている4つの安全管理措置の実施および「情報セキュリティに対する技術面での取り組み」や「物理セキュリティに対する取り組み」と一体化し、個人情報保護活動を推進しています。具体的な管理体制については、「情報セキュリティマネジメントシステム」の「情報セキュリティ推進体制」の項で述べたとおりです。

海外のグループ会社においても、「個人情報保護方針」に基づきながら、各国または各地域の法令および社会的な要求にあわせて、個人情報の保護に取り組んでいます。

〈4つの安全管理措置〉

(1) 組織的安全管理措置:
　規程、体制の整備運用および実施状況の確認等
(2) 人的安全管理措置:
　非開示等契約の締結、教育・訓練等
(3) 物理的安全管理措置:
　入退館(室)の管理、盗難防止措置等
(4) 技術的安全管理措置:
　情報システムへのアクセス制御、不正ソフトウェア対策等

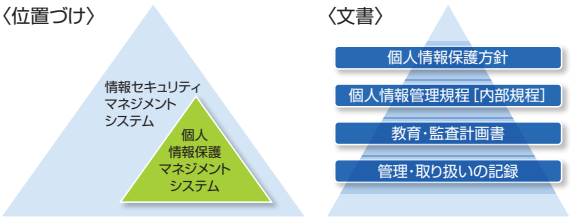
個人情報保護に対する取り組み

個人情報保護マネジメントシステム

管理体制の統合に併せて、個人情報保護の仕組みである「個人情報保護マネジメントシステム」（PMS）についても、個人情報保護固有の一部運用を除いて、「情報セキュリティマネジメントシステム」（ISMS）の一部として位置づけました。PMSにおけるPDCAは、「情報セキュリティマネジメントシステム」として実施しています。

また、PMSの基本要素を文書として記述した「PMS文書」は、「個人情報保護方針」「個人情報管理規程（内部規程）」、監査・教育等の「計画書」、PMS実施の「記録」から成ります。

日立製作所 個人情報保護マネジメントシステムについて >>



個人情報の管理と適切な取り扱い

日立では、お預かりした個人情報については、社内規程である「個人情報管理規程」に則って、厳格な管理と適切な取り扱いに努めています。

各職場ごとに個人情報保護責任者（情報資産管理者）を置き、日立が取り扱う「すべての個人情報」を特定し、当該個人情報の重要性およびリスクに応じて、台帳を管理し、適切な措置を講じています。

また、個人情報保護マネジメントシステム定着化のため、定期的に個人情報保護教育、個人情報保護監査、職場での運用状況の確認を行っています。

あわせて、すべての従業員に、「個人情報保護／情報セキュリティカード」を配付し、日立の個人情報保護に関する理念および管理と取り扱いに関する遵守事項を周知徹底しています。

職場での取り組み事項 >>

〈すべての個人情報〉

- ·個人情報の特定、分類
- ·個人情報の台帳登録
- ·適切な取り扱い
- ·個人情報保護監査
- ·リスクの認識、分析、対策
- ·個人情報の定期見直し
- ·個人情報保護教育
- ·職場での運用状況の確認

マイナンバー制度への対応

日立では、マイナンバー制度に対応した社内規程に則り、厳格な管理と適切な取り扱いに努めています。マイナンバーの管理体制を確立して、マイナンバー取り扱い業務のリスクを評価し、適切な措置を講じています。

国外の個人情報保護関連法制度への対応

近年、ITの高度化や社会経済活動の国際化に伴うプライバシーリスクの高まりを受け、世界各国で個人情報保護関連法制度の規定・改定の動きが活発になっています。

特に、欧州一般データ保護規則（GDPR）は欧州の法律ですが、個人情報の取り扱い義務や罰則の強化などの影響が欧州以外にも及びます。そこで、日立ではGDPRに対する取り組みとして、欧州の地域統括会社、欧州事務所を含む日立グループ全体で連携し、GDPRの適用を受ける業務の特定（欧州のお客様からお預かりした個人情報やグローバル人財データベースに含まれる従業員情報等）とそのリスク評価、リスクに応じた適切な安全管理措置の実行、全従業員を対象とした教育等を実施しています。また、欧州当局のGDPRの施行状況や社内の対応状況を継続してモニタリングし、適切な措置を講じます。

個人情報保護に対する取り組み

委託先の管理強化

ここ数年、個人情報の取り扱い委託先から漏えい事故が多く発生し、社会的問題となっています。日立では、早くから個人情報の委託先管理を強化し、個人情報の取り扱いを委託する際の社内規程を定め、規程に則って、委託先を監督しています。委託する際には、日立と同等以上の個人情報保護の水準にある委託先を選定するために、日立グループが定めた委託先選定基準によって評価、選定を行っています。さらに、管理体制の確立、原則再委託禁止など厳格な個人情報管理条項を盛り込んだ契約を締結したうえで、委託しています。また、定期的に委託先再評価や監査を実施するなど、委託元としての責任を自覚し、委託先の監督を行っています。

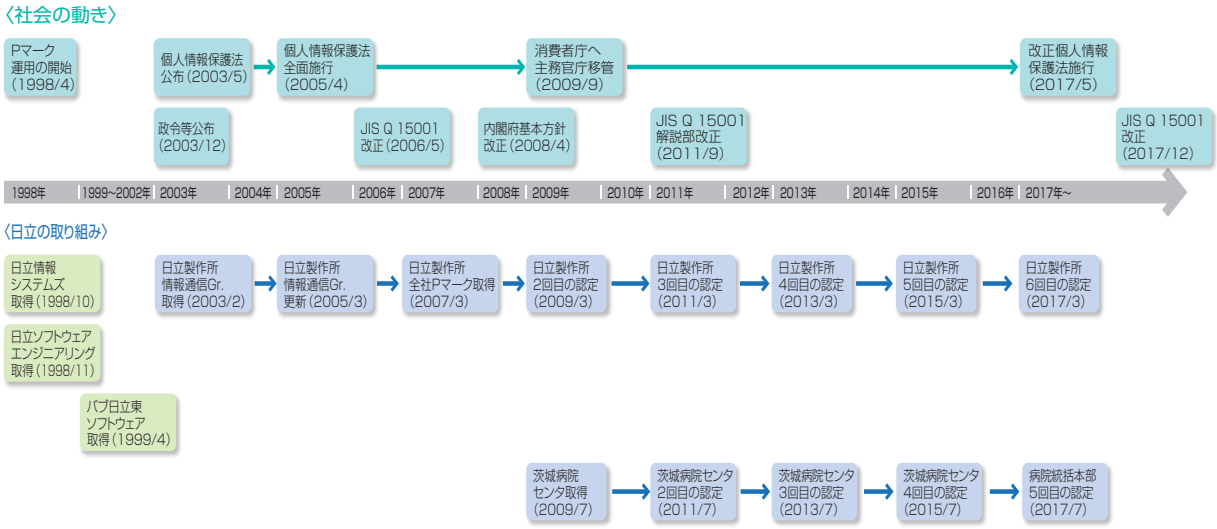
日立グループ全体の取り組み（プライバシーマーク取得推進状況）

日立グループでは、グループ一体となり、個人情報保護に取り組んでいます。2018年5月31日現在、44事業者が「プライバシーマーク」を取得し、法令より管理レベルの高い個人情報の保護と取り扱いを行っています。また、プライバシーマーク取得会社を主体として、「日立グループPマーク連絡会」を組織し、定期的に情報交換会、勉強会、外部有識者を招いての講演会等を実施するほか、グループ全体として、個人情報保護に関する情報共有化および研鑽を重ねています。

病院等医療施設も独立した事業者として個人情報保護に取り組んでいます。

日立では、2009年7月に企業立病院である病院統括本部が取得、患者をはじめ関係者の個人情報の保護とその適切な取り扱いに努めています。

日立製作所プライバシーマークへの取り組み >>



お客様に提供する情報セキュリティの取り組み

IoT時代の社会インフラを支える日立のセキュリティ

変化するIoT時代において、お客様のシステムやサービスを守るため、日立はセキュリティのビジョンとして「Evolving Security for changing IoT world.」を掲げ、セキュリティを進化させます。

進化の方向性

日立は、3つの方向性でお客様のビジネス進化と、セキュリティの進化を加速します。

●進化1:ITセキュリティをOT/IoTセキュリティへ

社会インフラシステムの構築・運用の実績を持つ日立だからこそ、OT/IoTの守り方を知っています。

●進化2:日立社内で実証を重ねたセキュリティを顧客へ

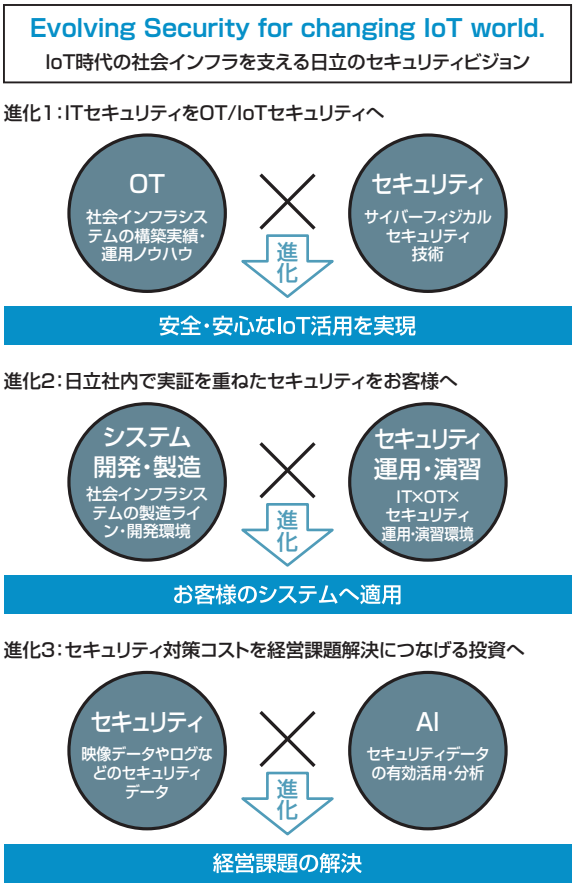
日立には、社会インフラシステムの開発・製造とセキュリティ運用・演習を行う環境があります。

●進化3:セキュリティ対策コストを経営課題解決につなげる投資へ

セキュリティデータをAIで分析することで、経営課題解決にむけたソリューションに活用できます。

OT:Operational Technology
IoT:Internet of Things
AI:Artificial Intelligence

進化の方向性 >>



日立のセキュリティアプローチ

脅威やリスクからビジネスを守るには、システムでの対策だけでは万全とは言えません。システム対策だけでなく、組織・運用まで意識した、包括的なセキュリティが求められています。

日立は、お客様の安全・安心を実現するため、「組織で守る、システムで守る、運用で守る」というセキュリティ提供のアプローチをとります。

セキュリティ対策のためのシステム構築は勿論、対策の効果を継続的に維持するための組織マネジメントシステムや、異常な振る舞いを監視・検知する運用方策も合わせて提供します。

日立のセキュリティアプローチ >>

お客様に提供する情報セキュリティの取り組み

進化するセキュリティ

お客様の課題にともに取り組むイノベーションパートナーとして、新たな価値創造とOT/IoTセキュリティの実現を支える新しいサービスやソリューション、実用化に向けた日立社内での実証実験など、進化するセキュリティについてトピックをご紹介いたします。

重要インフラ事業者向けのサイバー防衛訓練サービス

サイバー攻撃対応のための総合訓練・検証施設を開設し（日立の大みか事業所内）、日立がこれまで培ってきた制御システムと情報システムの技術・ノウハウを組み合わせた、重要インフラ事業者向けのサイバー防衛訓練サービスを提供開始しました。

第一弾として、電力事業者を対象に、お客様の実システムを模したシステム環境を施設内に構築し、システム監視や指揮命令を行う関連部門の組織訓練を目的としたプログラムと、サイバー攻撃に備えた運用手順の検証やセキュリティ製品の評価ができるサービスをスタートしました。（P.44を参照）

施設 内観 >>

制御システム向けセキュリティ監視ソリューション

制御システム内のセキュリティインシデント発生を早期検知し、従来特定が困難であった発生元や伝播ルート、影響範囲を分析・可視化するとともに、緊急時に行う一連の判断・対応を迅速化し、被害拡大を防ぐための一次対処を支援しました。

USBメモリの不正使用によるセキュリティインシデントを防止するUSB管理ソリューション

近年、制御システムにおいてUSBメモリの不正使用によるセキュリティインシデントが増加しています。制御システム内にある制御装置や端末などのUSBポートに取り付けるだけで、当該装置や端末のUSB接続を管理する、USB管理ソリューションの提供を開始しました。

サイバー攻撃の脅威を早期に検知する新規アルゴリズムを開発、「Hitachi Anomaly Detector」として製品化へ

制御システムへの導入が可能な、サイバー攻撃の脅威を早期に検知するアルゴリズムの開発に成功しました。正常なシステム状態を定義し、現状と照合しながら自動学習し、異常を検知します。新製品「Hitachi Anomaly Detector」として提供を開始します。

Hitachi Anomaly Detectorは、内閣府が進める戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人:NEDO）で日立が受託した研究開発の成果を活用し、開発したソフトウェア製品です。

セキュリティインシデントの発生率と損害額を定量化するサイバーリスク診断手法の開発

損害保険ジャパン日本興亜株式会社とSOMPOリスケアマネジメント株式会社とともに、産業・重要インフラ分野における適切なセキュリティ投資判断の支援を目的に、セキュリティインシデントの発生率と損害額を定量化する共同研究を実施し、「セキュリティ診断システム」と「損害発生モデルシミュレータ」の開発および技術検証を行いました。

お客様に提供する情報セキュリティの取り組み

日立とトレンドマイクロがセキュリティ人財育成に関する新たな共同事業を立ち上げ

日立とトレンドマイクロは、国内で不足するセキュリティ人財の育成加速を目的に、日立が有するシステムの開発・運用や人財育成のノウハウとトレンドマイクロが有する国内外の脅威動向や最新の攻撃シナリオを組み合わせた「サイバー攻撃対応研修」提供を10月から開始します。今後、本共同事業では、新しい研修サービスの開発を進め、人財の育成加速に寄与していきます。

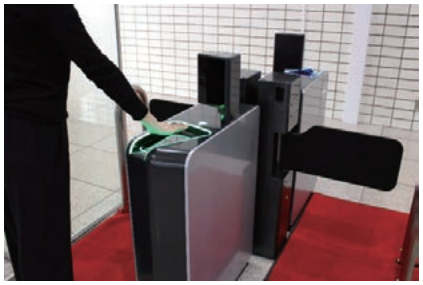
「ウォークスルー型指静脈認証ゲート」を使用した実証実験

フィジカルセキュリティ入退館ゲートの実用化に向けて、東京都品川区にある日立の大森オフィスにおいて、社内1,000名規模のリアルデータを用い、実運用と同等レベルでの評価を目的に実証実験を行いました（2017年3月～2018年2月）。

実証実験で使用されている「ウォークスルー型指静脈認証ゲート」は、動きのある手からの指静脈の高速かつ安定した撮影を実現。さらに装置に手を触れずに認証できる「非接触型」のデザインとなっています。

改札機並みの高いスループットによる利便性、高い認証性能などを実証することで、将来、大規模イベントなど個人の特定が望まれる分野への適用を検討しています。（P.49を参照）

ウォークスルー型指静脈認証ゲート >>



プライバシー保護の取り組みのホワイトペーパー公開

パーソナルデータの利活用を検討されている事業者の方に向け、パーソナルデータの利活用において日立が実施しているプライバシー保護の取り組みをホワイトペーパーにまとめ、公開しました（2017年10月）。

ホワイトペーパーでは、プライバシー保護に関する基本的な考え方とともに、日立における具体的な取り組みとして、プライバシー保護に関する組織・制度の構築、プライバシー影響評価の実践、開発業務におけるプライバシー保護対策、生活者のプライバシー意識調査の継続実施等の内容について整理しています。また、実際にプライバシー保護対策を適用した事例についても記載しています。（P.38～39を参照）

日立インシデントレスポンスチーム(HIRT)寺田真敏が総務大臣奨励賞を受賞

日立の寺田真敏が「サイバーセキュリティに関する総務大臣奨励賞」を受賞しました。

寺田は、1998年に日立内に企業内CSIRT日立インシデントレスポンスチーム(HIRT)、2007年には国内のシーサート6チームと共に日本シーサート協議会を立ち上げ、2018年現在、日本シーサート協議会運営委員長としてシーサート活動の普及を推進しています。また、JVN(Japan Vulnerability Notes)サイト(https://jvn.jp/)の整備など国内の脆弱性対策を推進するための活動を2002年より続けています。

表彰状>>

[サイバーセキュリティに関する総務大臣奨励賞]
地方自治体、民間企業、各種団体等の現場において、ネットワーク環境等のサイバーセキュリティ向上の観点から、特に顕著な功績があり、今後サイバーセキュリティ分野で更なる活躍が期待される個人または団体（チーム）に対し、平成29年度から総務大臣奨励賞を授与するもの

お客様に提供する情報セキュリティの取り組み

日立のセキュリティソリューション「Secureplaza」

日立グループの総合力でビジネスのセキュリティ強化と課題解決に貢献するソリューションを提供します。

システム対策だけでなく、組織・運用まで意識した、包括的なセキュリティ

●組織で守る

さまざまなセキュリティリスクに備えるには、第一に、組織としての対応が不可欠です。組織においてセキュリティガバナンスを確立し、人材育成やリスクアセスメントを通じて、段階的・継続的にセキュリティレベルを向上させることが重要です。

●システムで守る

日々進化する脅威からビジネスを守るには、セキュリティ対策ソフトを導入するといった単一の防御策だけでは、対応しきれなくなっています。さまざまな対策手段を複合して組み合わせた多層での防御策が必要です。

●運用で守る

サイバー攻撃の多様化・高度化は、事業の継続を脅かしつつあります。サイバー BCPの策定により万一の事象に備えるとともに、インシデントの検知、現場での一時対処、関連情報の収集・分析・的確な対応策の策定・実行などを迅速に遂行するSOC/CSIRTの構築と経営層まで巻き込んだ体制でのセキュリティ運用が重要です。

サイバー BCP:サイバー攻撃を想定した事業継続計画
BCP:Business Continuity Plan
SOC:Security Operation Center
CSIRT:Computer Security Incident Response Team

日立セキュリティソリューション「Secureplaza」 >>

1 セキュリティガバナンスの確立と人材育成

・セキュリティガバナンスの確立
・セキュリティ人材の育成、従業員のリテラシー向上

2 サイバーセキュリティ対策の強化

・既知・未知を問わずさまざまな脅威からITシステムを防御
・制御システム特有のセキュリティ対策

3 フィジカルセキュリティ強化と業務課題解決

・エリアの重要度に応じたアクセス制御・監視
・映像監視・分析技術によるセキュリティ高度化
・フィジカルセキュリティ利活用による業務課題解決

4 情報漏えい防止とプライバシー保護

・5W1Hの観点で情報漏えいのリスクを回避
・データ持ち出し制御による情報漏えい防止
・パーソナルデータ利活用に向けたプライバシー保護

5 ID管理強化と利便性向上

・組織における効率的なID管理の実現
・特権IDのアクセス管理強化
・指静脈認証を用いたセキュリティ強化と利便性向上

6 インシデントの的確な把握と迅速な対応

・適切な判断と迅速な対応を可能にする統合運用監視
・CSIRT構築・運用を支援 セキュリティ高度化
・セキュリティ監視および調査・分析を支援

情報系製品・サービスへの取り組み

情報系製品・サービスに対する情報セキュリティ確保の取り組み

日立製作所では、お客様へ提供する情報系製品・サービスのセキュリティを確保するため、セキュリティ対応施策の検討・策定体制を有し、セキュリティマネジメントプロセスに沿ってそれらを運用、改善する活動を推進しています。本活動は、社内セキュリティガバナンス体制のもと、情報系製品・サービスを提供する事業部門が中心となり推進しています。

セキュリティ確保に向けた取り組み

お客様へ提供する情報系製品・サービスのセキュリティ確保のために推進している取り組みを以下に記します。

●情報系製品・サービスのセキュリティ対応施策の策定・推進

情報系製品・サービスのセキュリティを適切に確保することを目的に、情報系製品・サービスを提供する事業部門を対象に、セキュリティ対応施策を検討、策定する体制を有しています。(図1参照)本体制では、製品・サービスの開発・運用におけるセキュリティ施策など、情報系製品・サービスを提供する事業部門に固有の施策の策定・運用を推進しています。本活動には、関連するグループ会社も参画しており、連携して施策化を進めています。策定された施策は、関連する事業部門に展開され、各事業部門において運用されます。

● セキュリティマネジメントプロセスに沿った製品・サービスの開発・運用

製品・サービスの開発・運用の各フェーズごとに、セキュリティマネジメントプロセスを定義し、それを規則化することで組織における確実な実施につなげています。規則はまずマネジメントプロセスの全体像を規定し、その下に細則や基準を設けて、より具体的な活動内容を規定する体系としています。更に支援ツールや事例をナレッジとして提供することで活動が確実、適切かつ効果的に推進できるようにしています。(図2参照)

マネジメントプロセスの中核を担うのは、セキュアシステム開発運用マネジメント基準です。日立が提供する情報系製品・サービスの開発・運用において適用される本基準は、セキュリティランクの概念を採用し、ランク付けの指標を定義。セキュリティランク別に開発・運用時のセキュリティ確保に必要なセキュリティマネジメントプロセスを示しています。(図3参照) セキュリティランクの採用は、リスクの高さを認識し適切な対応をとることを促すだけでなく、リスクとコストのバランスの考慮にもつながります。また、本基準が示すプロセスは、日立において標準化されている情報システム開発プロセスとも連携した内容となっています。

規則化されたセキュリティマネジメントプロセスの内容は、前述のセキュリティ対応体制により、定期にまたは必要に応じて随時に改訂されます。これは、発生したインシデント、顕在化したリスク、運用した結果などからのフィードバックに基づき実施され、マネジメントプロセスがより適切なものになるよう継続的な改善を行うことを目的としています。

図1. 情報系製品・サービスのセキュリティ対応施策の検討・策定体制 >>

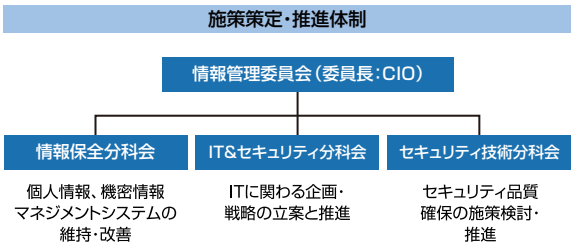
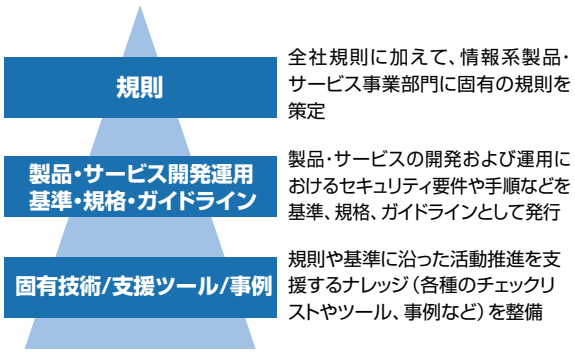


図2. 情報系製品・サービスセキュリティ規則体系 >>



情報系製品・サービスへの取り組み

図3. セキュアシステム開発運用マネジメント基準のセキュリティプロセス（抜粋）>>

企画	基本設計	詳細設計・製造	テスト	運用準備・移行	運用
・セキュリティランクの設定 ・開発環境のセキュリティ方針の作成 ・セキュリティ要件および対策の明確化 等	・セキュリティ方式設計の実施 ・基本設計のデザインレビュー 等	・通常時運用手順へのセキュリティ関連内容の反映 ・セキュリティインシデント対応手順の作成 等	・セキュリティ方式設計に対するテスト計画の策定 ・脆弱性点検 ・テスト結果の評価 等	・稼働前レビュー ・脆弱性定期分析 等	

●脆弱性点検の実施

脆弱性攻撃による被害の抑止を目的に定期的脆弱性診断を実施しています。点検のタイミングは、新規開発時、環境変更時および定期実施としています。点検方法は、チェックリストを用いた定性的なものと、脆弱性点検ツールを用いたものがあり、これらを単独または併用することで、システム特性や運用状況に沿った適切な点検が行えるようにしています。なお、インターネットへの接続は、一般に高いリスクを伴うことから、インターネット接続に対する認可制度を設けており、承認を得なければインターネットへの接続や公開などが行えない仕組みをとっています。

●インシデント対応

脆弱性を悪用したセキュリティインシデントの発生可能性の低減を目的に、情報系製品・サービス提供部門における脆弱性関連情報のハンドリングプロセスをガイドにまとめ、これに基づき活動を推進しています。（日立におけるインシデントハンドリングの全体像については「セキュリティインシデントへの取り組み（P.34-35）」を参照）また、大規模なインシデント発生時の対応体制および対応マニュアルを整備、訓練を実施することで迅速かつ的確な対応ができるよう備えています。

情報系製品・サービスへの取り組み

ソフトウェア製品に対するセキュリティ確保の取り組み

近年、ソフトウェア製品の脆弱性が社会基盤に与える影響は、ますます大きくなっており、製品のセキュリティ確保が不可欠となっています。ソフトウェア製品を安心してお使いいただくため、グローバルな視点で、設計／開発から運用までの各フェーズでセキュリティの確保に努めています。

セキュリティ確保への取り組み

日立が提供するソフトウェア製品は、社会インフラの中核を担う製品が多いことから、セキュリティの確保は重要不可欠です。お客様が安心できる製品を提供することはベンダーの責務であり、製品の設計から実装、運用までのソフトウェアのライフサイクル全般において、セキュリティを考慮した仕組み作りが重要です。ソフトウェア製品の開発にあたっては、従来の開発プロセスに対して、セキュリティを確保するための施策を取り入れています。これを「製品セキュリティライフサイクル」と定義し、情報セキュリティの国際評価基準であるISO/IEC 15408（コモンクライテリア）などの考え方も取り入れながら、グローバルな水準でのセキュリティの確保に努めています。

「製品セキュリティライフサイクル」に基づくソフトウェアの開発

「製品セキュリティライフサイクル」では次の事項に重点を置いた開発プロセスを確立しています。

① 要件定義
　製品のセキュリティに関する全体方針、セキュリティを確保するための開発方針の決定
② 設計
　脅威分析に基づいたセキュリティ要件の決定とセキュリティを考慮した機能設計の具体化
③ 実装（セキュアプログラミング）
　チェックリストと静的検証ツールを活用したソースコードレベルでの脆弱性問題の摘出
④ テスト
　セキュリティツール（スキャナ）による脆弱性検査とセキュリティチェック項目に基づいたテストの実施
⑤ サポート
　運用開始後に発見された脆弱性問題への迅速な対応対策版の作成と情報提供によるサポート

また、開発者、検査担当者に対してセキュリティに関する技術、脆弱性問題の動向などの啓発、情報共有を行っており、これらを継続的に実施することで、セキュリティを確保した製品開発に取り組んでいます。

ソフトウェアの脆弱性問題への対応の考え方

ソフトウェアの脆弱性問題は、設計、実装、テストフェーズで刈り取ることが基本ですが、新たな脆弱性が発見されたり、攻撃手法が登場することが考えられます。したがって、ソフトウェア製品の運用フェーズにおける対応も考慮しておく必要があります。

これらの取り組みは、平成29年経済産業省告示第19号「ソフトウェア製品等の脆弱性関連情報に関する取扱規程」、「情報セキュリティ早期警戒パートナーシップガイドライン」にも対応しており、脆弱性問題の連絡から、対策方法をお客様に提供するまでの手順を定めています。また、この仕組みは「HIRT※」によるインシデント対応活動（CSIRT）とも連携しており、関係機関と協力して、製品の脆弱性問題に対応しています。

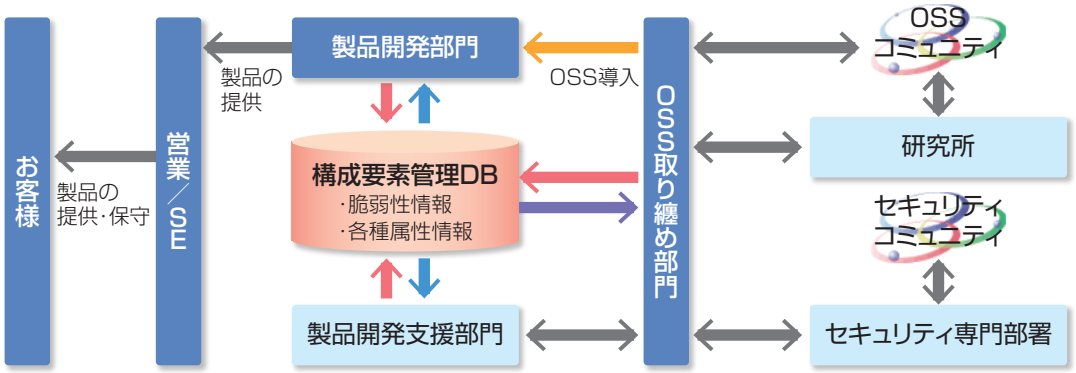
※HIRT：Hitachi Incident Response Team
　CSIRT：Computer Security Incident Response Team

情報系製品・サービスへの取り組み

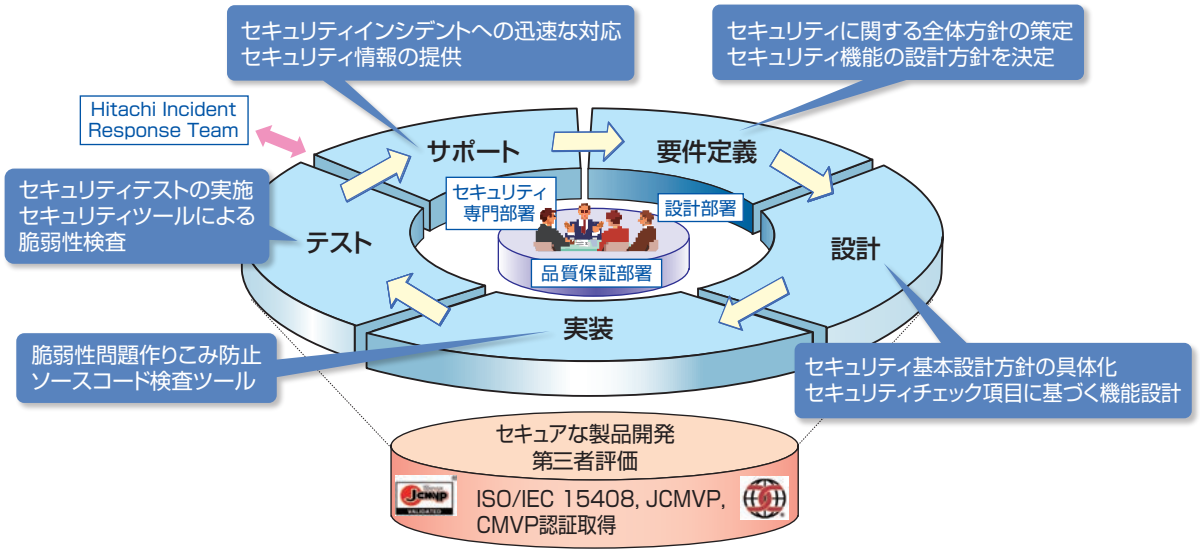
オープンソースソフトウェア（OSS）への対応

近年では著名なOSSにおける脆弱性情報の公表事例が目立つようになりました。これに対応するため、製品で利用するOSS情報を一元管理し、問題の解析と 影響有無の判断と対策方針の決定を迅速に行うための取り組みを行っています。

構成要素管理DBを利用したOSS活用体制 >>



製品セキュリティライフサイクル図 >>



第三者評価・認証制度の活用

「製品セキュリティライフサイクル」での取り組み、すなわち、セキュリティを確保する取り組みを客観的に示す指標として、国際セキュリティ評価基準であるISO/IEC 15408などによる第三者評価・認証にも取り組んでおります。

この基準は、「政府機関の情報セキュリティ対策のための統一基準」等でも活用されており、製品開発における「セキュリティ確保」の取り組みを客観的に示すことができます。

また、「製品セキュリティライフサイクル」に基づくソフトウェアの開発を行うことで、ISO/IEC 15408などの国際基準と同等水準の製品開発が可能となります（取得製品は、「第三者評価・認証」の「ITセキュリティ評価・認証の取得状況」を参照ください）。

参考情報 >>

■ITセキュリティ評価及び認証制度（JISEC）
https://www.ipa.go.jp/security/jisec/index.html

■暗号モジュール試験及び認証制度（JCMVP）
https://www.ipa.go.jp/security/jcmvp/index.html

■Cryptographic Module Validation Program（CMVP）
https://csrc.nist.gov/projects/cryptographic-module-validation-program
JCMVP（Japan Cryptographic Module Validation Program）

情報系製品・サービスへの取り組み

クラウドコンピューティングにおける情報セキュリティへの取り組み

Hitachi Cloud（プラットフォームリソース提供サービス/エンタープライズクラウドサービス）

新たなITの提供形態であり、社会インフラの1つとなるクラウドにおいて、日立は種々のセキュリティに関する取り組みを行い、企業情報システムに適用可能な「安全・安心クラウド」を実現します。

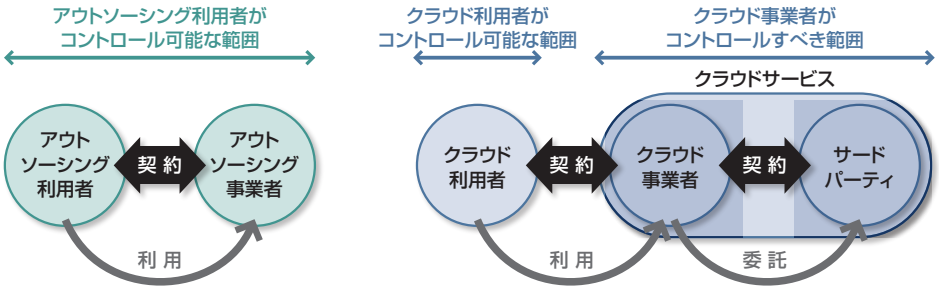
クラウドコンピューティングとセキュリティ

電力や水道のように、ITにおいても、施設・装置を所有するのではなく、サービスとして利用する「クラウドコンピューティング」（以下「クラウド」）が広く普及しています。クラウドでは、ハードウェアやソフトウェアの保守などに加え、セキュリティ対策についてもサービス提供者（クラウド事業者）が行うことから、利用企業のIT部門（クラウド利用者）は、これらの業務から開放され、自社のコアコンピタンスを実現するIT構築に専念できます。反面、クラウドにおいては色々な利用者がサービス提供者の環境を共用するため、情報漏えいなどを懸念される方も少なくありません。

また、ITに関するコンプライアンスなど社内システムならば管理/監査できる内容が把握できなくなるのではないかといった危惧を抱かれる場合があります。

このように、クラウドでは、「（他利用者とのリソースの）共用」と「（事業者の環境の）利用」というクラウド独特の特性に対応した情報セキュリティが必要となります。また、業務システムにおいて一部にクラウドを利用したような場合には、ITシステム全体として、従来システムと同等な情報セキュリティの確保が求められます。

従来の業務委託とクラウドとのコントロール範囲の違い>>



(a) 通常の業務委託時　　(b) クラウド利用時

クラウドコンピューティングの情報セキュリティに関する動向

このような状況に対し、種々の業界団体、公的機関などがクラウドに関する情報セキュリティのガイドラインや規格を策定しています。主なものとして以下があります。

また、経済産業省のガイドラインに基づいて日本代表よりISO/IEC SC 27に提案した国際標準案が、ISO/IEC 27017として規格化されています。

この推進・普及のため、日本セキュリティ監査協会のもとにクラウド事業者・監査事業者がメンバとなり設立された「クラウドセキュリティ推進協議会」に日立も参加し活動を行っています。

タイトル	Security Guidance for Critical Areas of Focus in Cloud Computing	Cloud Computing Risk Assessment	クラウドサービス利用のための情報セキュリティマネジメントガイドライン	ASP・SaaSにおける情報セキュリティ対策ガイドライン	中小企業のためのクラウドサービス安全利用の手引き
発行者	CSA（Cloud Security Alliance） 米国の非営利団体、ITベンダ、クラウドサービス事業者などが参加	ENISA（European Network and Information Security Agency） 欧州ネットワーク情報セキュリティ庁 （欧州連合（EU）の機関）	経済産業省 商務情報政策局 情報セキュリティ政策室	総務省 「ASP・SaaSの情報セキュリティ対策に関する研究会」	独立行政法人 情報処理推進機構（IPA）セキュリティセンター
対　象	クラウド事業者 クラウド利用者	クラウド事業者	クラウド事業者 クラウド利用者	クラウド事業者	クラウド利用者 （特に中小企業）
概　略	ドメイン（課題領域）の主要な問題点と助言を提示	クラウドのリスクとコントロールを提示	クラウド利用時の確認事項、提供時の用意すべき機能を提示	組織・運用・物理・技術的対策を提示	中小企業向けに確認項目を提示

情報系製品・サービスへの取り組み

「安全・安心クラウド」を実現する情報セキュリティへの取り組み

日立グループでは「Hitachi Cloud」をクラウドにおけるグローバルな統一ブランドとし、これに属す各サービスでは、このような動向も踏まえ「安全・安心クラウド」を実現するための取り組みを行っています。Hitachi Cloudのサービスの1つである「プラットフォームリソース提供サービス」を例にすると、前述のCSA、ENISA、経済産業省のガイドラインを横断的に用い、IaaS/PaaS/SaaSといったサービスの層に関し、サービス利用者と提供者の立場から整理したチェックリストを作成しました。各ガイドラインの特性を踏まえ、多様な情報セキュリティの観点を網羅し、体系的な自己チェックを実施することで、必要な対策・処置の整備を進めています。

特に、CSA Ver. 3.0※1が示す13の分野（Domain）について、それぞれの分野での同サービスとしての指針を明確にし、その指針を実現するために各種施策を実施しています。

1つ例を挙げると、「コンプライアンスと監査」の分野では、クラウドサービスの中でも、お客様のコンプライアンス規定を遵守したサービス実施や監査が必要となります。「プラットフォームリソース提供サービス」では、クラウドの中の処理について、お客様の社内と同等のコンプライアンスが徹底できることを指針としています。この指針を実現する施策としては、コンプライアンスに関わる報告や監査方法をお客様との間で契約に定め、お客様がコンプライアンス遵守を確認できるようにしています。

また、情報セキュリティに関する基準は、業種によっても異なることから、各業種の主要な基準に対する施策の整理も進めています。

1例を挙げると、公官庁・地方自治体などの公共分野においては、内閣サイバーセキュリティセンター（NISC)が、「政府機関の情報セキュリティ対策のための統一基準群（平成28年度版）」※2を発行し、行政機関としての基準を定めています。公共分野へのクラウドサービス適用に関し、これら基準からの要件を整理し、サービスに反映させ情報セキュリティの強化を図っています。

Hitachi Cloudでは、これまで製品事業やSI事業の中で日立が蓄積してきた情報セキュリティについてのノウハウの活用を進めると共に、業界団体や標準化の動向も踏まえ、お客様に安心して使って頂けるクラウドを実現するための取り組みを続けてまいります。

*1：Cloud security alliance : Security guidance for critical areas of focus in cloud computing V3.0
https://cloudsecurityalliance.org/ (2011年11月)
*2：内閣サイバーセキュリティセンター（NISC）：政府機関の情報セキュリティ対策のための統一基準群（平成28年度版）
http://www.nisc.go.jp/active/general/kijun28.html

情報系製品・サービスへの取り組み

パーソナルデータの利活用におけるプライバシー保護の取り組み

IoTやAI、ロボティクス等の技術進展に伴い、多種多量なデータの利活用による超スマート社会の実現が期待されていますが、生活者のプライバシー保護への関心も高い状況にあります。日立は、安全・安心を確保した価値創出に向けてプライバシー保護に取り組んでいます。

パーソナルデータの利活用とプライバシー保護

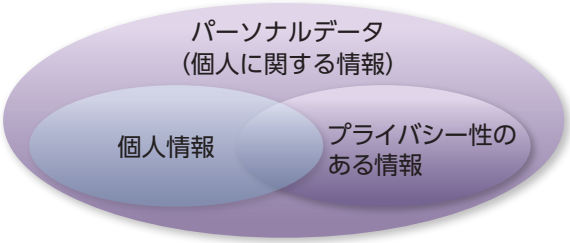
我が国では、2016年に策定された第5期科学技術基本計画において、Society5.0による超スマート社会※1の実現が重点テーマとなりました。さまざまなモノがネットワークでつながり、AI等を活用して多種多量のデータを解析し、新たな価値が創出される社会が期待されており、パーソナルデータを利活用することを有望視しています。

また、国民や消費者のプライバシーを保護するために、制度面の整備や見直しが進められています。我が国では、パーソナルデータの利活用を推進しつつ、個人情報を適切に保護することを目的とし、2017年5月に改正個人情報保護法が全面施行されました。EUでも、一般データ保護規則（GDPR:General Data Protection Regulation）が2018年5月より施行されました。

図1に示す通り、パーソナルデータには、個人情報と一部重複して、"位置情報"や"購買履歴"などのプライバシー性のある情報が含まれます。パーソナルデータの利活用のためには、個人情報保護とともに、プライバシーを保護する必要があり、これらデータを豊かな国民生活の実現に役立てることが社会の発展に大きく寄与します。

※1：必要なもの・サービスを、必要な人に、必要な時に、必要なだけ提供し、社会の様々なニーズにきめ細かに対応でき、あらゆる人が質の高いサービスを受けられ、年齢、性別、地域、言語といったさまざまな違いを乗り越え、活き活きと快適に暮らすことのできる社会。

図1. ベン図「パーソナルデータの種別と関係」>>



日立のプライバシー保護の取り組み

日立は、人々が暮らしやすい持続可能な社会の新しい課題の解決にも積極的・先行的に取り組んでおり、個人やお客様の安全・安心に寄与するべくプライバシー保護の取り組みを進めています。

●プライバシー保護諮問委員会の運営

日立は、2012年よりビッグデータビジネスにおいてプライバシー保護に取り組み、2014年には、情報・通信システム関連部門全体に展開し、プライバシー保護を統括する「パーソナルデータ責任者」およびプライバシー保護に関する知見を集約してリスクの評価や対応策を支援する「プライバシー保護諮問委員会」を設置しています。昨今では、日立全体でのIoTへの注力を背景に支援範囲をIoT事業に拡大しており、個々の社員がお客様と協力して適切な対策を行ない、プライバシーリスクの低減に取り組んでいます。

●プライバシー影響評価の実施

パーソナルデータを取り扱う業務において、日立独自のチェックリストを用いて、プライバシー影響評価を実施しています。加えて、リスクが高い、或いは、判断に悩む案件に関しては、プライバシー保護諮問委員会の専門家がリスク対策を支援しています。これまでの実績は約300件超におよび、実案件における対応実績に基づき、チェックリスト等は常に評価・改善しています。

●プライバシー保護教育

パーソナルデータ利活用とプライバシー保護の両立を図るためには、個々の社員がその重要性を理解し、プライバシー対策を実践する必要があります。そのため、プライバシー保護に関する定期的な教育や情報共有を行うとともに、プライバシー保護のあり方について検討しています。

情報系製品・サービスへの取り組み

日立におけるプライバシー保護対策の事例

●ヒューマノイドロボットの活用による実証実験

ロボットには、カメラやマイクが搭載され、話しかけた方の音声や画像といったパーソナルデータを取得します。このようなロボットによる音声や画像の記録は、まだ一般の人々が容易に想定できる状況にはないと考え、話しかけた方のプライバシー保護に配慮し、実証実験の実施主体や取得データの内容、データ保存期間等を掲示物により告知しました。なお、この掲示物は、人々がロボットに話しかける前に認識できる位置に設置し、問い合わせにも迅速に対応できるよう、相談窓口や対応者を配置しました。

プライバシーに関する掲示

ロボット は録画および録音をしています。

取得したデータは下記の目的にて使用します。

(1) ロボットを用いたサービススタッフとしての事前検証実験

(2) ロボットの機能向上 とその支援システムの機能向上

実施者	株式会社　日立製作所
取得データ	ロボット はカメラとマイクを搭載しています。 ロボット周辺ではこれらデバイスにて映像データおよび音声データを取得しています。
保有・利用期間	日立製作所は、ロボットの実証実験を2年間実施することを計画しています。 取得したデータは、ロボットの機能向上およびその支援システムの機能向上という目的で2年間、保有・利用します。 保有・利用期間終了後、取得したデータは速やかに消去します。
第三者提供の有無	取得したデータの第三者提供は行いません。
お問い合わせ先	お近くのスタッフ、または 株式会社　日立製作所　×××ビジネスユニット　××× 電話：xx-xxxx-xxxx

ロボット周辺（半径3メートル以内）では録画と録音が行われています。
録画や録音を希望しない場合は、ロボット周辺に近づかないようご注意ください。

お客様に安全にご利用いただけるサービス実現をめざして

技術の進展により新たに可能となったパーソナルデータの利活用においても、プライバシー保護は重要です。日立は、2013年にプライバシー保護の取り組みをホワイトペーパーにまとめて公表※2して以降も、多数の業務に対応してきました。これらの経験に基づくノウハウをお客様とのビジネスにおいても活用・展開していくとともに、安心・安全なデータ利活用に関する社会的なコンセンサスを醸成していくため、日立は最新のプライバシー保護の取り組みを踏まえてホワイトペーパーを改訂し、公表しました※3。同書が広く読まれ、お客様にも参考にしていただくとともに、多様な方からご意見をいただきながらこの取り組みを改善していきたいと考えています。

日立は、意識調査や法制度・技術等の動向把握、実案件における対応ノウハウの活用等を通じて、個人の安心を確保し、お客様に安全にご利用いただけるサービスを提供することで、超スマート社会の実現に貢献していきます。

※2:「ビッグデータビジネスにおける日立のプライバシー保護の取り組み」(2013年5月公表)
http://www.hitachi.co.jp/products/it/bigdata/field/statica/wp_privacy.pdf

※3:「パーソナルデータの利活用における日立のプライバシー保護の取り組み」(2017年10月公表)
http://www.hitachi.co.jp/products/it/bigdata/bigdata_ai/personaldata_privacy/index.html

物理セキュリティ製品・サービスへの取り組み

物理セキュリティ製品・サービスによるソリューション強化に向けた取り組み

日立では、オフィス・ビル単位から複数拠点・広域エリアまでを対象に、①映像監視システム、②映像解析システム、③入退室管理システム、④遠隔監視・サポートを提供し、人・モノ・情報の監視・制御やお客様の業務・経営課題解決を支援する物理セキュリティソリューションの強化を図っています。

物理セキュリティ強化の背景

(1) 情報セキュリティと物理セキュリティ

ITの普及やIoT技術の進歩により企業情報や顧客情報のデジタル化が進み、業務システムがネットワーク化したことによって、その情報漏えいのリスクも高まっています。このリスク低減のために情報セキュリティ強化が必要とされています。その一環として、情報を保管する部屋への入室制限、重要施設内の映像監視、ロッカーや金庫などのアクセス管理など、物理セキュリティの必要性が高まっています。

物理セキュリティ導入においては、守る場所、守るものを明確にした上で、適切なセキュリティレベルを設定し、そのレベルに応じたシステムを構築することが重要です。

また、物理セキュリティシステムを構成する各装置には、IoT機器として捉えられるものも数多くあります。このため、セキュリティ対策の弱いIoT機器の乗っ取りやそれに伴う重要システムの侵入等により、物理セキュリティシステムが有する画像データ・個人情報・企業情報の搾取・改ざんや重要システムへの攻撃といったリスクが想定されIoTデータ利活用の活性化は更なる脅威の高まりに繋がります。

物理セキュリティシステム自体に対しても情報セキュリティ対策を施すことが重要です。

(2) オフィス・ビルにおける物理セキュリティ要件

オフィス・ビルの物理セキュリティには、ビルや居室への入退室を管理・制御する入退室管理システムや、オフィス・ビルに出入りする人の流れや各エリアの状況をカメラで監視する映像監視システムがあります。

入退室管理システムは、オフィス・ビル内のエリアごとに必要とされるセキュリティレベルに応じて、ICカードや指静脈認証といった個人認証技術を組み合わせることが重要です。また、PC・業務システムへのアクセス管理や、文書印刷時の認証に用いるといった情報管理システムとの連携や、認証結果に基づいてエレベーターの行先階を制限するといった設備管理システムとの連携も有効な要件です。

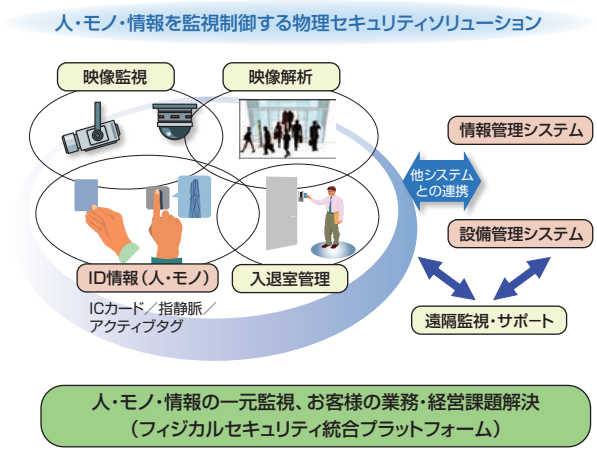
近年は、物理セキュリティ目的だけではなく、映像解析システムや入退室管理システムを設備管理システムと連携させて空調・照明を制御し、省エネを図るという取り組みも重要になっています。

さらに、複数拠点をもつ企業では、各拠点のセキュリティレベルを統一し、統括部門により一元管理することが求められています。

(3) 複数拠点・広域エリアにおける物理セキュリティ要件

発電所・空港・工場・鉄道といった複数拠点・広域エリアの物理セキュリティは、外周、エリア敷地内、車両、ビル等に設置した多数の監視カメラ・入退室管理装置・IoTセンサーによって人・モノの動態（流れや状況）を全体監視することが重要です。

また、複数拠点・広域エリアは非常に多くの動態情報を有するので、ネットワーク帯域と映像格納領域の負荷を低減しながらカメラ映像解析によって不審者・不審物の自動検知を行うなど、多数の装置や複数拠点の情報を集約・自動監視することで監視業務を省力化することも重要です。



物理セキュリティ製品・サービスへの取り組み

ソリューション強化のコンセプトと製品・サービス

物理セキュリティを確保するためには、映像監視システム・映像解析システム・入退室管理システムと個人認証・ID情報管理技術を適切に組み合わせ、また必要に応じて情報管理システムや設備管理システムとの連携運用を図ることで、人・モノ・情報の動態を監視・制御し、お客様の業務・経営課題解決を支援する仕組みを構築することが重要です。

このような考え方に基づき、下記のような特長のある製品・サービスやフィジカルセキュリティ統合プラットフォームを活用したソリューションを提供しています。

(1) 映像監視

近年、IPネットワークを使ったネットワークカメラの導入が進んでいます。各所に設置されたネットワークカメラは、日立が開発した超解像技術により鮮明な映像を1/3～2/3に圧縮することでネットワーク帯域やレコーダ/映像サーバの記憶領域の負荷を低減でき、導入コストを抑えた高度な映像監視システムを提供しています。さらに、多拠点のライブ映像や再生映像を一元管理できる映像統合管理システムも提供しています。

(2) 映像解析

カメラ映像の解析により、人・モノの動態を見える化することができます。カメラ映像に写った人数をカウントしたり、設定した領域に人が滞在したことを侵入として検知したりするなど、監視業務の自動化を進めています。このような映像解析は、設置されたカメラごとに処理を割り付けることができ、状況分析や不審者・不審物・異常行動などの検知に役立てることができます。

(3) 入退室管理

各種非接触ICカード、強固なセキュリティを保証する指静脈認証、無線による個人認証が可能なアクティブタグなどを組み合わせることで、利用環境に適した入退室管理機能を提供することができます。複数の拠点を管理しなくてはならない企業においては、セキュリティポリシーを統一することにより、1枚のカードですべての拠点に入ること許可したり、拠点や部門などの単位で入退室を制限したりするといった権限設定が簡単にできます。

インターネットブラウザによって簡単に操作できるため、容易にシステムを導入・運用することができます。また、各拠点にサーバを置かないクラウド方式でもサービスとして提供でき、中小規模の拠点にも容易に導入可能です。

さらには、情報管理システムや設備管理システムとの連携により、セキュリティ強化や省エネ制御などにも対応可能です。

(4) 遠隔監視・サポート体制

全国に展開した拠点のサービスネットワークとつながっているカスタマーセンター /コールセンターが、24時間365日稼動の常時監視体制で、お客様のセキュリティ関連システムの安定稼動、緊急時の対応をサポートします。

(5) フィジカルセキュリティ統合プラットフォーム

人・モノ・情報の一元監視やお客様の業務・経営課題解決のため、フィジカルセキュリティ統合プラットフォームを活用したソリューションを提供します。

このプラットフォームは、入退室管理装置・監視カメラといった各種フィジカルセキュリティシステムやIoTセンサーによって現場データを収集・蓄積して一元監視するだけでなく、収集・蓄積したデータを分析してお客様の業務・経営課題の改善に向けた情報提供や制御を行うソリューションの構築に活用します。

たとえば、工場や物流現場ではライン作業時のカメラ映像によって正常作業からの逸脱などを検知して是正することで生産性を向上させたり、商業施設ではカメラ映像に写る人物の性別・年齢や購買行動を分析して商品の種類や陳列を変更することで売上向上させたりすることを支援します。

また、カメラ映像だけでなく、各種フィジカルセキュリティシステムやIoTセンサーから収集したビッグデータをBI（Business Intelligence）ツールやAIを活用して分析することで、より高度なソリューションを提供することもできます。

このような特長をもつ物理セキュリティの製品・サービスによって、オフィス・ビル単位から複数拠点・広域エリアまでの資産や安全・安心を守り、お客様の業務・経営課題解決を実現するトータルソリューションの強化を図っています。

制御系製品・システムへの取り組み

制御系製品・システムに対する情報セキュリティ確保の取り組み

重要インフラを支える制御系システムは、近年、情報通信システムとの接続・連携が進み、サイバー攻撃をはじめとする情報セキュリティリスクが高まっています。システムを継続的かつ安定的に運営していくために、これまで以上にセキュアなシステムとお客様の機密情報の厳格管理が求められています。日立製作所 制御プラットフォーム部門は、そうした課題の解決に取り組んでいます。

背景と目的

社会インフラの基盤となる制御系システムを核とする情報制御システムは、24時間稼動することを前提としており、高い信頼性が求められています。情報セキュリティは、安全にかかわるものであり、情報資産を適切に管理、維持、運用し、特にお客様関連情報の機密を完全に維持することにより、情報制御システムの継続的かつ安定的な運営が可能となります。この要件を満足させるため、情報制御システムは、物理的に他システムから遮断することを原則とし、外部からの脅威に対して情報セキュリティを確保しています。一方、「誰もが、自由自在に情報にアクセスできる社会をめざして」という国家IT戦略のもと、「情報連携基盤の開発」等の施策が実行されています。このような環境変化により、情報制御システムに関するセキュリティの脅威が多様化し、情報セキュリティ技術の役割は今後ますます増大していきます。また、システム開発のためにお客様の重要な情報を組み込む場合も多く、これらの情報漏えいは直ちに社会インフラの脅威となります。これらの課題に対する制御プラットフォーム部門の取り組みを以下に述べます。

お客様の機密情報の管理と開発プロセスの整備

●情報セキュリティマネジメントシステム（ISMS）の確立

制御プラットフォーム部門は、電力、交通、鉄鋼、上下水道、産業、パワーエレクトロニクスなどの社会インフラ・産業基盤を支える情報制御システムソリューション事業を展開しており、組織的な情報セキュリティマネジメントを必要としています。また、お客様の情報やそれに基づいて設計する結果の機密保持が特に重要です。制御プラットフォーム部門では、この要請に応えるため、トップマネジメント指揮のもと、情報セキュリティマネジメントシステム（ISMS）の国際規格（ISO/IEC 27001:2005）に基づくISMSを構築し、2010年1月に、情報制御システム部門の認証取得が完了しました。その後も、適用分野の拡大を図りながら、ISMS認証を継続しています。

現在、ISMS国際規格の改訂（ISO/IEC 27001:2013）に伴い、制御プラットフォーム部門のISMSの改訂を推進中です。

●セキュリティを考慮した製品開発プロセスの整備

2005年に以下の開発プロセスを制定し、システム開発に適用してきました。

（1）開発に着手した時点で、セキュリティリスクを洗い出す
（2）設計レビューでセキュリティリスク設計（保護対象の設定、対策方針）を検証する
（3）セキュリティ要件は、工場出荷時およびお客様に引き渡す前に、セキュリティ検査ツール等で確認する

しかしながら、制御系システムに対するセキュリティリスクの高まりと、これに呼応した「国際規格制定と認定の加速」、「顧客の制御ベンダに対するセキュリティ認証取得要求」の動きなど、制御系システムを取り巻く環境にも変化が見られつつあります。

制御プラットフォーム部門では、これらの課題に対して2012年に発足した技術研究組合制御システムセキュリティセンターなど、国内外の組織と連携して対応しています。

国際規格への対応としては、IEC62443やNERC CIP（北米電力の規格）、WIB（欧州の産業系の規格）等の分野ごとの規格の要件を調査し、遵守するべき要件と対応をセキュリティ標準として策定しガイドライン化しました。

制御系製品・システムへの取り組み

制御系システムのセキュリティ

●制御系システムのセキュリティリスクと政府の取組み

制御系システムでは、広域での運用や事業者間での連携、IoT(Internet of Things)技術のシステム適用が開始され、システムが日々進化し、効率化が図られています。その一方でサイバー攻撃は標的型攻撃のように、巧妙化、多様化しており、制御系システムがサイバー打撃を受け、セキュリティの脅威にさらされる事案も出てきています。

政府では、制御系システムへのサイバー攻撃の対策について、内閣サイバーセキュリティセンター (NISC)を中心に各府省庁が連携して取り組んでいます。例えば、2015年11月に「サイバーセキュリティ基本法」が施行され、2015年12月に「サイバーセキュリティ経営ガイドライン」が経済産業省により策定され、サイバー攻撃に起因するセキュリティ脅威への対応が進められています。

●日立のセキュリティコンセプト

制御系システムをセキュリティの脅威から守るためには、その対策は重要ですが、それだけでは十分とは言えません。サイバー攻撃手法は日々進化しており、セキュリティ対策後もシステムの継続的な改善が必要です。さらには、万が一事象が顕在化した場合に、迅速に問題箇所を特定し、対策・復旧できる体制を構築しておくことが大切です。

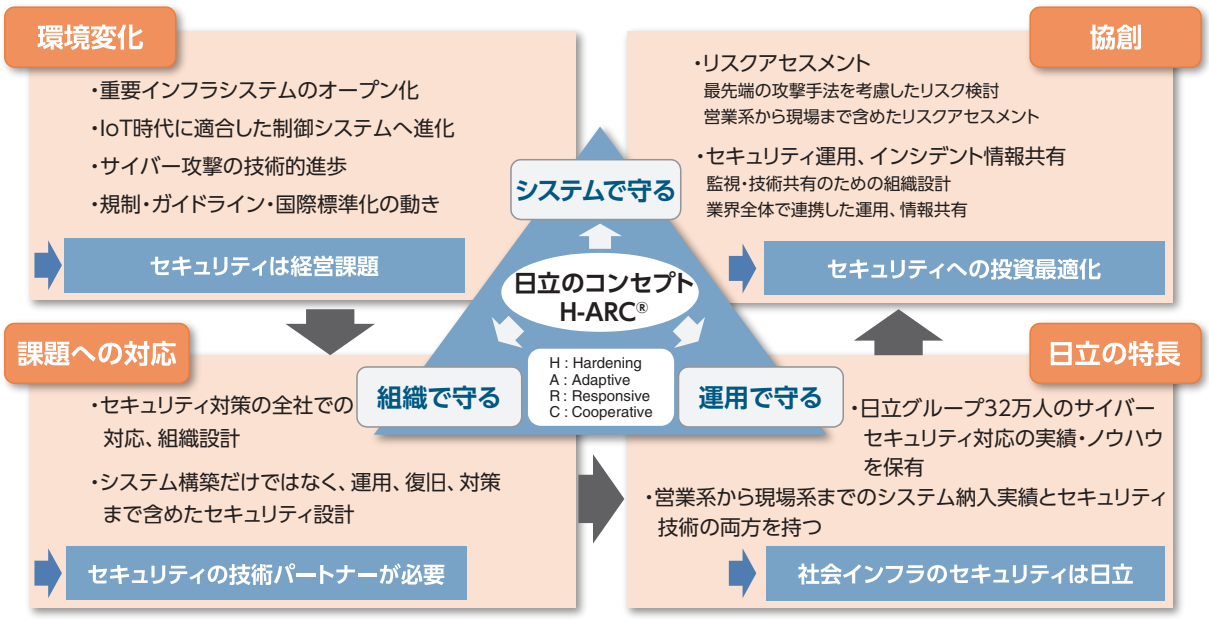
日立製作所では、「システムで守る。組織で守る。運用で守る。」をコンセプトに、H-ARC®という考え方を用いてそのコンセプト実現に取り組んでいます。H-ARC®は、セキュリティ基盤製品(H:Hardening=強じん性)を基に、「システム」で新たな脅威に対する事前対策・防御を継続的に強化・実施(A:Adaptive=適応性)と「運用」で攻撃発生後の被害を最小化・復旧を短時間化(R:Responsive=適応性)と「組織」で異なる組織・事業者間の協調(C:Cooperative=協調性)を支えるセキュリティ運用管理サービスにより、制御系システムを守る考え方です。

●セキュリティ基盤製品

セキュリティ基盤製品として、サイバー・フィジカル両面から製品を提供しています。サイバーセキュリティでは、例えば、サイバー空間での不正侵入を防止するために、外界からの不正アクセスを物理的に遮断し、制御系システムを守ることができる一方向中継装置を提供しています。
一方、フィジカルセキュリティでは、指静脈認証を用いた入退出管理システム、爆発物を探知するためのゲート内蔵型爆発物探知システムを提供しています。

●セキュリティ運用管理サービス

制御系システムを守るためには、セキュリティ対策後も、継続的な監視が必要です。的確なセキュリティ運用設計、セキュリティ脅威の早期把握、迅速な対応を可能としなければなりません。そのためには、制御系システムからのタイムリーな情報収集、効果的な状況分析、的確な対応策の策定、迅速な実行が不可欠です。
日立製作所は、これらを実行するセキュリティオペレーションセンター (SOC:Security Operation Center)の構築、実際の運用代行、セキュリティ技術の専門家や自社のSOCでの運用ノウハウを持つ専門家による分析の支援、セキュリティ脅威に対する人財教育に関するサービスを提供しています。



組織強化への取り組み

サイバー防衛訓練サービス

サイバー攻撃対策にはシステムの強化と並んで、それらに携わる人材や組織の強化も必要となっています。日立では、サイバーインシデント発生時の実践的な対処を目的とした訓練サービスを提供し、重要インフラシステムのセキュリティ強化に貢献していきます。

サイバー防衛訓練サービスの特徴

サイバー防衛訓練サービスでは、ヒトに加えて組織の強化にも着目したサイバー攻撃への対応訓練を提供します。お客様のサイバーBCPの検証や改善を支援し、サイバー攻撃に対して迅速に対応できる組織づくりに貢献します。

実際のサイバーインシデントを再現するために、情報システムと制御システムを実際の企業インフラに近い環境として実装した訓練設備（Nx Security Training Arena）を構築しました。この設備において、日立がこれまで培ってきた技術・ノウハウを基にした訓練カリキュラムを提供します。情報システム・制御システム環境およびカリキュラムはお客様の企業に適したものにカスタマイズしてご提供することも可能です。

サイバー防衛訓練サービスのねらい

（1）情報システムと制御システムの連携環境によるサイバー BCP模擬訓練

情報システムと制御システムが配置された環境を活用し、複数の異なるシステムに対するサイバー攻撃を基点としたサイバー BCPの検証をサポートします。

（2）組織間連携を主眼としたSOC/CSIRT運営訓練

受講生はさまざまな役割（情報システム/制御システム担当者、SOC、CSIRT、マネージャ、経営層など）に分かれて訓練に臨みます。受講生は役割ごとに物理的に隔離された部屋に配置されることで拠点間のコミュニケーションを訓練します。限られたコミュニケーション手段の中でCSIRTやマネージャによるインシデント対応運営訓練を実施します。

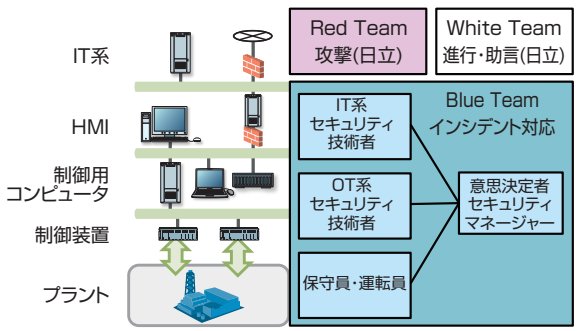
訓練中に受講者が行き詰った場合には、随時、講師が対応方法などをアドバイスします。また、訓練終了後には訓練中の対応などについてのフィードバックもあります。

（3）最新・多様なインシデントパターンへの対応

訓練シナリオでは、機器故障からセキュリティインシデントまで多様な事象を発生させることが可能です。発生しているインシデントがサイバー攻撃に起因する事象か判断するために、複数のシステムの情報を確認するなど複合的な対応を訓練することが可能です。

また、日立内のHIRTや研究所と連携して最新のセキュリティ動向を提供します。

サイバー防衛訓練サービスを通して顕在化した課題や、セキュリティに関する潜在的な課題に対し、日立はNx Security Training Arenaを基点にあらゆる角度から継続的にお客様のより強い組織作りに貢献します。



研究開発

日立のセキュリティビジョンを具現化、さらに進化させるための研究開発

深刻化するサイバー攻撃に対する「組織で守る」「システムで守る」「運用で守る」という3つのセキュリティ提供のアプローチをさらに進化させるためのセキュリティ技術の研究開発に取り組んでいます。

はじめに

近年、サイバー攻撃の脅威が深刻化し、従来のITシステムだけではなく、制御システムを含めた社会インフラ全体に影響を及ぼすようになってきています。これに対して、日立は「組織で守る」「システムで守る」「運用で守る」という3つのセキュリティ提供のアプローチを採用しています。

日立の研究開発部隊は、日立がこれまでに培ってきたセキュリティ技術と、日立の電力、鉄道、ガス、水、製造、情報通信、金融、公共など多種多様な社会インフラシステムに関するノウハウを融合し、この3つのアプローチをさらに進化させるセキュリティ技術の研究開発に取り組んでいます。

「組織で守る」を進化させる

近年、サイバー攻撃の脅威が深刻化する中でセキュリティ対策は必要不可欠なものになっています。しかし、セキュリティインシデントは発生リスクや投資対効果（ROSI）の定量的な算出が困難なため、どこまでコストをかけて対策をとるべきかの判断が難しいと言われています。

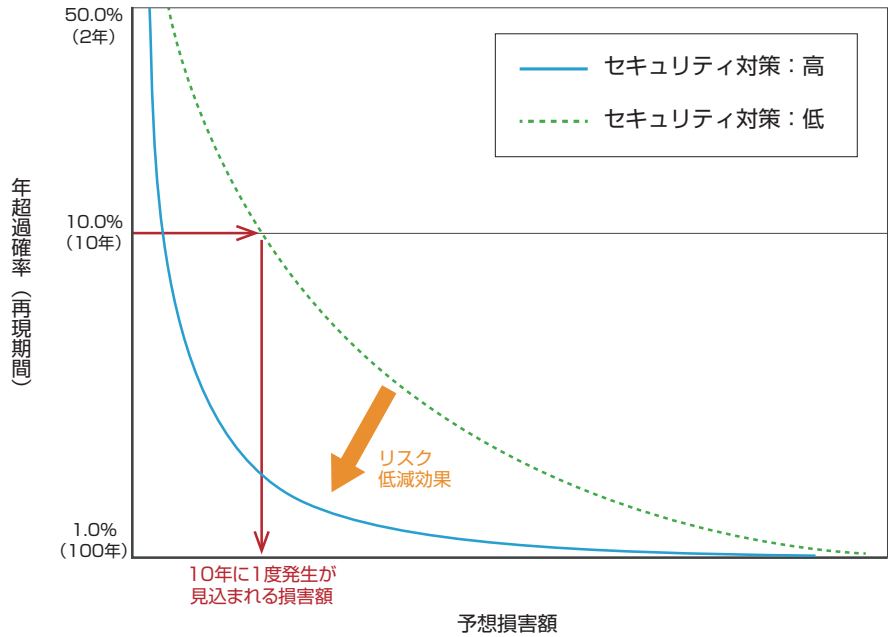
ROSI:Return on Security Investment

●セキュリティリスク診断技術

損保ジャパン日本興亜とSOMPOリスケア、日立の3社は、日本の産業・重要インフラにおけるサイバーセキュリティ対応の促進を目的に共同研究を実施しました。本共同研究では、損保ジャパン日本興亜およびSOMPOリスケアが損害保険事業で培ったリスク評価技術と、日立が産業・重要インフラ分野のシステム構築で培ったセキュリティ対策技術や脆弱性リスクの評価手法を組み合わせ、サイバーリスクの総合的な定量的診断手法の開発を行っています。

具体的には、大規模生産工場を想定し、サイバー攻撃による損害発生リスクをシミュレーションで定量化する技術を開発、検証を行った結果、システム構成やセキュリティ対策状況に応じたサイバーリスクを、セキュリティインシデントの発生率と損害額として算出できることを実証しました。

図. 予想損害額と1年間に予想損害額を超過してしまう確率の関係を示す曲線>>



「システムで守る」を進化させる

サイバー攻撃の対象がITシステムから制御システムを含めた社会インフラ全体へと拡大するにつれ、従来の情報/データの保護を主な目的としたセキュリティ対策だけでは対応しきれなくなってきています。

日立では、従来の情報セキュリティ対策技術では対応できなかった制御システムに対するセキュリティ監視の技術や映像データを分析して不審者などを検出するフィジカルセキュリティ技術を開発しています。

●制御システム向けセキュリティ監視

制御システムは、システム停止が容易でないことから、システム改修を伴うセキュリティ対策を頻繁に施すことが困難です。一方で昨今では、システムを常時監視し日々進化するサイバー攻撃に対応することが求められています。

日立では、セキュリティ監視装置を新たに開発、日立の「NX NetMonitor」をはじめとしたインシデント検知装置群を組み合わせて、既存の制御システムに対しても利用可能なセキュリティ監視ソリューションを開発しました。システムに与える影響が小さいため、頻繁なシステム改修が困難な制御システムにおいても、導入後の検証コストや稼働リスクを最小限に抑えながら、保守員によるインシデントの早期検知と一次対処を実現します。これにより、制御システムにおけるインシデントの発生元や影響範囲の特定を迅速化し、それらをネットワーク接続から遮断する一次対処までを行うことが可能になるため、インシデント被害の拡大を防ぐことができます。

●広域人物追跡技術

空港、駅などの大規模施設や街区などの公共空間では、安全確保のために防犯カメラによる監視や警備が行われています。しかし、限られた人員で全ての映像を確認することは困難なため、これまで、服装の色や、入口などで事前に撮影した顔の画像を手掛かりに、人物を発見・追跡する技術が開発されてきました。

日立は、AIによって性別や年齢層、服装など多数の特徴情報をリアルタイムに判別することで該当する人物を見つけ出し、さらに、その人物がどのような足取りを取ったのかを、リアルタイムに広域の防犯カメラ映像の中から抽出する技術を開発しています。本技術の特長は以下の通りです。

（1）人物の外見と動作の特徴を判別・検索する、高速人物発見技術

（2）人物の全身画像を詳細に解析し、同一人物の映像を抽出する、高速人物追跡技術

図. 本技術を活用した広域人物追跡システム

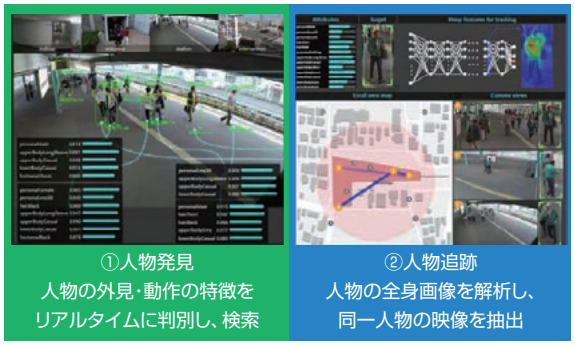
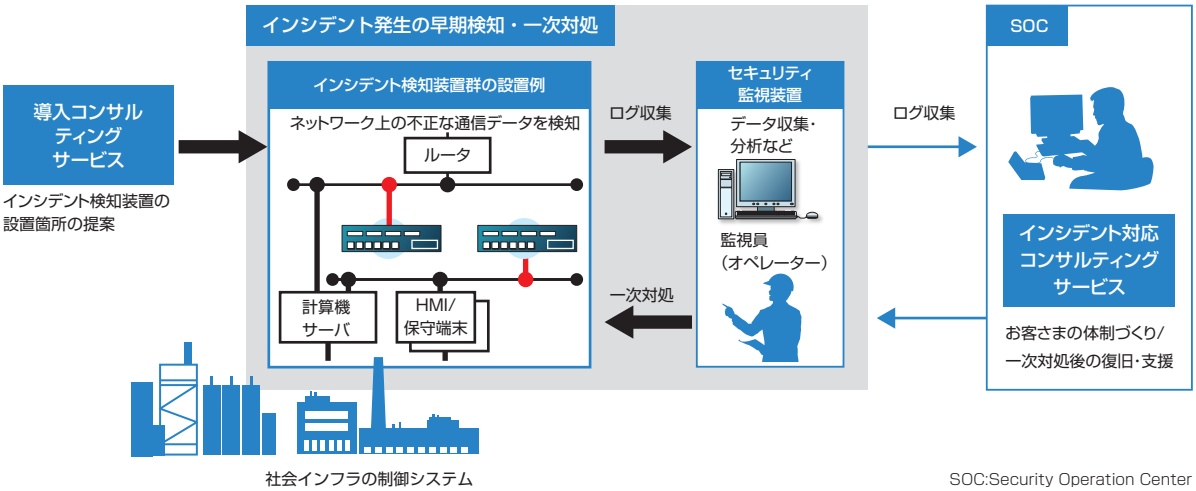


図. 制御システム向けセキュリティ監視のイメージ >>



研究開発

「運用で守る」を進化させる

サイバー攻撃は年々増加しており、短時間に多拠点が攻撃されるリスクも高まっています。日立では、サイバー攻撃の増加/高度化に対応したセキュリティ運用を実現するため、AIを活用してセキュリティ監視業務を効率化/高度化する技術や、複数の組織間でインシデントに共同対処する技術を開発しています。

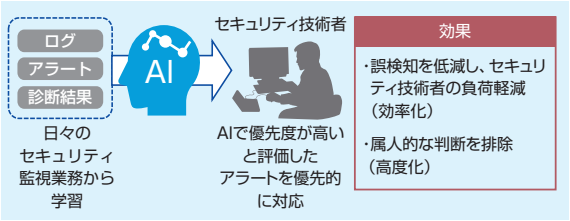
●AIを活用したセキュリティ監視業務の効率化・高度化

セキュリティ監視業務では、SIEM等のセキュリティ機器が上げるアラートをアナリストが分析、本当のインシデントによるものかを判定しています。膨大なアラートへの対応はアナリストにとって大きな負荷となっています。

日立では、このようなアナリストの分析業務を代替する、AI活用アラート自動判定技術を開発しました。本技術では、まずAIが過去のアラートと人の判断結果との関係性を学習、学習関係性に基づき、アラートの対策優先度を自動で判定します。過去のアラートの分析結果といった「事実」を基にAIが判定を行うため、アナリストによって判定結果が異なることも回避できます。実証実験を行った結果、見逃しを防止しつつ最大95%のアラートを削減し、大幅な効率化ができることを確認しました。

SIEM:Security Information and Event Management

図. セキュリティ監視業務へのAI活用のイメージ >>



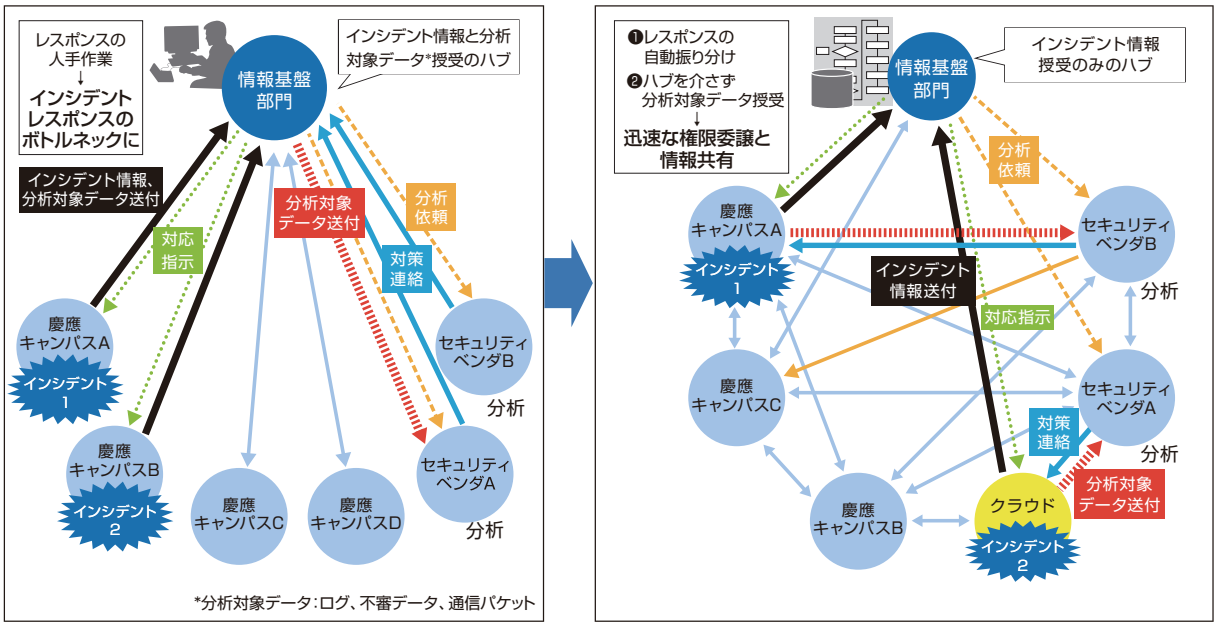
●分散セキュリティオペレーション

従来のインシデントレスポンスでは、特定のセキュリティ対応チームをハブとして、インシデント情報と分析データを集約、人手作業で複数のセキュリティ対応チームに分析依頼と分析データの送付を行っていました。

日立は、「分散型セキュリティオペレーション」という、特定のセキュリティ対応チームがすべてのインシデントレスポンスに関与するのではなく、各組織にあるセキュリティ対応チームが自律分散的にインシデントに対処し、必要に応じて連携する技術を開発しています。情報収集や分析など、インシデントレスポンスに求められる機能を形式化/標準化し、それぞれのセキュリティ対応チームが持つ機能を互いにリアルタイムで確認、処理を委託する専門チームを機械的に振り分けます。

本技術の効果を検証するため、慶應義塾インフォメーションテクノロジーセンターで監視しているインシデントの分析対象データを、日立の「オープンラボ横浜」に送付、分析を委託する実証環境を構築、評価を開始しました。

図. 分散セキュリティオペレーションのイメージ >>



図（a）従来のセキュリティオペレーション

図（b）動的認証認可技術を用いた分散型セキュリティオペレーション

研究開発

本人認証技術を進化させる

セキュリティ確保には、正当な権限を持つ人物かどうかを確認する本人認証が欠かせません。これまで、日立は、指静脈認証技術を開発、入退室システムや金融サービスなどへ展開してきました。デジタル化の進展に伴い、本人認証はより多様なサービスで必要となっています。「組織で守る」「システムで守る」「運用で守る」を進化させる上でも本人認証は要となります。そこで、日立独自の指静脈認証技術をコアに、本人認証技術を進化させる技術の開発も進めています。

● ウォークスルー型指静脈認証技術

現在用いられている多くの本人認証方式では、立ち止まって認証を行う必要があるため、人が集中すると混雑が発生します。一方、立ち止まらずに本人を認証する方式では、高い認証精度を得にくいという課題があります。

日立は、指静脈認証技術をさらに進化、(1) かざした複数の指の位置や向きを瞬時に検知する技術、(2) 指の位置や向きに合わせて静脈パターンを撮影する技術、を開発しました。これにより、さまざまな位置や向きでかざした指の静脈を瞬時に検知、多くの人が集まる大型施設でも、歩きながら指をかざすだけのスムーズで正確な本人確認を実現します。

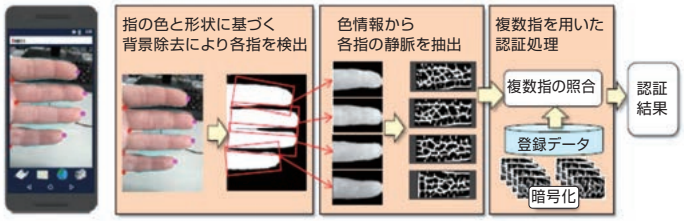
● スマホ指静脈認証技術

近年、オンラインショッピングや個人情報の管理などをスマートフォンで行う利用者が増えています。スマートフォンでの本人認証手段には、パスワードや指紋などの方法がありますが、より安全で高精度な方式の需要が高まっています。

日立は、スマートフォンに標準搭載されたカメラで高精度に指静脈認証を実現する技術を開発しました。

具体的には、スマートフォンのカメラで撮影したカラー画像から各指を検出、静脈パターンを安定的に抽出するとともに、複数の指の静脈パターンを組み合わせることで認証精度を高めます。これにより、偽造やなりすましが困難な指静脈認証がスマートフォンで利用できるようにしました。

図. スマートフォン搭載のカメラによる指静脈認証の基本原理 >>



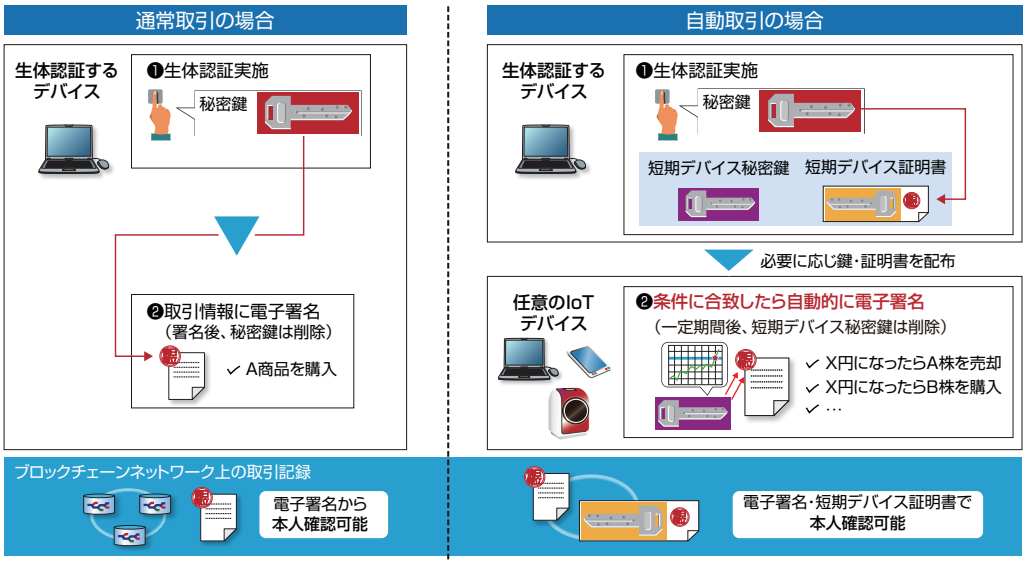
● PBI-ブロックチェーン技術

ブロックチェーンは、第三者機関の仲介なしで取り引きが可能な取引基盤として、仮想通貨取引、商品売買、病院での受診履歴管理など多様な用途への活用が期待されています。ブロックチェーン上での取引の信頼性は、ユーザーが取引情報に対して電子署名を付与し、その正当性を誰もが検証可能にすることで担保されています。一方で、電子署名を生成するための鍵が紛失・漏えいすると、ブロックチェーン上の資産喪失や、なりすましによる不正取引発生につながります。

日立は、生体情報から電子署名を生成できる、日立独自の技術、PBIをブロックチェーン上で利用可能とする、PBI-ブロックチェーン連携技術を開発しました。生体情報自体を鍵として利用できるため、鍵を外部管理する必要がなくなります。また、設定した条件に従って電子署名を自動生成可能な、自動取引向け短期デバイス証明書生成技術も開発、取り引きごとに認証してはならない煩わしさも解消しました。

PBI:Public Biometrics Infrastructure

図. PBI-ブロックチェーン連携技術の概要 >>



情報セキュリティに関する社外活動

日立では、従業員それぞれのもつ経験や知識を活かし、情報セキュリティに関する各種社外活動に参画することにより、よりセキュアなIT社会の実現のために活動しています。

国際標準化活動

次のセキュリティに関する国際標準化活動に参画しています。

●ISO/IEC JTC1/SC27

国際標準化機構（ISO）と国際電気標準会議（IEC）による国際標準化のための合同技術委員会ISO/IEC JTC1のサブコミッティであるSC27では、情報セキュリティマネジメントシステム（WG1）、暗号とセキュリティメカニズム（WG2）、セキュリティ評価技術（WG3）、セキュリティコントロールとサービス（WG4）、アイデンティティ管理とプライバシー技術（WG5）に関する規格化が検討されています。

●ISO TC292

ISOのテクニカルコミッティ（TC）292では、一般的なセキュリティマネジメント、事業継続マネジメント、レジリエンスおよびエマージェンシーマネジメント、不正防止対策および管理、セキュリティサービス、ホームランドセキュリティ等、様々なセキュリティに関する規格化が検討されています。

●ISO TC262

ISOのTC 262はリスクマネジメントをテーマとしており、全てのリスクを対象とし、用語、原則および指針、リスクアセスメント技法などの規格化が検討されています。

●ITU-T SG17

国際電気通信連合（ITU）の電気通信標準化部門（ITU-T）のスタディグループ（SG）のひとつであるSG17では、サイバーセキュリティ、通信事業者向けセキュリティ管理、テレバイオメトリクス、通信･アプリケーションサービスに対するセキュリティ機能、スパム対策、ID管理などの規格化が検討されています。

●IEC TC65/WG10, WG20

IECのTC 65では産業用オートメーション、計測、制御の標準化が進められています。その中のWG10では、制御システムにおけるネットワークと制御装置のセキュリティに関する規格化が検討されています。また、WG20では、制御システムにおけるセキュリティと機能安全の両立に関する規格化が検討されています。

●OASIS CTI

構造化情報標準促進協会（OASIS）のサイバー脅威インテリジェンス（CTI）では、サイバー攻撃活動を記述し、交換するための脅威情報構造化記述形式、検知指標情報自動交換手順に関する規格化が検討されています。

シーサート（CSIRT）活動

日立では、日立グループにおけるシーサート活動に加え、HIRT（Hitachi Incident Response Team）を窓口（PoC: Point of Contact）として社外シーサート活動に参画しています。また、社外シーサート組織等との連携として、脆弱性等に関する情報の共有・交換を推進しています。

●FIRST

FIRST（Forum of Incident Response and Security Teams）は、大学、研究機関、企業、政府機関などが加盟する信頼関係に結ばれたインシデント対応チームの国際コミュニティです。2018年6月末時点で、89ヵ国、431チームが加盟しています。

●日本シーサート協議会（NCA）

日本で活動するシーサート組織間の情報共有・連携を通して、シーサート活動上の課題解決を図るために設立された団体です。シーサート設立の促進・支援、インシデント発生した場合のシーサート間の連携体制作りなど、国内のシーサートコミュニティが、いざというときに協力できるよう、組織自身が自主的に「インシデント対応基礎能力」の向上を図れる場を提供しています。日立は、協議会発足メンバーであり、2015年からは運営委員長の立場で、国内のシーサート活動の普及を推進しています。

その他活動

上記活動に加えて、次に示すセキュリティに関する研究・検討、普及・啓発などを推進する各種社外活動へ参画しています。また、全国で開催される各種セミナー、学会などにおける講演も行っています。

- 独立行政法人情報処理推進機構（IPA）10大脅威執筆者会 他
- 一般財団法人日本情報経済社会推進協会（JIPDEC）ISMS専門部会、制御システムSMS専門部会 他
- 一般財団法人日本サイバー犯罪対策センター（JC3）
- 特定非営利活動法人日本セキュリティ監査協会（JASA）
- NPO日本ネットワークセキュリティ協会（JNSA）
- 日本ISMSユーザグループ（J-ISMS UG）
- 一般社団法人日本電気計測器工業会（JEMIMA）PA・FA計測制御委員会、セキュリティ調査研究WG
- 技術研究組合制御システムセキュリティセンター（CSSC）
- 一般社団法人電子情報技術産業協会（JEITA）情報セキュリティ調査専門委員会 他
- 一般社団法人ICT-ISAC
- フィッシング対策協議会
- 独立行政法人製品評価技術基盤機構（NITE）評価機関認定技術委員会
- ロボット革命イニシアティブ協議会 産業セキュリティアクショングループ

他

第三者評価・認証

日立では、個人情報保護、情報セキュリティマネジメント、製品に関する第三者評価・認証の取得を推進しています。

プライバシーマーク取得状況

日立が一般財団法人 日本情報経済社会推進協会（JIPDEC）から取得したプライバシーマークの使用許諾状況は、以下のとおりです（2018年5月末日現在）。

株式会社日立製作所
株式会社日立製作所　病院統括本部
日立健康保険組合
日立オムロンターミナルソリューションズ株式会社
株式会社日立社会情報サービス
沖縄日立ネットワークシステムズ株式会社
株式会社日立情報通信エンジニアリング
株式会社日立コンサルティング
株式会社日立インフォメーションエンジニアリング
株式会社日立ICTビジネスサービス
株式会社日立インフォメーションアカデミー
株式会社日立テクニカルコミュニケーションズ
株式会社日立システムズ
株式会社北海道日立システムズ
株式会社日立システムズエンジニアリングサービス
株式会社日立システムズネットワークス
株式会社セキュアブレイン
株式会社四国日立システムズ
株式会社日立システムズフィールドサービス
株式会社九州日立システムズ
株式会社日立システムズパワーサービス
株式会社日立ソリューションズ
株式会社日立ソリューションズ・クリエイト
株式会社日立ソリューションズ東日本
株式会社日立ソリューションズ西日本
日立SC株式会社
株式会社日立ハイシステム21
株式会社日立フーズ&ロジスティクスシステムズ
株式会社日立インスファーマ
株式会社日立パワーソリューションズ
株式会社日立産業制御ソリューションズ
株式会社日立ケーイーシステムズ
株式会社日立ビルシステム
株式会社日立ハイテクソリューションズ
日立ヘルスケアシステムズ株式会社
株式会社日立ソフテック
株式会社日立保険サービス
株式会社日立アーバンインベストメント
株式会社日立アーバンサポート
株式会社日立ドキュメントソリューションズ
株式会社日立ドキュメントプリンティング
株式会社日立総合計画研究所
株式会社日立技術情報サービス
株式会社日立マネジメントパートナー

ISMS認証取得状況

日立が、一般社団情報マネジメントシステム認定センター（ISMS-AC）から情報セキュリティマネジメントシステム国際規格（ISO/IEC 27001）に基づくISMS認証を取得した組織は、以下のとおりです（2018年5月末日現在）。

株式会社日立製作所（金融第二システム事業部 公共系金融システム部門）
株式会社日立製作所（社会ビジネスユニット　公共システム事業部）
株式会社日立製作所（サービス&プラットフォームビジネスユニット 制御プラットフォーム統括本部）
株式会社日立製作所（サービスプラットフォーム事業本部）
株式会社日立製作所（社会システム事業部）
株式会社日立製作所（ヘルスケアビジネスユニット　ヘルスケアソリューション事業部第一部
株式会社日立製作所 ディフェンスビジネスユニット（横浜事業所/池袋分室）及び株式会社日立アドバンストシステムズ（本社）
日立オムロンターミナルソリューションズ株式会社
株式会社日立社会情報サービス
沖縄日立ネットワークシステムズ株式会社
株式会社日立インフォメーションエンジニアリング
株式会社日立ICTビジネスサービス（メディアソリューション部　メディアサービスグループ）
株式会社日立システムズ（公共・社会事業グループ）
株式会社日立システムズ（金融プラットフォーム事業部ソリューション本部　クラウド基盤サービス部）
株式会社日立システムズ（公共プラットフォーム事業部）
株式会社日立システムズ（コンタクトセンタ&ビジネスサービス事業部）
株式会社日立システムズ（SHIELD　セキュリティセンタ）
株式会社日立システムズ（スマートソーシング&サービス事業部）
株式会社北海道日立システムズ（公共・社会システム統括本部/民需システム統括本部）
株式会社四国日立システムズ
株式会社九州日立システムズ（アプリケーション事業部）
株式会社日立システムズパワーサービス（マネージドサービス事業部データセンタ運営本部 データセンタシステムサポート部 第三システムサポートグループ）
株式会社日立ソリューションズ（セキュリティ診断業務）
株式会社日立ソリューションズ・クリエイト（官公庁関連のシステム開発・システム構築及び保守サービス）
株式会社日立ソリューションズ西日本（SaaS型給与支援システムの環境構築、及び運用管理）
日立SC株式会社（本社）
株式会社日立ファルマエヴォリューションズ
株式会社日立パワーソリューションズ（カスタマーサービス部SRCグループ及び遠隔監視グループ）
株式会社日立ケーイーシステムズ（東京オフィス開発センター）
日本スペースイメージング株式会社
株式会社日立ハイテクソリューションズ（ソリューションセンター）
株式会社日立国際電気（東京事業所）
株式会社HYSエンジニアリングサービス（サービス統括本部）
株式会社 日立マネジメントパートナー

ITセキュリティ評価・認証の取得状況

（独）情報処理推進機構（IPA）が運用するISO/IEC 15408に基づく「ITセキュリティ評価および認証制度」によって認証された主な製品は、次のとおりです（2018年6月末現在[認証製品アーカイブリストへの掲載を含みます]）。

製　品	TOE種別※1	認証番号	評価保証レベル※2
HiRDB/Parallel Server Version 8 08-04	データベース管理システム	C0225	EAL4+ALC_FLR.1
HiRDB/Single Server Version 8 08-04	データベース管理システム	C0216	EAL4+ALC_FLR.1
HiRDB Server Version 9（Linux版）09-01	データベース管理システム	C0351	EAL2+ALC_FLR.2
Smart Folder PKI MULTOS application 03-06	スマートカード用アプリケーション ソフトウェア	C0014	EAL4
Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software 8.0.1-02	Access Control Device and Systems	C0536	EAL2+ALC_FLR.1
Hitachi Virtual Storage Platform G1000, Hitachi Virtual Storage Platform VX7 Control Program 80-01-25-00/00（R8-01A-06_Z）	ストレージ装置制御ソフトウェア	C0514	EAL2+ALC_FLR.1
Hitachi Unified Storage VM Control Program 73-03-09-00/00（H7-03-10_Z）	ストレージ装置制御ソフトウェア	C0513	EAL2+ALC_FLR.1
Hitachi Unified Storage 110用マイクロプログラム　0917/A	ストレージ装置制御ソフトウェア	C0421	EAL2
Hitachi Unified Storage 130用マイクロプログラム　0917/A	ストレージ装置制御ソフトウェア	C0420	EAL2
Finger Vein Authentication Device UBReader2 Hardware: D, Software: 03-00	生体認証装置	C0332	EAL2
証明書検証サーバ 03-00	PKI	C0135	EAL2
CBTエンジン 01-00	CBT試験システム 主要アプリケーション	C0288	EAL1+ASE_OBJ.2、 ASE_REQ.2、ASE_SPD.1
汚染拡大防止システム SHIELD/ExLink-IA 1.0	セキュリティ管理ソフトウェア	C0090	EAL1

暗号モジュール試験・認証の取得状況

IPAが運用するISO/IEC 19790に基づく「暗号モジュール試験および認証制度（JCMVP）」または米国NISTとカナダCSEが運用するFIPS140-2に基づく「Cryptographic Module Validation Program（CMVP）によって認証された主な製品は、次のとおりです（2018年6月末現在）。

製　品	認証番号	レベル
Hitachi Virtual Storage Platform（VSP）Encryption Adapter	2727	Level 2
Hitachi Virtual Storage Platform（VSP）Encryption Board	2694	Level 1
Hitachi Virtual Storage Platform（VSP）Encryption Module	2462	Level 2
Hitachi Virtual Storage Platform（VSP）Encryption Engine	2386	Level 1
Hitachi Unified Storage Encryption Module	2232	Level 1
HIBUN Cryptographic Module for User-Mode 1.0 Rev.2	JCMVP #J0015、CMVP#1696	Level 1
HIBUN Cryptographic Module for Kernel-Mode 1.0 Rev.2	JCMVP #J0016、CMVP#1697	Level 1
HIBUN Cryptographic Module for Pre-boot 1.0 Rev.2	JCMVP #J0017、CMVP#1698	Level 1
Keymate/Crypto JCMVP ライブラリ（Solaris版 および Windows版）	JCMVP #J0007	Level 1
Keymate/Crypto JCMVPライブラリ	JCMVP #J0005	Level 1

※1. TOE（Target Of Evaluation）
評価の対象となるソフトウェアやハードウェアなどの製品のことをTOEといいます。関連する管理者および使用者の手引書（利用者マニュアル、ガイダンス、インストール手順書など）を含むことがあります。

※2. EAL（Evaluation Assurance Level）
ISO/IEC 15408では、規定した評価項目（保証要件）に対する保証の度合いを、EAL1から7まで7段階のレベルで規定しており、段階が上がるごとに評価の内容が厳しくなります。
・EAL1は、セキュリティ機能の妥当性とテスト、セキュリティを維持するためのガイダンスが客観的に評価されます。
・EAL2は、一般的な攻撃能力を想定した脆弱性分析、製造から運用開始まで、製品の完全性の観点から評価が追加されます。通常の開発ライフサイクルにセキュリティ的な視点を加味しています。
・EAL3は、EAL2で得られる保証に加えて、テストの網羅性や開発時の製品の改ざんを防止するための開発環境の評価が実施されます。
・EAL4は、一般的な商用製品として最高位とされており、開発環境での開発資産の保全性やソースコード、要員の信頼性など開発ライフサイクル全般にわたって評価されます。
・ALC_FLR.1は、製品にセキュリティの欠陥が発見された場合、必要なパッチを提供する基本的な手続きを客観的に評価します。規格では規定のEALに含まれない保証要件を追加することができ、その場合、EAL2+ALC_FLR.1のように表記します。
ALC_FLR.2は、利用者からの脆弱性情報の報告受付けと利用者への通知手続きが求められます。

日立グループの概要

会社概要 (2018年3月末日現在)

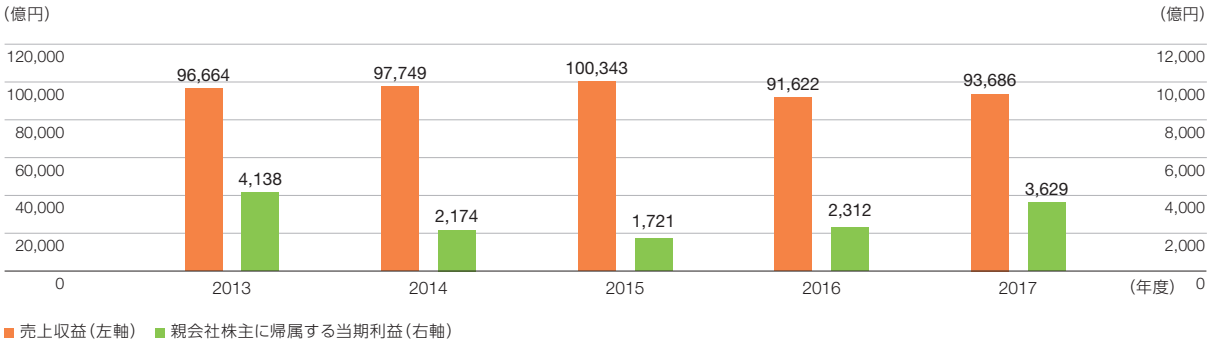
商号	株式会社 日立製作所 Hitachi, Ltd.
設立年月日	大正9年(1920年)2月1日 (創業明治43年〈1910年〉)
本店の所在地	東京都千代田区丸の内一丁目6番6号
代表者	代表執行役 執行役社長兼CEO 東原 敏昭
資本金	458,790百万円
従業員数	(個別)34,925人 (連結)307,275人
連結子会社数	879社(国内202社、海外677社)
持分法適用会社数	407社

財務ハイライト (2018年3月期連結IFRS)

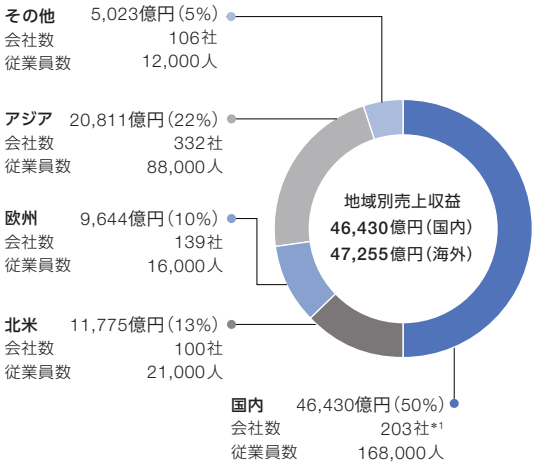
売上収益	93,686億円(前期比102%)	設備投資額*2	3,749億円(前期比99%)
EBIT*1	6,442億円(前期比136%)	研究開発費	3,329億円(前期比103%)
継続事業税引前当期利益	6,386億円(前期比136%)	総資産額	101,066億円
親会社株主に帰属する当期利益	3,629億円(前期比157%)		

※当社の連結財務諸表は、国際財務報告基準(IFRS)に基づいて作成しています
*1 EBIT:継続事業税引前当期利益から、受取利息の額を減算し、支払利息の額を加算して算出した指標
*2 2015年度より、従来、設備投資額に含めていたファイナンス、リースに該当する賃貸資産への投資額について、設備投資額から除いて開示しています

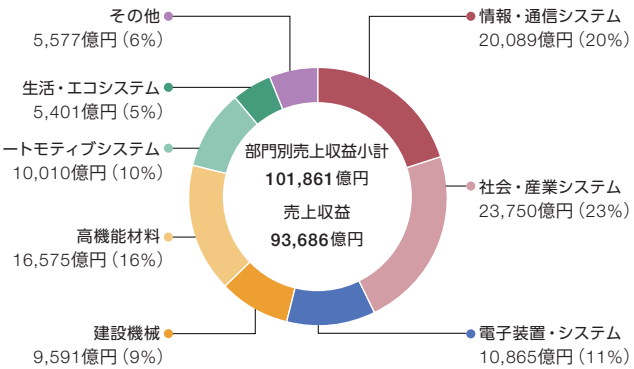
●売上収益／親会社株主に帰属する当期利益の推移



●地域別売上収益／構成比
(2018年3月期 連結IFRS)



●事業部門別売上収益／構成比
(2018年3月期 連結IFRS)



*1 株式会社日立製作所および国内連結子会社202社、計203社

株式会社 日立製作所
情報セキュリティリスク統括本部
〒100-8280 東京都千代田区丸の内一丁目6番6号
TEL.03-3258-1111

Printed in Japan (H) (2018.09)