HITACHI
Inspire the Next

情報セキュリティ報告書 2016

Information Security Report 2016

日立グループ

ごあいさつ

日立グループは、長年培ってきた制御・運用などのOT（Operational Technology）と先進的なIT、プロダクト・システムを組み合わせ、お客様やパートナーとの協創によって新たな価値を創造する、社会イノベーション事業に取り組んでいます。今後は、更にデジタル技術を活用してソリューションを進化させてIoT（Internet of Things）時代のイノベーションパートナーをめざし、安心・安全・快適に暮らせる社会の実現に向けて貢献していきたいと考えております。

近年、情報セキュリティを取り巻く環境は急激に変化してきています。ネット社会やIT技術の急速な進展により、クラウド、スマートデバイス、SNSなど、経済性や利便性に寄与する新技術やサービスの利用拡大に伴い、情報セキュリティに対するリスクが高度化・複雑化しています。特に、昨今増大している標的型攻撃メールなどによるサイバー攻撃は益々巧妙化してきており、不正アクセスによる情報搾取に加え、重要設備に障害を与えるなど社会への影響が深刻になっています。一方で、IoTやビッグデータなどを通じてお客様の企業情報や一般市民の皆様の個人情報を扱う企業として、プライバシーの保護を含む人権を意識した経営が必要になってきていると認識しています。

このような中、日立グループは従来から「情報セキュリティ方針」のもと、規則・体制の整備、IT技術などを活用した安全対策の整備、一般従業員やセキュリティ専門職への教育、監査による点検など、情報セキュリティマネジメントサイクルをグローバルで推進し、情報セキュリティの充実を図っております。また、サイバーセキュリティを強化するために、官民が連携した取り組みにも積極的に参画するとともに、日立インシデントレスポンスチームを中心に全社の事業部門が連携し、蓄積してきたノウハウと最新技術を駆使し、こうした脅威への対抗策を開発・構築してまいりました。ここで確立した成果はお客様にも提供することで、より一層安心・安全な社会インフラシステムにおけるイノベーションの実現をめざしてまいります。

本報告書でご紹介する私たちの情報セキュリティに関する活動が、少しでも皆様のお役に立ち、日立グループに対する更なる信頼の向上につながれば幸いです。

株式会社 日立製作所
執行役専務 CIO
大森 紳一郎

情報セキュリティ報告書

INDEX

日立グループにおける情報セキュリティへの取り組み

製品・サービスの情報セキュリティ確保に向けた取り組み

〈本報告書の概要〉

●報告範囲・期間：2015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：2016年8月発行

情報セキュリティガバナンスの基本的な考え方

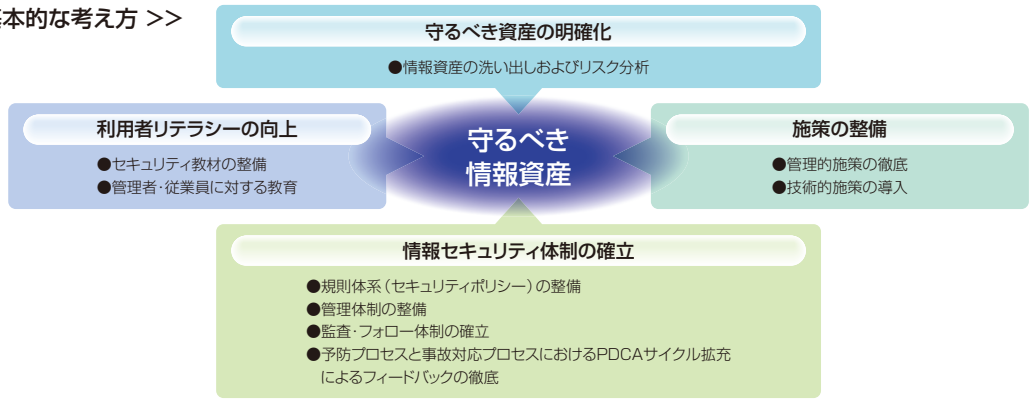
情報セキュリティガバナンスの取り組み方針

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 >>



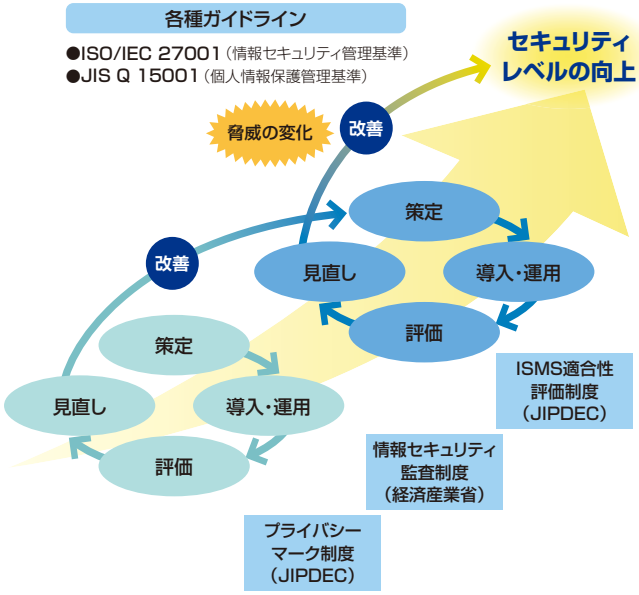
（1）予防体制の整備と事故発生時の迅速な対応

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、トータルソリューションを提供できるグローバルサプライヤーとして、日立の技術情報や、お客様からお預かりしている情報など、さまざまな情報を取り扱っており、これらの情報価値を保護するために、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適切な維持に努めています。

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洩の防止、マイナンバーなど個人情報の保護など、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展開しています。

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。

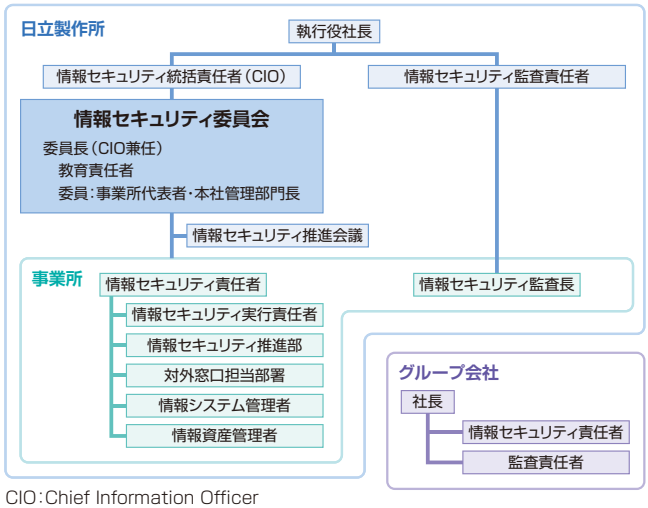
情報セキュリティ委員会の決定事項は、全事業所実務者が出席する情報セキュリティ推進会議を通じて、各事業所に徹底されます。

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。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 >>



CIO：Chief Information 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、下表に記載のごとく規則を定め、情報セキュリティの維持に努めています。

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

グループ会社も同等の規則を定め、情報の管理を行うよう推進しています。

●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。「情報及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 15001:2006) 相当の規則としています。

「個人情報管理規則」は、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き等について定めています。

「個人情報取扱業務委託規準」は、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、個人情報の適切な管理・保護を定めています。

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、PDCA（Plan-Do-Check-Action）のサイクルに則って実施しています。

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。

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教育プログラムを設けて実施しています。

情報セキュリティに関する教育一覧 >>

対象者	形　態	内　容
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
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。

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及しています。

安全・安心な日立の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、日立グループ製品の更なる醸成に役立てています。

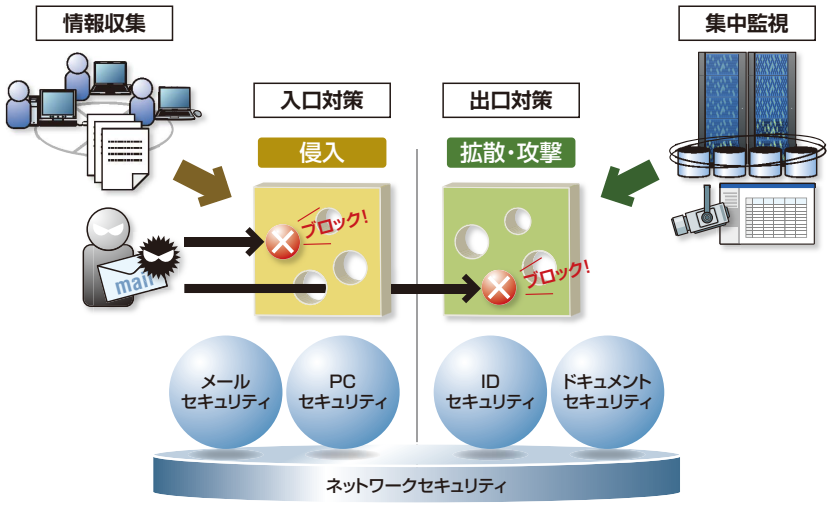
日立のITセキュリティ体系とサイバー攻撃に対応した多層防御

日立のITによるセキュリティ体系は、大きくは、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、PCセキュリティ、ドキュメントセキュリティ、IDセキュリティから成り、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、以下の考え方に則り、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

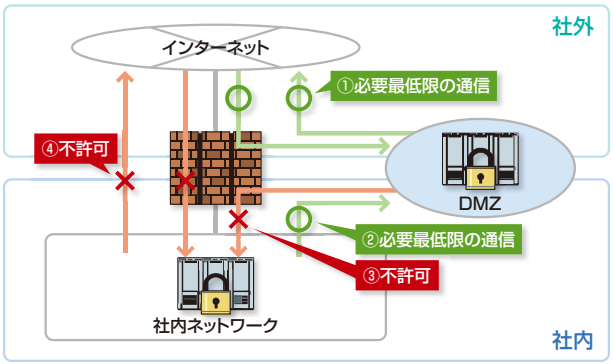
ネットワークセキュリティ

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。

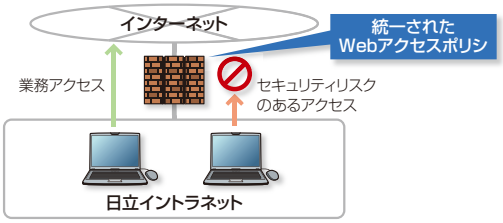
※1：DeMilitarized Zone　※2：Intrusion Prevention System



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。

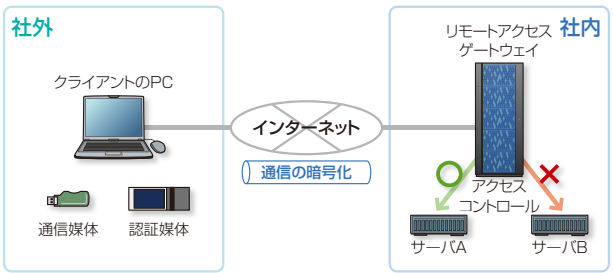
- 認証による、利用者の限定とログ保存およびログ監査
- 統一されたポリシーによる、URLフィルタリング
- Webウイルスチェック



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



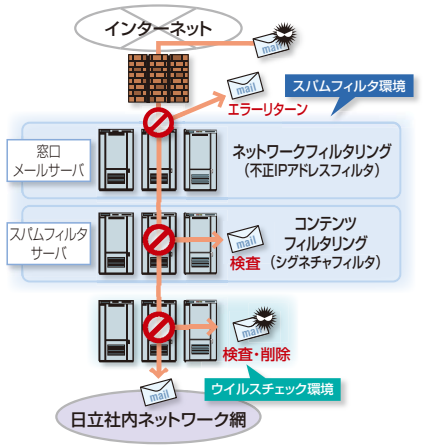
情報セキュリティに対する技術面での取り組み

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

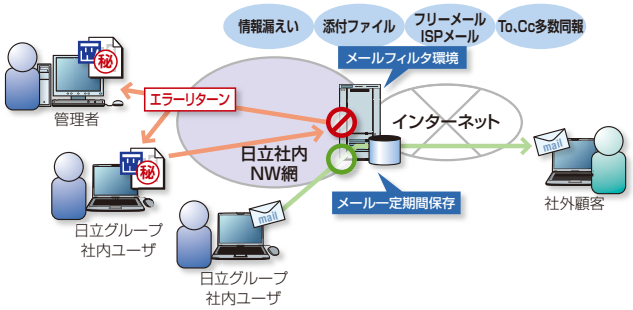
〈スパムフィルタ、ウイルスチェック構成〉



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。

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。



PCセキュリティ

情報を取り扱う道具・器であるPCのセキュリティ対策は、社内システム環境の末端（エンドポイント）に位置づけられ、最後の砦と考えられています。

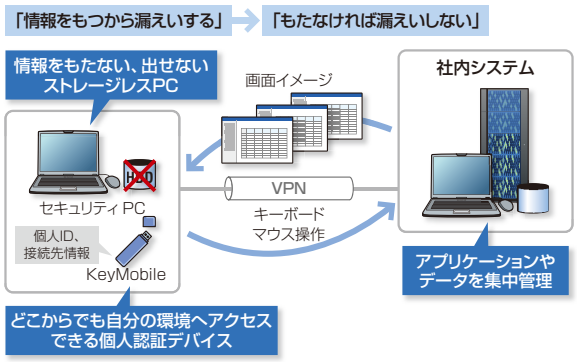
PCに関するリスクとして、以下が挙げられますが、内部・外部要因の組み合わせによってリスクが変化します。

（1）PC、外部媒体の持ち出しによる情報漏えい

（2）脆弱個所を突く不正アクセス、コンピュータウイルス感染

（1）については、次の2点に重点を置いて防止対策を講じています。

●モバイルPCのシンクライアント化

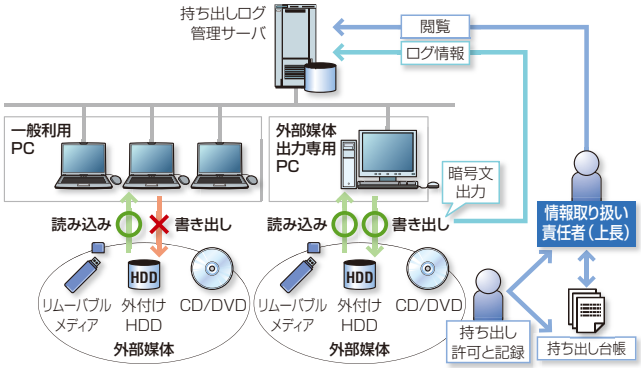


情報セキュリティに対する技術面での取り組み

●外部媒体の書き出し抑止と書き出し時のログ管理

従業員が利用するPCからは外部媒体への書き出しができないようにしています。情報を持ち出す場合、上長の承認を得て、専用PCから書き出します。定期的に書き出しログを確認し、不正持ち出しがないか確認します。

PCはその脆弱性によって時間の経過とともにリスクが高まりますが、定期的な対策が施されているか、点検するシステムを構築し、PCのセキュリティの維持・管理に取り組んでいます。



IDセキュリティ

情報セキュリティの基盤として、個人単位の「認証」「アクセス制御」が不可欠です。日立グループでは共通の認証基盤を構築し、グループ全体のセキュリティレベルの均一化、底上げを実施しています。

認証基盤の目的は次の3点です。

1. 認証／アクセス制御情報の管理

IT利用者の情報を共通システムで一元的に管理して情報の更新漏れを防ぎ、情報の鮮度維持、精度向上を図っています。

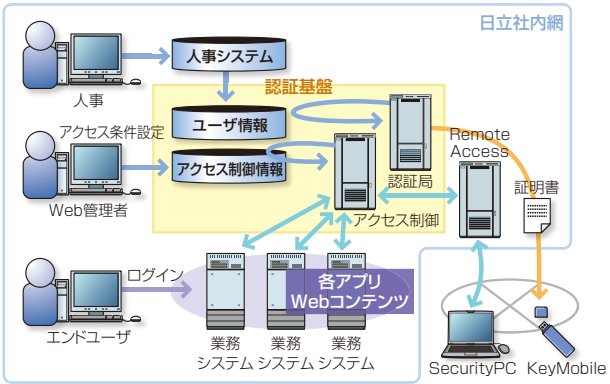
2. 個人単位での認証とアクセス制御

IT利用者単位に複数のアクセス権限を管理し、適切なアクセス制御を実施しています。

3. ユビキタス環境の促進

各業務システムが共通のアクセス制御を利用することで、日立グループの従業員ならどこからでも同じ条件で必要なシステムが利用できます。

なお、認証基盤へ格納する情報は鮮度が維持された、高い精度の情報でなければなりません。



そのため、以下の2つの措置を講じています。

1. IDの登録

人事部門が利用者の情報を登録し、更新された情報は即時に認証基盤へ反映させています。

2. 鮮度維持

IDはパスワードに有効期限を設定するだけでなく、IDそのものにも有効期限を設定し、期限経過後はIDが失効します。

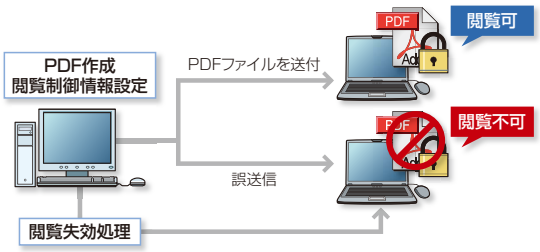
情報セキュリティに対する技術面での取り組み

ドキュメントセキュリティ

情報共有等でドキュメントの交換が頻繁に行われる半面、情報漏えいのリスクが高まっています。特に、電子ドキュメントは簡単に複製できることから情報漏えい時には被害が拡大します。このような状況を踏まえて、次の防止対策を講じています。

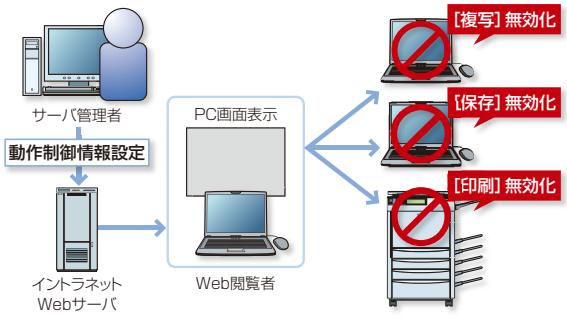
1. 電子ドキュメントの閲覧停止による情報漏えい防止

一般的には電子ドキュメントが漏えいした場合、その閲覧を停止することはできません。その対策として、ドキュメントに閲覧、複写、印刷などの可否を設定でき、万一、外部にドキュメント情報が流出した場合は、所持者の失効処理により、当該ドキュメントを閲覧停止できるようにしています。



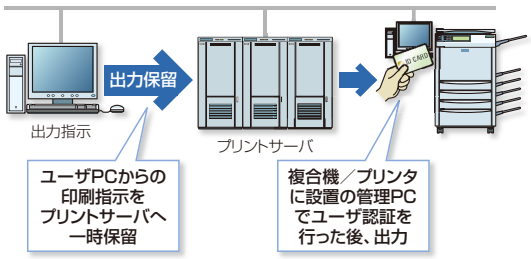
2. Webサーバコンテンツの情報漏えい防止

社内の情報共有にイントラネットWebが広く利用されていますが、ブラウザ上に表示された情報はパソコンにダウンロードすることが可能であり、また、紙媒体への印刷も可能であることから情報漏えいの危険性を常にはらんでいます。そのため、Webサイトに掲載している各コンテンツに複写、保存、印刷の可否を設定し、情報漏えいのリスクを軽減しています。



3. プリンターの出力用紙による情報漏えい防止

プリンターによって印刷された用紙が放置されていると、情報漏えいの原因となります。この問題は、PC上で印刷操作をした後、用紙の引き取り忘れによって発生するため、PC操作に加えプリンターでの操作を行うことで解決できます。PCからの操作ではプリンターサーバに印刷情報が蓄積されるのみとし、プリンター側に設置する管理PCから操作することによって、初めて用紙への印刷が可能となります。このとき、印刷者を特定するため、管理PCではIDカードによる個人認証を行います。



クラウド活用におけるセキュリティへの取り組み

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。

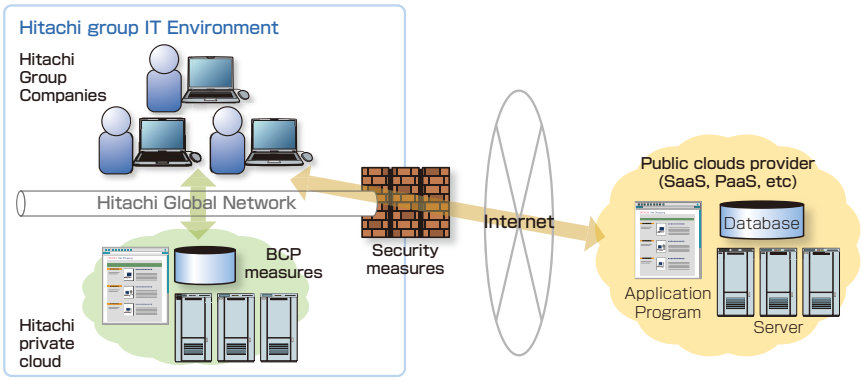
クラウド活用におけるセキュリティへの取り組み

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

図1 パブリッククラウドの位置付け >>



SaaS: Software as a Service　PaaS: Platform as a Service　BCP: Business Continuity Plan

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

物理セキュリティ強化の推進

情報漏えいの防止と防犯のためには、オフィスへの入退管理や防犯カメラの設置など物理セキュリティ対策が不可欠です。日立グループでは、全社統一方式の物理セキュリティ対策を推進しています。

物理セキュリティ対策の全社統一化

従来の物理セキュリティ対策は、入退管理を中心に各事業所が個別方式で行っていましたが、対策強化のため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全社統一基準による整備方式・管理の均質化

②日立グループの製品・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

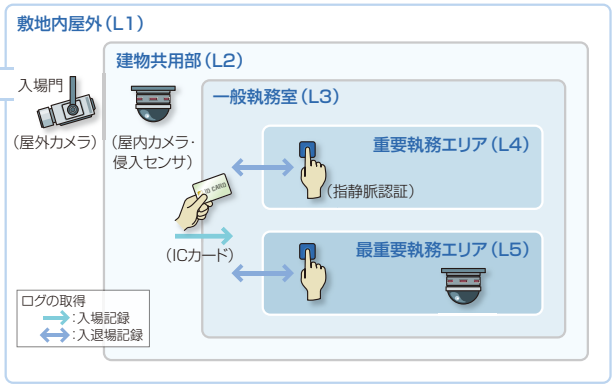
(1) 管理区域のセキュリティレベルの設定と整備の統一化

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、レベルに応じて入退管理方式、防犯カメラおよび侵入センサの設置基準を定めるとともに、設備を統一しています。

(2) 日立グループの製品と技術の活用

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。特に重要区域へ入場する際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。

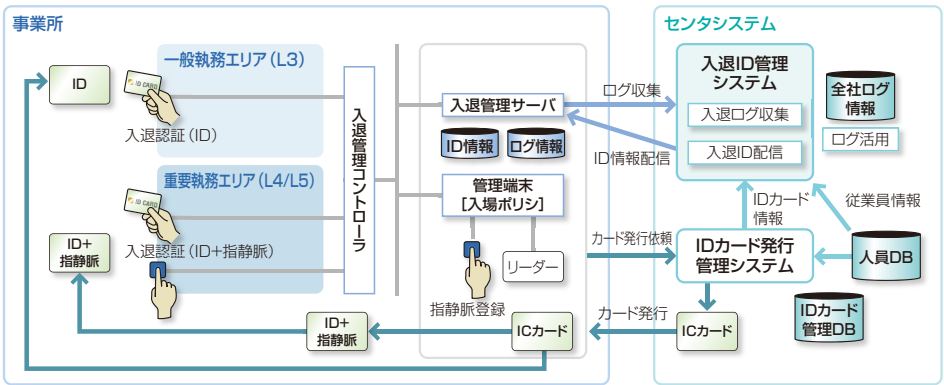
区域のセキュリティ対策レベルと対策方式 >>



(3) センタシステムを活用した運用業務の効率化

事業所の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を活用したIDカード発行管理システムと入退ID管理システムを開発し、使用しています。入退ログ等のフォレンジックデータを一元的に管理し、有効活用しています。

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。

ヒアリング等により、お取引先様のセキュリティ対策状況を確認

↓

お取引先様に情報セキュリティ要求基準を提示

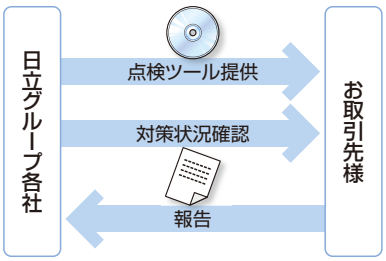
↓

情報漏えい防止契約を締結

(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。

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

セキュリティインシデントへの取り組み

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。

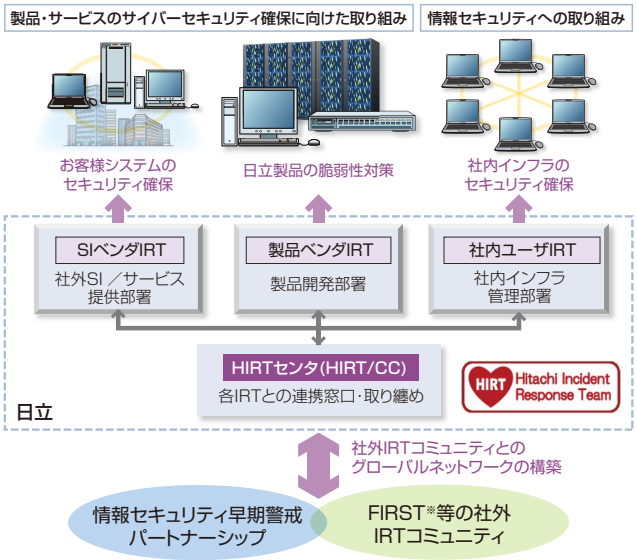
HIRTは、脆弱性対策とインシデント対応とを推進するために、下記のように、4つのIRT（Incident Response Team）という活動モデルを採用しています。4つのIRTとは、

（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

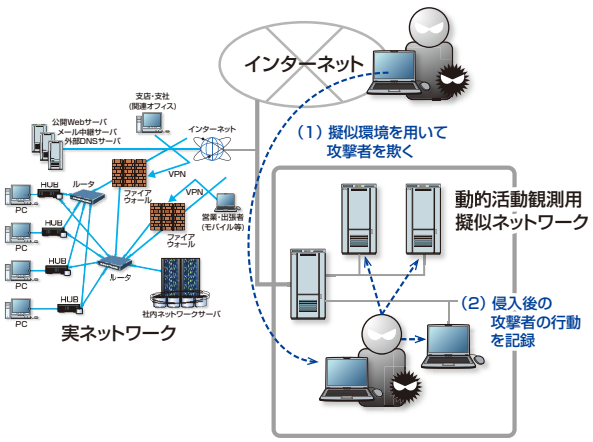
情報セキュリティ早期警戒パートナーシップ※1の推進などを通じて、脆弱性対策ならびにインシデント対応に関する情報やノウハウを組織内に展開しています。

※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。

攻撃者の行動を記録する動的活動観測システム >>



(3)製品・サービスのセキュリティ技術の向上

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、開発・管理プロセスの整備、エキスパート人材への技術継承を推進しています。

(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。

●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

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※2を用いた情報利活用基盤の整備、日本シーサート協議会を通じた組織間IRTの連携を推進しています。

※2 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※3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※4などを活用したインシデントオペレーションを推進しています。

※3 FIRST: Forum of Incident Response and Security Teams
※4 STIX: Structured Threat Information Expression

(3)研究活動基盤の整備

学術組織との共同研究、マルウェア対策研究人材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、人材育成の場の醸成、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/

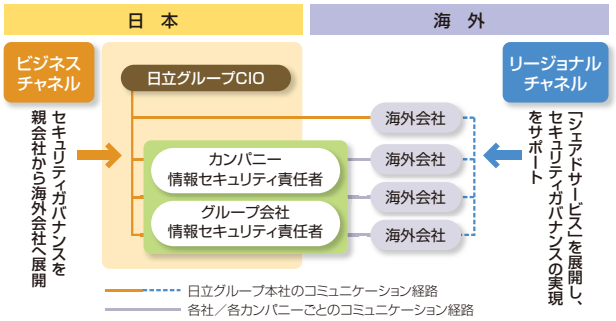
グローバル情報セキュリティの取り組み

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。

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、2015年3月に4回目の更新をしました。

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

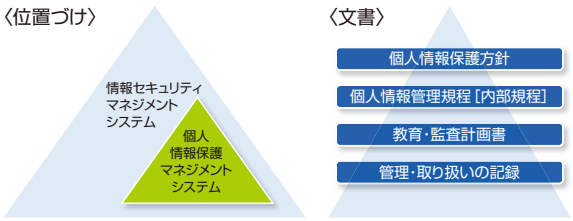
個人情報保護に対する取り組み

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。

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。

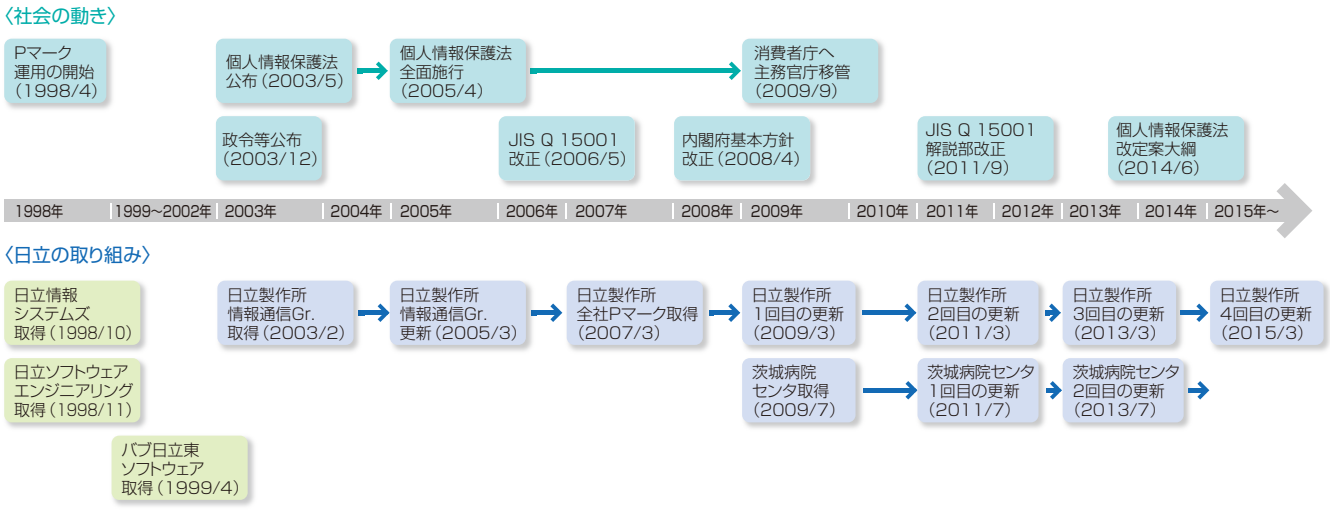
日立グループ全体の取り組み（プライバシーマーク取得推進状況）

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。2016年5月31日現在、57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 >>



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の活動を推進しています。この活動は、 グループ会社とも連携して推進しています。

セキュリティ確保への取り組み

お客様に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に、以下に示すセキュリティ方針、セキュリティ3か条を定め、そのもとで取り組みを推進しています。

情報系製品・サービスの提供に用いる情報システムおよび製品・サービス自体のセキュリティ品質の確保・維持のためのガイドラインの策定、施策の立案、情報セキュリティ関連技術動向の把握等の活動を実施しています。

●セキュリティ方針

深化した情報を迅速活用する社会の進展に対して、安全で信頼できる情報システム基盤を提供することは情報系製品・サービスを提供する事業者の使命である。

その活動は製品・サービスの事業者として、また日立グループ共通プラットフォームの利用者として、情報セキュリティを確保し、これを利用するお客様を含むあらゆるステークホルダの安全と価値に寄与するものでなければならない。

●セキュリティ 3か条

(1) セキュリティマネジメントシステムの確立

セキュアな情報系製品・サービスの提供とセキュリティインシデントへの迅速な対応のため、セキュリティマネジメントシステムを確立し、自主的に改善する。

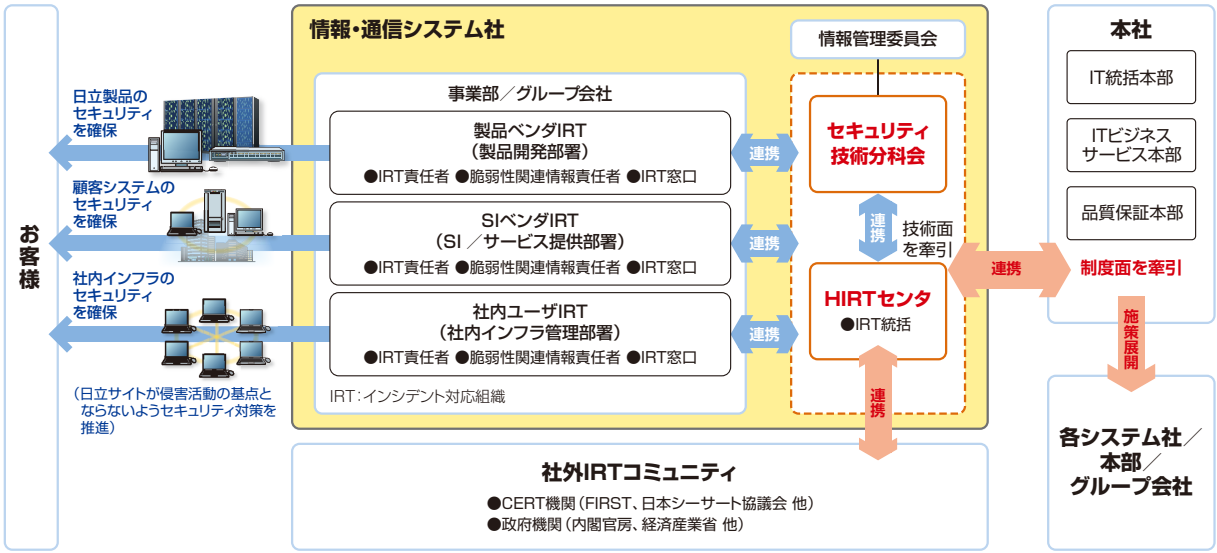
(2) セキュアな情報系製品・サービスの提供

製品・サービスおよびその開発・運用の業務プロセスにおけるセキュリティ確保のため、セキュリティ機能を設計・実装し、定期的な点検を行い運用し、セキュアな情報系製品・サービスを 提供する。

(3) セキュリティインシデントへの迅速な対応

社内外のセキュリティインシデントをモニターし、提供する情報系製品・サービスにかかわるセキュリティインシデントに速やかに対応する。また、脆弱性対策情報を利用者に開示し、セキュリティ事故の予防に努める。

●15年度推進体制



HIRT:Hitachi Incident Response Team(セキュリティインシデント／脆弱性対策対応組織。日立内専門家で構成)
FIRST:Forum of Incident Response and Security Team

情報系製品・サービスへの取り組み

グループ会社における活動

情報系製品・サービスを提供するグループ会社においても、提供する製品・サービスの情報セキュリティを確保するための組織を設置し、以下のような活動を推進しています。

(1) Webセキュリティの確保

社内外Webサイト／システムのセキュリティ品質確保のための専任部署を設置し、Webセキュリティインシデントに迅速に対応するとともに、自社Webサイト／システムのセキュリティに対する品質確保を支援（定期的な社外公開Webサイト／社内システムの診断、社外公開サイトの申請受付／合議／承認手続きの実施、Webセキュリティ関連の予防処置）しています。

(2) 開発・構築プロセスにおけるセキュリティの確保

セキュアなシステム構築のためのガイドラインを策定し、セキュリティ設計チェックリスト、脆弱性検出ツールなどを活用しています。

(3) 技術者向けセキュリティ教育

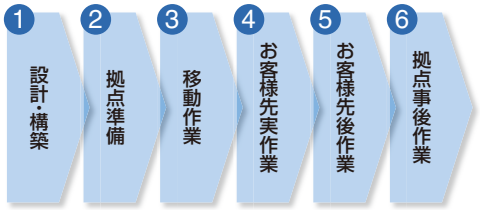
Webアプリケーション脆弱性防止対策講座、開発言語別セキュリティ講座、脅威分析講座などの技術教育により、開発・構築に携わる技術者のセキュリティレベルの向上、セキュリティ意識の向上を図っています。

(4) システム運用・保守サービスにおけるセキュリティの確保

システム運用・保守サービスの提供にあたっても、お客様の情報資産の漏えい、盗難、紛失、改ざん、不正使用などが発生しないようにセキュリティを確保しなければなりません。そのためにシステム運用・保守サービス提供の業務プロセスを明確にし、各プロセスでの行動を規定するセキュリティ規格を策定し、その規格に沿って活動しています。例えば、設計・構築プロセスでは、お客様の情報資産の特定、リスクの洗い出しと管理策の策定を行い、関係者への周知徹底を図っています。また、お客様先での実作業プロセスにおいて保守交換した障害HDDに対しては、トレーサビリティ確保の対策を講じています。

システム運用・保守サービス提供の業務プロセス >>

〈お客様向けサービス提供〉



〈社内日常作業〉

情報系製品・サービスへの取り組み

オープンミドル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。システムの中核を担う日立のオープンミドル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

日立が提供するオープンミドルウェア製品は、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。オープンミドル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の実施。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26年経済産業省告示第110号「ソフトウエア等脆弱性関連情報取扱基準」、「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。

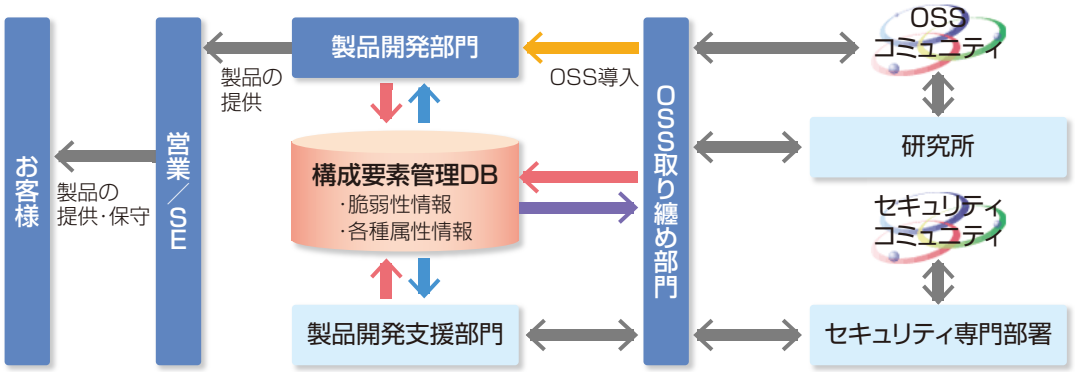
※HIRT：Hitachi Incident Response Team
　CSIRT：Computer Security Incident Response Team

情報系製品・サービスへの取り組み

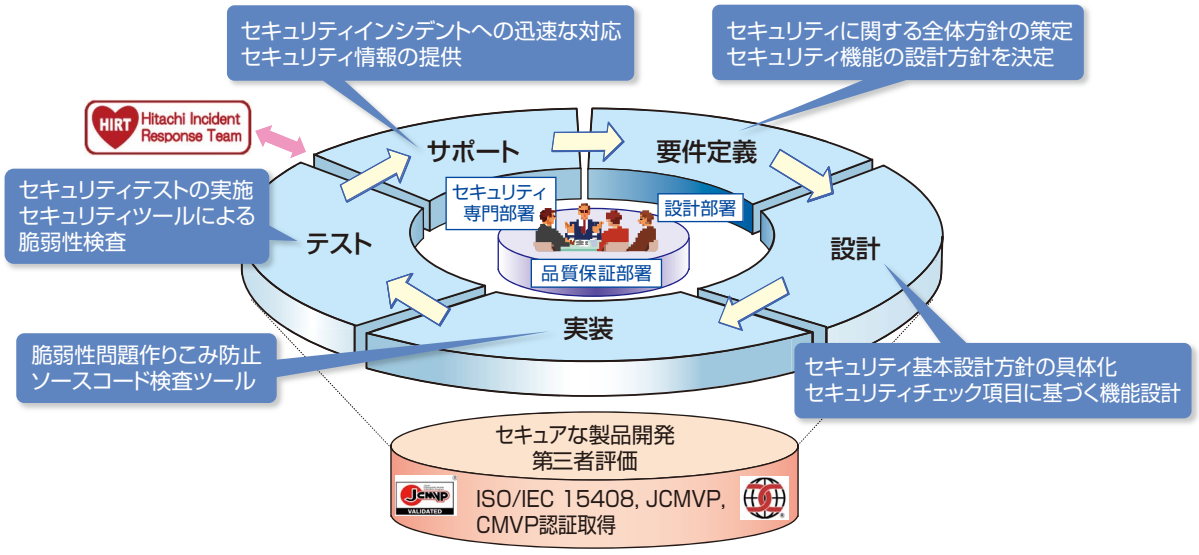
オープンソースソフトウェア（OSS）への対応

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、HiRDB、Hitachi Command Suiteといった主要なオープンミドルウェア製品で認証を取得しています。

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 >>

■日立製作所オープンミドルウェアのISO/IEC 15408情報

http://www.hitachi.co.jp/Prod/comp/soft1/sec_cert/index.html

JCMVP (Japan Cryptographic Module Validation Program)

CMVP (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）

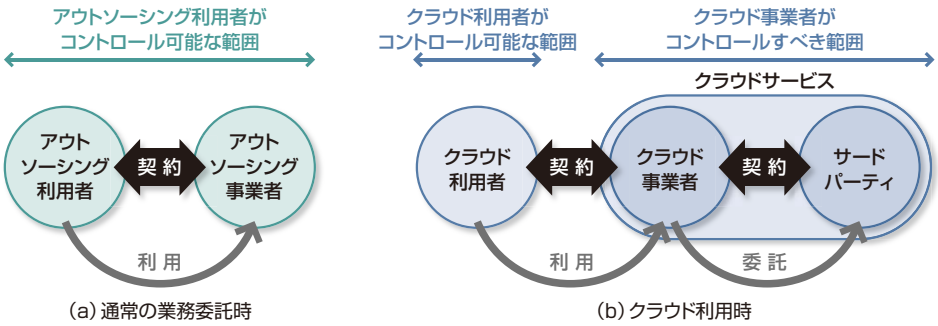
新たなITの提供形態であり、社会インフラの1つとなるクラウドにおいて、日立は種々のセキュリティに関する取り組みを行い、企業情報システムに適用可能な「安全・安心クラウド」を実現します。

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>>



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。

特に、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2015年12月に規格化されました。

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。

これらの取り組みについては、その内容を解説したホワイトペーパ※2を広く公開しています。

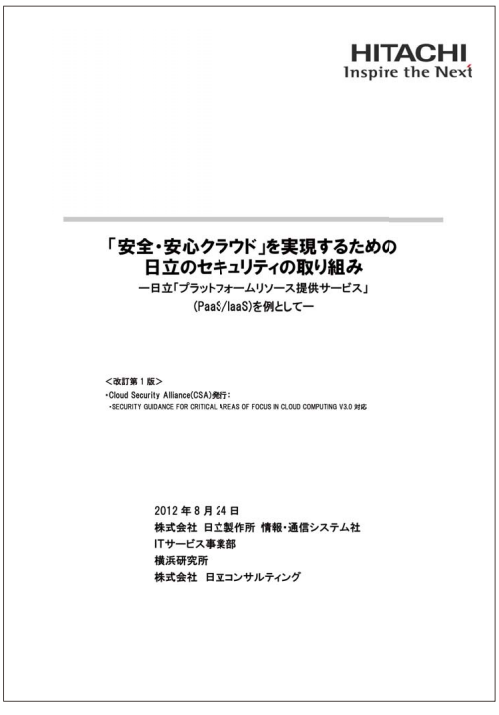
情報セキュリティに関する基準は、業種によっても異なることから、各業種の主要な基準に対する施策の整理も進めています。

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（平成26年度版）」※3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。この内容もホワイトペーパの『公共編』※4として公開しました。

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)
＊3：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（平成26年度版）
http://www.nisc.go.jp/active/general/kijun26.html
＊2、＊4：日立製作所：「安全・安心クラウド」を実現するための日立のセキュリティの取り組み
－ 日立「プラットフォームリソース提供サービス」（PaaS/IaaS）を例として －
－ 公共分野における日立「プラットフォームリソース提供サービス」（PaaS/IaaS）を例として －
http://www.hitachi.co.jp/cloud/solution/paas/platform.html

ホワイトペーパ >>



情報系製品・サービスへの取り組み

ビッグデータビジネスにおけるプライバシー保護の取り組み

近年の情報通信技術の進展に伴い、ビッグデータが大きな関心を集めている一方、ビッグデータを巡るプライバシー侵害の懸念も根強く指摘されています。日立では、ビッグデータの利活用を支援するサービスを展開する際に、お客様の安全・安心を確保する観点から、プライバシーを保護するための枠組みの構築に取り組んでいます。

ビッグデータとプライバシー

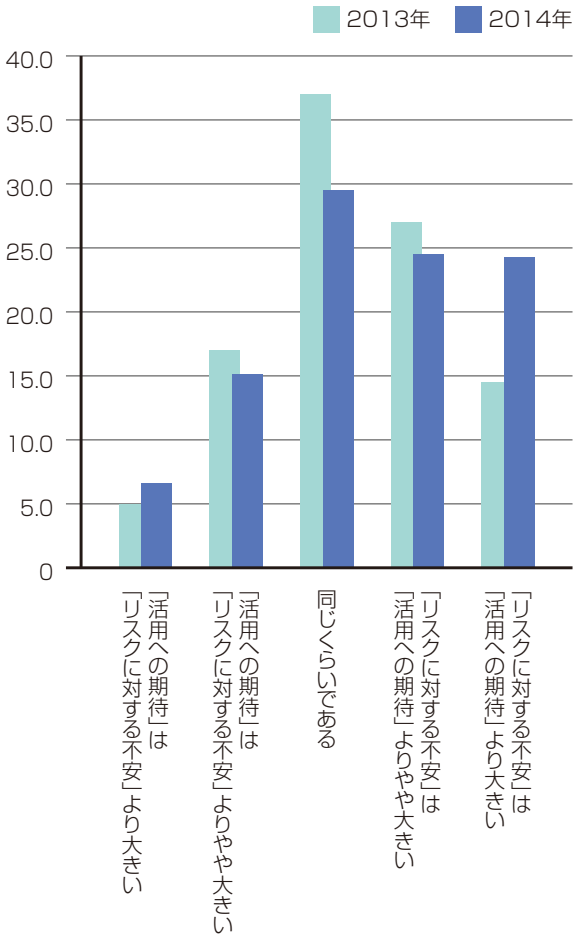
ビッグデータとは、「大量（Volume）、多様（Variety）、高速（Velocity）」という、いわゆる3Vの特性をもつデータ、および、それらを処理する新技術の総称です。SNS、スマートフォン、ICカード型電子マネーなどの普及により、大量かつ多様なデータが蓄積されるようになったこと、および、クラウド化と並列分散技術の進展によりデータを高速に分析することが可能となったことから、蓄積されたビッグデータを分析し、ビジネスに利活用しようという機運が急速に高まりつつあります。

こうした期待がある一方で、ビッグデータにおけるプライバシー侵害の懸念も根強く指摘されています。実際、ビッグデータの利活用を図ろうとして、プライバシー侵害が問題化した事例も、国内外で頻発しています。例えば、取り扱っているビッグデータの中には個人情報が含まれていなかったものの、それを分析した結果、特定の個人が識別可能となり、プライバシー侵害を引き起こしてしまった事例もみられています。

日立が株式会社博報堂と2014年8月に行った「第二回ビックデータで取り扱う生活者情報に関する意識調査※1」によると、前年の調査に比べ、生活者情報の利活用について「期待と不安が同じくらい」と回答した生活者の比率は減少し、「期待が不安より大きい/やや大きい」(計21.7%)、「不安が期待より大きい/やや大きい」(計48.8%)と回答した生活者の比率が高まっており、特に不安と考える生活者の比率が増えています（図参照）。これは、ビックデータに関する情報への接触機会が増え、期待と不安の両面、特に不安面において関心が高まった可能性が考えられ、プライバシー保護に対するニーズがますます高まっているといえます。

そのため、ビッグデータビジネスにおいて、個人のプライバシーを保護し、安全･安心なビッグデータ利活用を推進するためには、ビッグデータ特有のプライバシーリスクを把握し、プライバシー保護のための適切な施策を講じていく必要があります。

※1 http://www.hitachi.co.jp/New/cnews/month/2014/08/0804.html



情報系製品・サービスへの取り組み

日立のビッグデータビジネスにおけるプライバシー保護の取り組み

ビッグデータビジネスで取り扱うデータには、個人に関連する様々な情報が含まれます。その中には、個人情報が含まれることもあり、個人情報には当たらないもののプライバシー侵害につながり得る情報が含まれることもあります。そこで、日立のビッグデータビジネスにおいては、従来の個人情報保護対策に加え、プライバシー保護のために、以下のような対策を講じています。

●プライバシー・ガバナンス

ビッグデータを取り扱う際のプライバシー保護に対するガバナンスの確立のため、プライバシー保護のための組織・体制を構築するとともに、プライバシー保護方針を定め、社員に遵守させています。また、日立のプライバシー保護の取り組みについて、お客さまに情報を公開するとともに、その継続的な改善に努めています。

●プライバシー影響評価

ビッグデータを取り扱う際のプライバシー保護のための自主的取り組みとして、プライバシー影響評価（Privacy Impact Assessment、PIA）の実施に努めています。具体的には、プライバシー侵害のおそれのあるデータを取り扱うビッグデータ案件の開始に先立って、案件の責任者がチェックリストに基づいてプライバシーリスクを評価する仕組みを導入しています。評価の際には、プライバシーに関する動向や事例、法制度等様々なノウハウを有した専門部署からアドバイスを受けることが可能です。こうした評価の結果、プライバシーを侵害するリスクが十分に低いことが確認されてから、当該案件を開始するようにしています。

●プライバシー保護教育

適切なプライバシー保護とビッグデータの利活用の両立を図るためには、社員がプライバシーについて正しく理解し、各々がプライバシー保護を心がける必要があります。日立では、プライバシー影響評価を確実に行うために、ケーススタディを活用したプライバシー保護教育を実施しています。また、ビッグデータを取り扱う部署やグループ会社を含めて、プライバシーに関する定例の勉強会、検討会を開催しています。さらに、プライバシーに関するビジネス動向、制度動向等について、日々情報共有を行うとともに、プライバシーを保護するための対策等について検討を行っています。

お客さまに安心してご利用いただけるサービスの実現をめざして

ビッグデータにおけるプライバシー保護は非常に新しい話題であり、法制度面、技術面とも、現在、検討が行われている最中にあります。日立は、お客さまに安心してご利用いただけるサービスの実現をめざし、上記のような取り組みを拡大していくとともに、ビッグデータとプライバシーを巡る国内外の法制度、技術の変化の把握に努め、今後も適時適切にサービスに反映していきたいと考えています。

情報系製品・サービスへの取り組み

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、セキュリティの関わるスキル・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活動の概要

日立グループでは社会インフラへのサイバー攻撃の激化に伴い、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共有と連携を行い、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IT技術者や社内のIT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。

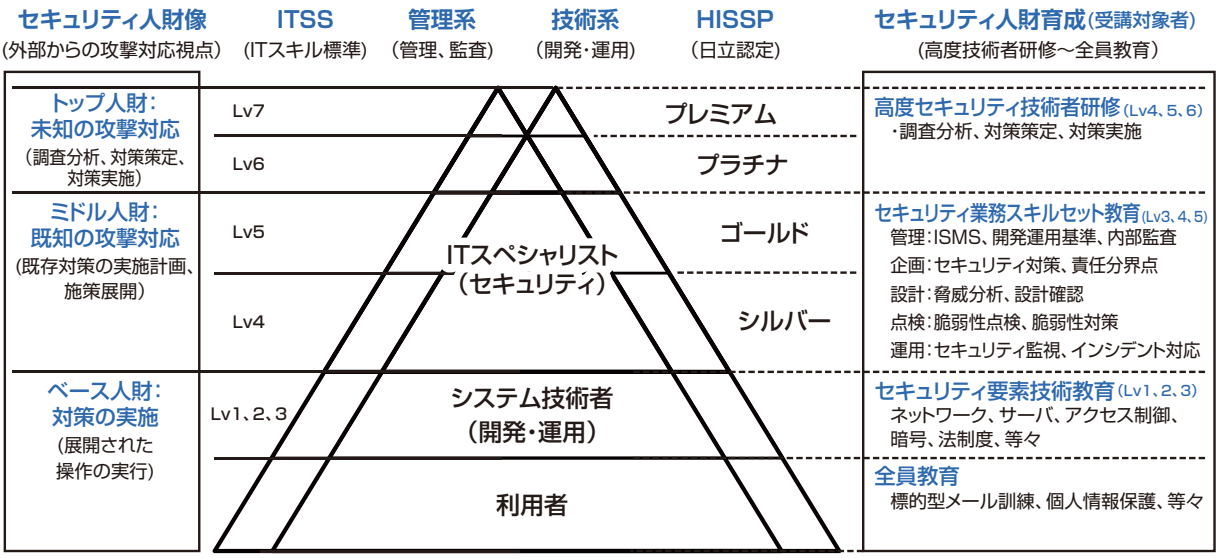
この活動では、組織的にサイバー攻撃に対応する人財像として、経済産業省が定めているIT関連能力を職種や専門分野ごとに明確化、体系化したITスキル標準（ITSS）をベースに、以下の3つのクラスに分類し、それぞれの層に必要な教育と演習を実施しています。

① 高度セキュリティ人財
未知の攻撃に対して調査分析し、対策を策定、実施できるトップ人財

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。

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） HISSP：日立認定情報セキュリティスペシャリスト（Hitachi Certified Information Security Specialist）

情報系製品・サービスへの取り組み

情報セキュリティ人財の発掘・評価

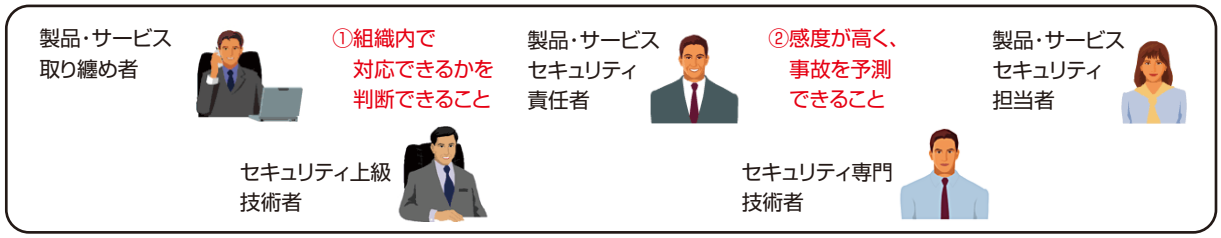
日立グループでは、2014年8月より、一般社団法人情報処理学会「認定情報技術者制度」の企業認定に準拠した日立ITプロフェッショナル認定制度（Hitachi Certified IT Professional）を創設、情報セキュリティスペシャリスト（HISSP：Hitachi Certified Information Security Specialist）として、情報セキュリティ人財の発掘と評価を開始しました。この認定では、公的資格の保有だけでなく、日立グループでの経験実績、社会への貢献（情報発信）を加味した認定基準を定め、スキルとキャリアを4段階（プレミアム、プラチナ、ゴールド、シルバー）で評価しており、2020年には1,000名の認定者をめざして認定審査を実施しています。

図２　HISSP 認定審査の観点と認定レベル >>

■審査の観点（HISSP要求事項）

✓プロとしてのIdentity(主体性)、Originality（創造性）、Productivity(生産性)を有しているかの審査

✓セキュリティの作り込みやインシデント対応で、責任感を持ち、自主的に、効率よく活動できる知識（スキル）と経験（キャリア）を有しているかの審査



■認定レベル（HISSPクラス）

【HISSPシルバー】

案件の情報セキュリティを担う情報処理技術者

【HISSPゴールド】

事業・組織の代表となる情報セキュリティ技術者

【HISSPプラチナ】

情報通信分野の代表となる情報セキュリティ技術者

【HISSPプレミアム】

日立の誇りとなる情報セキュリティ技術者

情報系製品・サービスへの取り組み

情報セキュリティ人財の育成・活用

●高度セキュリティ（トップ）人財の研鑽

高度化するサイバー攻撃に対処するため、各事業部門にIRT（インシデント・レスポンス・チーム）を設置し、高いセキュリティ技術を有する高度セキュリティ技術者を配置しています。高度セキュリティ技術者は、自らの研鑽で技術力を高めていくことが基本ですが、技術者間の情報交換の場や、実技、実践力を身につけるための場を日立インシデントレスポンスチーム（HIRT）から提供しています。

1）アドバンスドHIRTオープンミーティング
開かれた場では会話しずらいセキュリティの情報を交換する場。

2）HIRT技術継承講座
マルウェア解析・フォレンジック調査・ペネトレーション評価技術のような専門的なセキュリティ技術を継承する場。

3）HIRTオープンミーティング（ハンズオン）
新たな脆弱性を突いた攻撃への対処方法などを、サーバやネットワークの設定など、実際のマシン実習を通して、実践力をつける場。

4）HIRTオープンミーティング（外部講師編）
外部講師を招いて、セキュリティの世の中の情報を共有する場。

5）HIRTオープンミーティング（事務編）
各事業部門のIRT組織を運営するために必要な知識を得る場。

図3　高度セキュリティ（トップ）人財の研鑽 >>

情報系製品・サービスへの取り組み

●システム開発運用のセキュリティ（ミドル）人財の育成

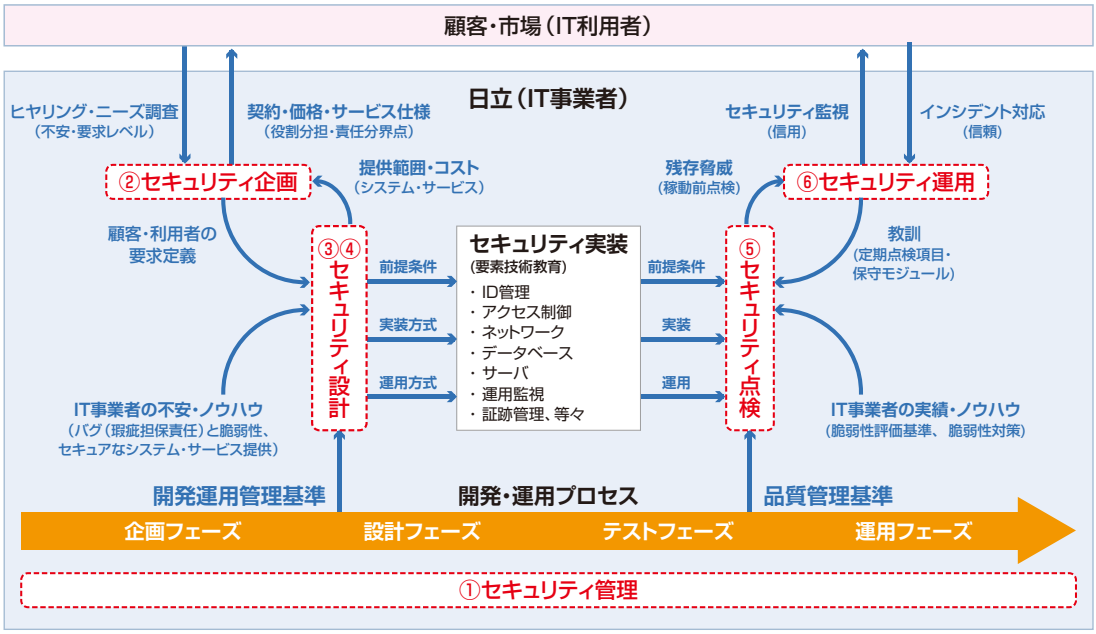
高度なセキュリティ人財の育成を進めるとともに、お客様へ製品サービスを提供するシステムエンジニアを対象として、セキュリティ品質を確保するためのセキュアシステム開発運用マネジメント基準に準拠した教育を実施しています。

この研修では、開発運用プロセスごとに、必要な規則、基準、手順、要素技術、ノウハウのスキルセット(①～⑥)を修得します。企画・設計段階でのセキュリティの作り込みや導入・運用段階でのインシデント対応を実施しています。

これにより、高度セキュリティ人財とお客様を橋渡し、サイバー攻撃に対して、セキュリティ対策や対応を実現できるミドル人財の育成を行なっています。

なお、社員全員にはIT利用者としての標的型メール訓練、個人情報保護等の全員教育、開発者にはセキュリティ実装のための要素技術教育を行っています。

図４ セキュアなシステム開発・運用のためのスキルセット教育 >>



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

日立では、①認定制度によるセキュリティ人財の発掘・評価、②高度セキュリティ技術研修とスキルセット教育によるレベルアップとともに、③セキュリティコミュニティにより、お客様に安心して製品・サービスをご利用いただくためのセキュリティ人財を育成しています。

物理系製品・サービスへの取り組み

物理セキュリティ製品・サービスのセキュリティ強化に向けた取り組み

日立では、オフィスや工場の物理セキュリティ向けの製品・サービスとして、①モニタリング映像統合管理システム、②統合型入退室管理システム、③指静脈認証ID管理、④センターからの常時遠隔監視・サポートシステムのサービス提供を行い、人・モノ・情報の流れを監視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

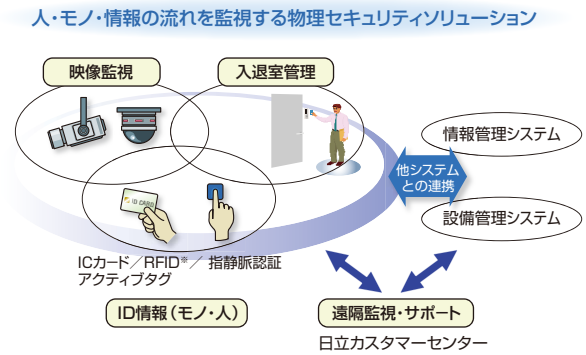
(1) 情報セキュリティと物理セキュリティ

ITの普及で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り、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も高まっています。

オフィスビルや工場の物理セキュリティ導入では、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。

(2) オフィスビルにおける物理セキュリティ要件

オフィスビル向けの物理セキュリティシステムとしては、ビルや居室への入退室管理システム、ビルに出入りする人の流れに沿って設置したカメラによる監視システムがあります。また入退室管理システムは、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。さらに認証結果を、PCや業務システムへのアクセス管理や、文書の印刷時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。また近年は、物理セキュリティ目的だけでなく、入退室管理システムと設備管理システムとを連携させて空調・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。



※ RFID: Radio Frequency IDentification

物理系製品・サービスへの取り組み

セキュリティ強化のコンセプトと製品・サービス

オフィスにおける物理セキュリティを確保するためには、カメラによる映像監視システムや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り、人・モノ・情報の流れを監視・制御する仕組みを構築することが必要です。さらに、ネットワークを活用し複数拠点のセキュリティレベルを統一し一元管理することが重要です。

このような考え方に基づき、物理セキュリティソリューションのために、下記のような特長のある製品・サービスを提供しています。

(1) 映像監視

オフィスビルの映像監視には、従来アナログカメラが多く用いられてきましたが、近年は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みつつあります。このようなネットワークカメラとアナログカメラを混用できるハイブリッドレコーダーを中心に、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モニタリング映像統合管理システムも提供しています。

(2) 入退室管理

日立の入退室管理システムは、各種非接触ICカード、指静脈認証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。また、システムをビル単位、企業グループ単位で導入した場合でも機能やデータの利用制限・閲覧制限が容易に行えます。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を許可したり、権限によっては入退室を制限するといった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、設備管理システムとの連携も可能で、セキュリティだけでなく省エネにも活用できます。

(3) 認証・ID情報管理

各種の非接触ICカードに加えて、既存のカードに貼り付けることで認証用IDを追加できるシールタグ、無線による個人認証を可能とするハンズフリー用アクティブタグ、各個人固有の指静脈のパターンデータに基づいて強固なセキュリティを保証する指静脈認証など、豊富な認証手段を提供しています。

(4) 遠隔監視・サポート体制

全国350拠点のサービスネットワークとつながっている日立カスタマーセンターが、24時間365日稼働の常時監視体制で、お客様のセキュリティ関連システムや、これと連携する設備管理システムの安定稼働、緊急時の対応をサポートします。

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、ビル・オフィス・工場などの資産を守るトータルソリューションの強化を実現しています。

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時間稼働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確実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、情報制御システムにおける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日立製作所 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

日立製作所は、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、認証取得が完了しました。その後も、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、インフラシステム社の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。

日立製作所では、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

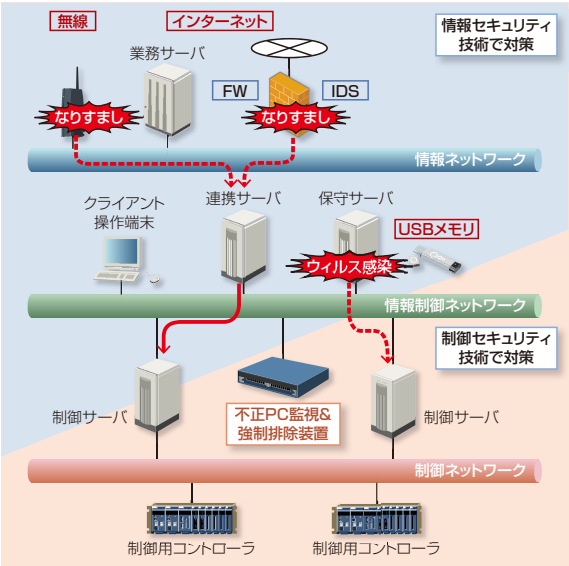
●制御系システムのセキュリティの考え方と全体像

近年、制御系システムを狙ったマルウェアであるStuxnetの登場により、国内外において、サイバー攻撃に対する制御系システムの脆弱性が顕在化してきています。これに対応するべく、欧米では、制御系システムセキュリティの国際規格の制定が加速し、国際認証取得の調達要件化が進んでいます。

一方、日本でも技術研究組合制御システムセキュリティセンターを中心に、制御装置向けのセキュリティ認証であるISASecure®EDSA（Embedded Device Security Assurance）認証スキームが開始されています。

情報制御システムは、稼働システムごとの運用に最適なシステム構成にするため、制御用コントローラ、制御サーバ、情報サーバ、データベースシステムと多種多様なシステムが混在しています。そのため、情報制御システムへのサイバー攻撃に対し、セキュリティレベルを確保・維持するに　は、FW（Firewall）、IDS（Intrusion Detection System）などの情報セキュリティ製品だけでなく、国際規格・認証に対応した制御セキュリティコンポーネントと情報制御ネットワーク用セキュリティ製品を組み合わせていく必要があります。

制御系システムへの適用例 >>



●制御セキュリティコンポーネント

ISASecure®EDSA 認証は、ISAセキュリティ適合性協会が運営する制御コンポーネントのセキュリティ保証に関する認証制度であり、セキュリティの強さを示す評価レベルごとに、必要な評価項目が定義されています。

制御用コントローラ「HISEC 04/R900E」は、これらの評価項目をクリアし、2014年にISASecure® EDSA認証を取得しました。今後も、セキュリティレベルの高い制御系製品を開発・提供していきます。

EDSA認証の評価項目と評価レベル >>

評価項目	内容	評価レベル（評価項目数）		
		LVL1	LVL2	LVL3
CRT	通信の堅牢性テスト	69	69	69
FSA	セキュリティ機能の実装評価	21	50	83
SDSA	ソフトウェア開発の各プロセスにおけるセキュリティ評価	129	148	169

CRT: Communication Robustness Testing　FSA: Functional Security Assessment
SDSA: Software Development Security Assessment

●情報制御ネットワーク用セキュリティ製品

制御系システムは、長期にわたって運用されることが多いため、システムの運用開始後も装置の改変により新旧装置が混在することがあります。そのため、システム全体のセキュリティレベルを維持するためには、セキュリティサポートした装置を導入するだけでなく、外部からの攻撃を侵入阻止するFWやIDSに加え、装置構成の変化を監視して不要なコンポーネントの接続を遮断することが有効です。日立グループが提供する不正PC監視&強制排除装置は、ネットワーク内を常時監視し、不審な装置を検出することができるので、情報制御システムのセキュリティ確保に効果が期待できます。

●システム運用面でのセキュリティ確保

情報制御システムにおいても、パスワード管理や入退室管理など運用面でのセキュリティ対策が重要です。これらは、基本的には運用者が主体で行うものですが、システムベンダーとして、お客様の課題に最適なソリューションを提案していきます。

製品・サービスのセキュリティを支える研究開発

安心・安全・快適な社会を実現するセキュリティ研究開発

ICT技術を用いた社会インフラシステムの高度化を実現するには、変化し続けるリスクに対処可能なセキュリティ技術が求められています。信頼性・安全性と利便性を両立した製品・サービスを世の中に提供し、人々が安心して生活できる社会を実現するために最先端のセキュリティ技術の研究開発に取り組んでいます。

セキュリティ研究開発の取り組み

ICT技術の普及・進展と利用拡大に伴い、セキュリティはより一般的な技術として様々な事業領域で適用が進んでいます。日立では、社会インフラシステムや企業情報システムを構築するうえでセキュリティ技術は必要不可欠であると認識し、1980年代より「暗号」「認証」「評価」を3つの柱として、事前のセキュリティ設計によってシステムを守るアプローチの研究開発に取り組んできました。

しかし、近年セキュリティ設計だけではカバーしきれない様々な課題が顕在化してきています。例えば、標的型攻撃に代表されるサイバー攻撃の高度化、日々新たに発見されるソフトウェアコンポーネントの脆弱性、インターネットバンキングにおけるなりすまし被害の急激な増加、ビッグデータ分析を活用する際の情報の秘匿やプライバシ保護の問題、IoTにおけるフィールドデバイスの保護などです。このような新たな課題に対しては、従来の技術に加え、攻撃を受けた後の対処を迅速かつ的確に行う事後対処や、データの秘匿と分析の両立、といった新たなアプローチが必要とされます。

安心・快適に生活できる、安全な社会を実現するのは、社会インフラ事業をリードする日立の責務であると認識し、日々高度化するさまざまな脅威に対抗すべく、世界最先端のセキュリティ技術の研究開発に取り組んでいます。

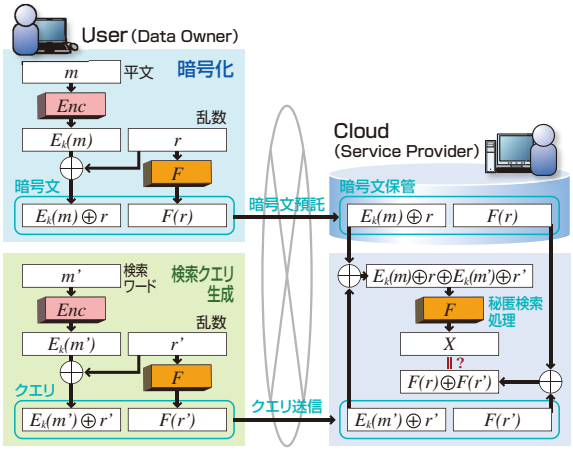
秘匿情報処理技術の開発

近年、クラウドを活用したサービスが大きな注目を集めていますが、クラウドにおけるセキュリティに対するユーザの不安が大きく、機密性の高いデータを扱う業務をクラウドに預託する妨げとなっています。たとえ、クラウドにデータを暗号化した状態で預託したとしても、クラウド上でデータの検索・照合を行う場合には、暗号化したデータをいったんクラウド上で復号しなければならず、クラウド管理者も含めた第三者への情報漏えいに対するリスクが問題となってきました。

日立は、クラウド上で、暗号化したままデータの検索・照合ができる検索可能暗号技術を開発し、高い安全性を保ちながら、大容量データでも検索・照合などの処理を可能としました。従来は、同一データを複数回暗号化した場合、暗号文は全て同一となってしまうため安全性に不安がありましたが、本技術では、毎回異なる乱数を用いることにより、同一のデータであっても全く異なる暗号文になるようにランダム性を高めています。また、高速処理が可能な共通鍵暗号技術を用いることで、暗号化による処理のオーバーヘッドを最小限に抑え、大容量データも効率よく検索・照合します。

本技術は、2014年に独立行政法人 国立精神・神経医療研究センターと株式会社日立ソリューションズが共同開発した「Remudy WEB患者情報登録システム」に適用され、世界初の実用化された秘匿情報処理技術となっています。今後、医療ヘルスケア分野への本技術の活用を推進すると共に、パブリッククラウドに適用可能な汎用セキュリティソリューションとして、サービスの提供をめざします。

検索可能暗号データフロー >>



製品・サービスのセキュリティを支える研究開発

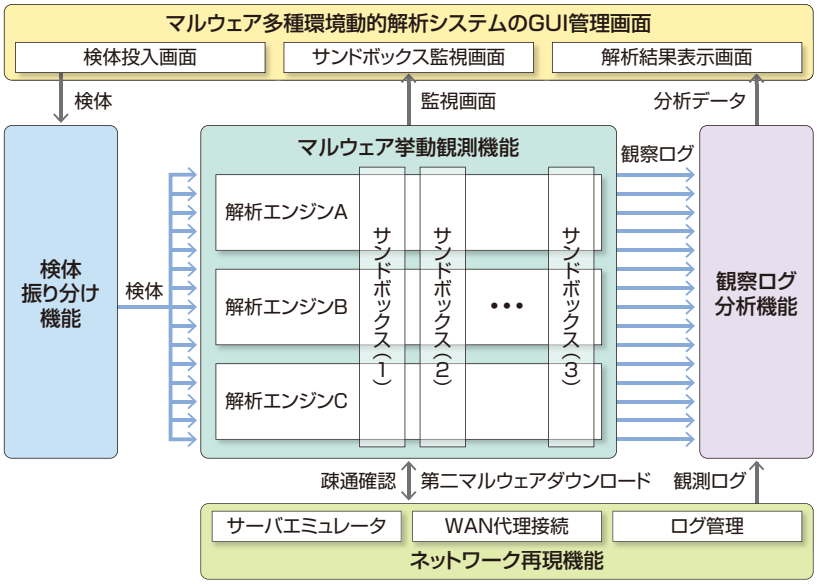
未知の標的型攻撃に備えるマルウェア動的解析技術の開発

近年、サイバー攻撃に悪用される新種のマルウェアの約半数はウイルス対策ソフトで検知できないと言われています。このため、既存の対策をすり抜け組織内にマルウェアが侵入してしまうケースが増えています。このようなマルウェアに対抗するには、マルウェアの特性を解明し、被害拡大防止策を早急に講じる必要があります。マルウェアの特性を解明する手法として、マルウェアを特殊な環境で実行して挙動を観測する動的解析手法が用いられていますが、最近のマルウェアは実行環境を限定することで解析環境での解析を逃れるタイプが増えています。

このような背景から、日立では、複数種類の動的解析環境を用いてマルウェアを多角的に解析するマルウェア動的解析技術の研究開発を行っています。また、マルウェア解析のノウハウをスクリプト化することで、観測結果からマルウェアの挙動を自動抽出する技術を開発しました。この技術により、マルウェアによるネットワーク接続などの不正行動を容易に解明することができ、マルウェア侵入後の対策に繋げられるようになります。

本技術を、組織の情報システム部門やSOC(セキュリティオペレーションセンタ)に導入することにより、マルウェア解析業務を行っている専門家の作業コストを大幅に削減できるほか、専門家不在の組織でも容易にマルウェアの脅威を明らかにすることができ、インシデント対策に役立てることができるようになります。

マルウェア動的解析技術の概要 >>



製品・サービスのセキュリティを支える研究開発

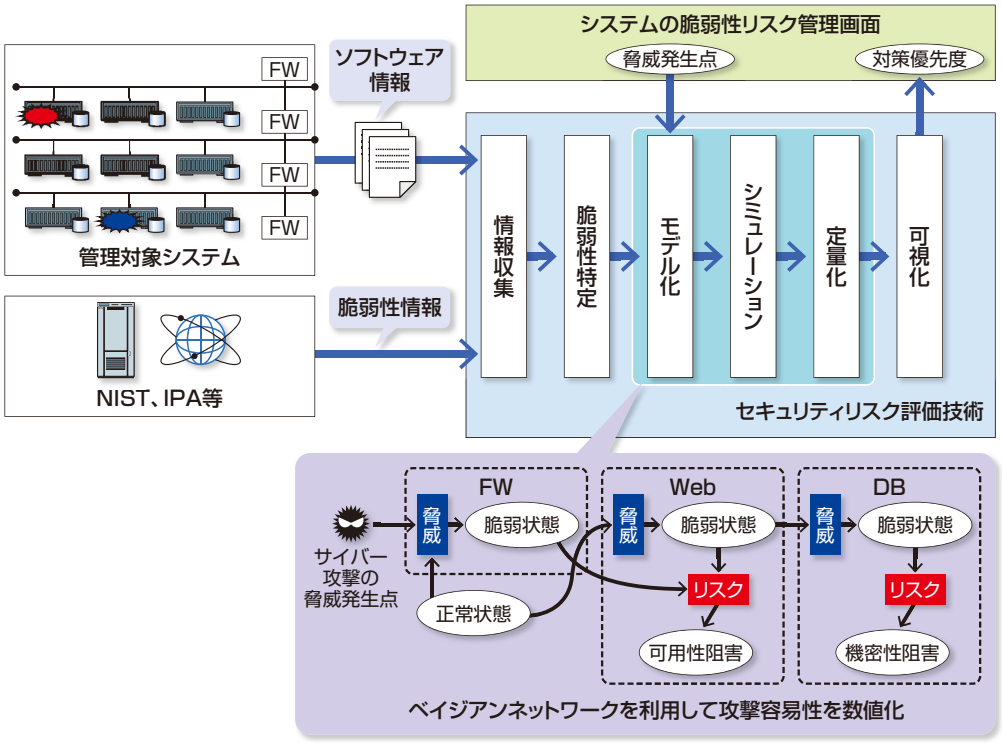
重大脆弱性の公開に迅速に対応可能なセキュリティリスク評価技術の開発

ソフトウェア等のセキュリティ上の不具合を記した脆弱性情報の公開は年々増加しており、2014年はセキュリティ情報公開機関(米国NISTなど)から約8,000件もの脆弱性情報が公開されました。その中でも高い関心を集めた「Heartbleed」というOpenSSLの脆弱性の場合、脆弱性情報の公開直後から同脆弱性を狙った攻撃が急増したため、企業等の情報システム部門は迅速な対処が求められました。このような場合、対処すべき脆弱性の特定や優先度付けが必要となり、高度な情報セキュリティスキルが求められます。しかし、個々の組織でそのような専門家の確保や育成は困難な状況でした。

そこで日立では、システムの脆弱性を迅速に特定するとともに、サイバー攻撃の侵入経路を解析して優先的に対処すべき脆弱性を順序付けする技術を開発しました。本技術では、機器から取得したソフトウェア情報と公開脆弱性情報とを突き合わせ、脆弱性の有無を自動的に特定します。また、システムに内在する各脆弱性のリスクの大きさは、脆弱性のある機器へのサイバー攻撃の到達可能性や容易性、影響度に依存します。そのため、本技術では、ネットワーク構成情報などからサイバー攻撃の到達可能性を自動解析し、各システムにおいて侵入可能な経路を網羅的に抽出します。そして、ベイジアンネットワーク技術により、各経路における侵入確率と各脆弱性の影響度を算出します。本技術により、高度な情報セキュリティスキルが必要であった脆弱性対策の優先度付けを自動で行うことが可能となり、脆弱性への一律かつ迅速な対応が期待できます。

本技術を、組織の情報システム部門やCSIRT(コンピュータセキュリティインシデント対応チーム)に導入することにより、脆弱性対策業務の作業コストを大幅に削減できるほか、専門家不在の組織でも容易に対策の優先順位を明らかにすることができ、効果的なセキュリティ運用に役立てることができるようになります。

攻撃経路を考慮したセキュリティ評価技術の概要 >>



製品・サービスのセキュリティを支える研究開発

自律進化型セキュリティ運用技術の開発

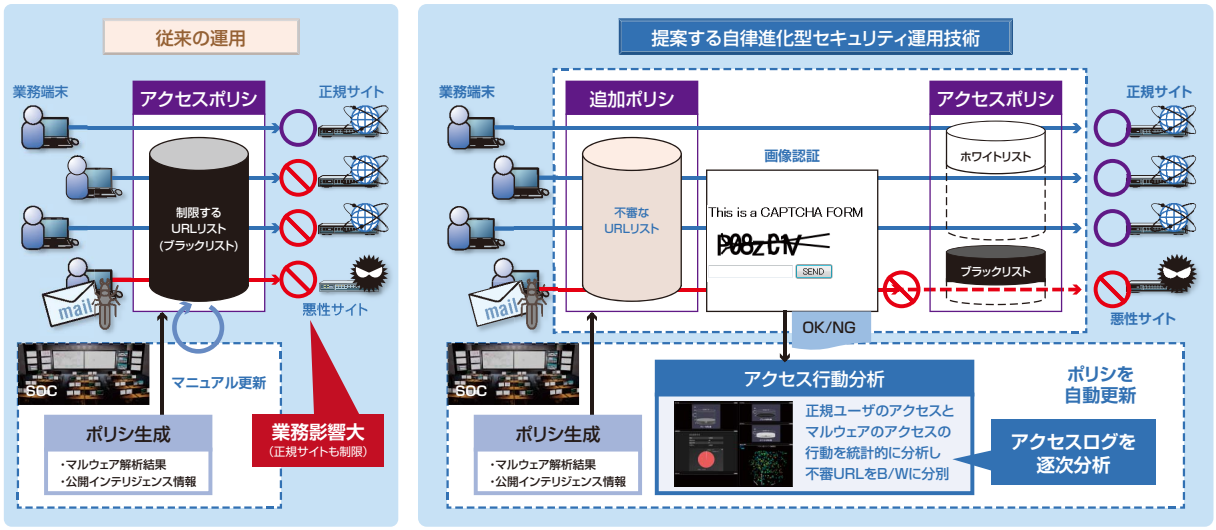
近年、サイバー攻撃の激化に伴い、24時間体制のセキュリティ運用の重要性が増してきています。セキュリティの運用には高度な専門知識を持つオペレータを必要となりますが、そのような人財が不足している状況です。そこで日立では、セキュリティ運用を効率的に行う「自律進化型セキュリティ運用技術」を開発しています。

セキュリティ運用の一つに、不正通信の検知や遮断があります。これまでは、危険と判断した通信をブラックリストに登録し、これに合致する通信を遮断する方法がとられてきました。しかし、疑わしい通信を全てブラックリストに登録してしまうと本来の業務が停止してしまう恐れがあります。そのため、不正通信といったインシデントの発生が疑われる状況では、即時に対応してリスクを抑える「リスク低減」と、業務への悪影響を最小限に抑える「業務影響低減」の両立が求められます。

このような課題を解決するのが「自律進化型セキュリティ運用技術」です。本技術では、一律に通信を止めるのではなく、一旦グレーなものとして保留します。そして、従業員あるいはマルウェアがグレーなサイトにアクセスしようとしたときに、人間によるアクセスなのかプログラムによるアクセスなのかを判断するための「チューリングテスト」を行います。そして、一定以上の従業員が上記テストに成功した場合、そのサイトを安全なサイトとみなしてグレーリストからホワイトリストに自動で振り分けます。また一定以上失敗したサイトを、マルウェアによるアクセスだとみなしてブラックリストに振り分けます。このように、従業員の認証結果を統計的に分析してアクセスポリシが自律進化する仕組みのおかげで、利用者が増えれば増えるほど精度が高まる正のネットワーク効果が期待できます。

現在、チューリングテストの一つとして知られている画像認証を用いた実装と実証実験による評価を進めています。

自律進化型セキュリティ運用技術の概要 >>



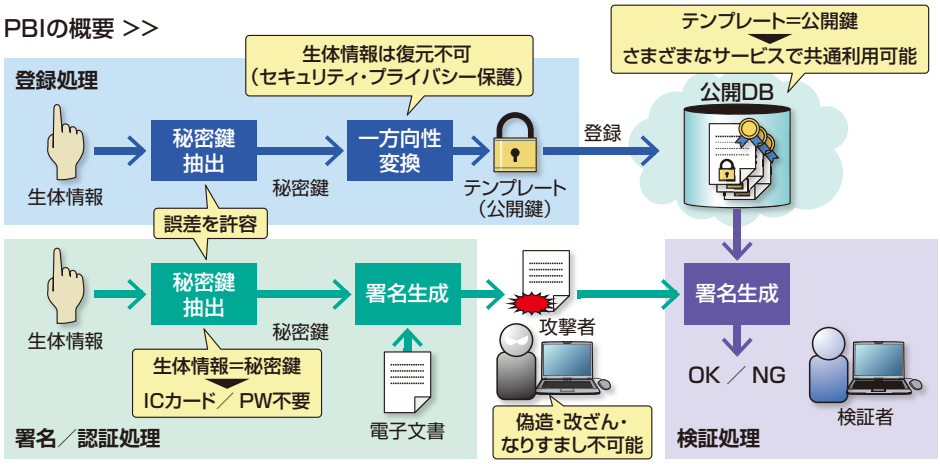
製品・サービスのセキュリティを支える研究開発

安全・安心・便利な個人認証サービスを実現するPBI技術の開発

クラウドサービスや電子決済、国民IDなどの普及拡大に伴って、不正アクセスによる情報漏えいや不正取引等の被害が急増しており、確実なユーザ認証が求められています。パスワードに代わる確実で便利な認証手段として生体認証への期待が高まっていますが、プライバシの懸念などから広範な普及に至っていません。また指紋や静脈などの生体情報は取り換えができないため、登録生体情報（テンプレート）を強固に保護・管理する必要があり、複数の異なるサービス間で共通利用することはできませんでした。

このような背景から、日立では、生体情報を決して元に戻せない形に変換したまま登録・認証を可能とすることで、プライバシを強固に保護しつつ、複数サービス間でのテンプレートの共通利用を安全に実現する、PBI (Public Biometrics Infrastructure) 技術を開発しました。この技術により、ユーザは1回生体情報を登録するだけで、様々なサービスを手ぶらかつパスワードレスで、安全・安心に利用することができます。またPBI技術により、生体情報を「秘密鍵」とする電子署名や公開鍵暗号を実現することができます。これにより、電子決済や電子行政サービスの安全性を支えている公開鍵認証基盤(PKI)を、ICカードやパスワードに頼ることなく生体情報に基づいて安全・便利に実現することができるようになります。

PBIの概要 >>



製品・サービスのセキュリティを支える研究開発

サイバーフィジカルシステムを支える軽量暗号技術の開発

近年、RFIDタグやセンサで収集された人や物の状態に関する情報(フィジカル情報)と、クラウドコンピュータ上に蓄積されるさまざまな情報(サイバー情報)を組み合わせて快適なサービスを提供するサイバーフィジカルシステムが注目されています。例えばスマートシティの分野では、RFIDタグを活用して人の位置や物の状態を把握し、日常生活に必要な電力量を調整するなど、利用者が所有するIDカードと組み合わせることで、効率的なサービスの提供が可能になります。一方、RFIDタグはカードリーダなどで容易に読み取ることができるため、そのID情報を追跡されると個人のプライバシーを侵害されるリスクがあります。

このようなリスクを軽減する技術として、ID情報の付け替えを行うID秘匿認証プロトコルの研究開発が進められていますが、タグチップ内で複雑な暗号処理を実行するため、小型化および消費電力を抑える効率的な実装方法の確立が課題でした。

日立は、電気通信大学などと共にこの課題の解決に取り組み、ID秘匿認証プロトコルを実装したRFIDタグチップの実現に取り組みました。そして、アナログ信号処理回路とデジタル信号処理回路を1つの回路に集積することで、ID情報を秘匿したまま認証を行うために必要なデジタル信号を処理する部分の回路規模の小型化と電力の効率化を図り、新電波法の特定小電力無線局に対応したUHF帯(920 MHz帯)での動作確認に成功しました。また、従来の半分の消費電力で動作する暗号実装技術を開発しました。これにより、ID値が固定である従来のRFIDタグを用いたシステムと比べて、よりプライバシー性の高いシステムの実現が期待されます。

お客様のセキュリティを実現する トータルセキュリティソリューション Secureplaza

日立のトータルセキュリティソリューションSecureplaza（セキュアプラザ）

情報セキュリティは、①ITを取り巻くさまざまな脅威への対策、②個人情報保護法やサイバーセキュリティ基本法などの法令の遵守、③国家施策や各種標準化・業界ガイドラインへの対応、の3つの側面からトータルに対応することが必要です。日立は、日々移り変わるこれらの課題の解決と継続的な組織セキュリティの実現を支援する、トータルセキュリティソリューションSecureplazaを提供します。

組織システムにおけるセキュリティ対策

システム保護、事業継続性、社会的責任、組織ブランドの維持など、さまざまな観点から組織における情報セキュリティ対策が不可欠な時代となっており、これを実現するためには次の3つの側面から取り組む必要があります。

(1)ITシステムを取り巻く脅威への対策
(2) コンプライアンスへの対応、法令遵守
(3) 各種標準化・ガイドラインへの対応

(1)においては、次々に出現するネットワーク経由の新たな脅威への対策や情報漏えい防止対策など、(2)においては、個人情報保護法やサイバーセキュリティ基本法をはじめとする法令の遵守や、マイナンバー制度への対応など、(3)においては、ISO/IEC 27000シリーズなどの国際標準やPCI DSSをはじめとする業界ガイドラインへの準拠など、広範にわたった対策が必要となっています。これらへ総合的に対応するのが、Secureplazaです。

トータルセキュリティソリューション：Secureplaza

1996年頃より、IPプロトコルやWebシステムなどのインターネット技術を組織システムインフラで活用する動きが加速し始め、さらにPC端末の高機能化とも相まって、セキュリティへの対応が非常に重要な課題となってきました。

そうした課題を解決するため、お客様のさまざまなセキュリティ要件に柔軟に対応できるトータルセキュリティソリューション体系として、1998年にSecureplazaを策定、発表しました。その後も、次々に出現する新たな脅威への対策、個人情報保護法をはじめとする法令の遵守、また、国際標準や業界ガイドラインへの準拠など、組織が直面するさまざまなセキュリティ課題の解決に向け、ソリューションを継続的に拡張しています。本ソリューションの体系は以下の特長を備えています。

① ITセキュリティから物理セキュリティまで、組織システムにおけるさまざまなセキュリティ対策を、カバーします。
②300以上のセキュリティ商品群を有し、さまざまな要件（脅威種別、セキュリティレベル、システム構成、要求仕様、業務フロー、コストなど）に柔軟に対応できる体系となっています。

Secureplazaソリューション体系 >>

ソリューションカテゴリ	脅威・課題	Secureplaza対応ソリューション
セキュリティ統制	●セキュリティ規則・ルールの不備 ●インシデント対応不備	GR ガバナンス・リスク管理 Governance and Risk Management
ID管理	●情報システムの不正利用 ●厳密な本人認証	IM ID管理 Identity Management
物理セキュリティ	●外部からの不正侵入 ●書類・物品の盗難・紛失・誤廃棄	TZ 物理セキュリティ Trusted Zone Management
データセキュリティ	●情報の破壊・改ざん ●情報漏えい	DS データセキュリティ Data Security
ネットワークセキュリティ	●サイバー攻撃 ●マルウェア感染・脆弱性を突く攻撃	NS ネットワークセキュリティ Network Security

お客様のセキュリティを実現する トータルセキュリティソリューション Secureplaza

今後のセキュリティ対策の方向性とSecureplazaでの取り組み

組織システムは、メインフレームによる集中処理の時代から、分散処理、CSS化、ネットワーク処理へと、低コスト化、利便性向上、業務効率の向上を第一義として、サーバや情報の分散配置、リッチクライアントの利用、インターネットやクラウドの活用へと発展してきました。一方で、特定の組織や企業を狙った標的型攻撃など、さまざまな新しい脅威が顕在化するとともにリスクが増大化し、コンプライアンスの課題なども浮上しています。それらに対して、さまざまなセキュリティ対策が後付けとなる形で講じられてきました。また、ビッグデータの利活用、IoT※の進展、マイナンバー制度への対応などにより新たなセキュリティの課題が顕在化しています。

現行システムをサイバー攻撃などから保護するための緊急対策は今後も重要な対応ですが、システム構築の検討フェーズでセキュリティ要件を組み込み、計画的なセキュリティ対策を中長期的に実施することが重要になっています。また、セキュリティの抜本的な改善と、運用管理の効率化、クラウドセキュリティサービスの活用を含めた、組織にとってより最適なシステムの構築を実現するための主要な要件を、Secureplazaでは以下の通り分類し、多様なニーズに対応できるソリューションをそろえています。

①組織としてのリスクマネジメント
②ユーザ認証・ID管理
③人や物（書類・物品等）の物理的管理
④情報（データ）自体のセキュリティ確保
⑤ネットワーク利用におけるセキュリティ対策

※IoT：Internet of Things
（家電や自動車などあらゆるモノがインターネットに接続されること）

①組織としてのリスクマネジメント

組織としてのセキュリティ方針なしに、セキュリティ対策はありえません。また、組織内でのインシデントを的確に把握し、これに対応できる体制も不可欠です。このようなエンタープライズリスクマネジメントを実現するためのセキュリティポリシーの策定、CSIRT※1体制の確立、SIEM※2によるSOC※3整備を支援するのが、Secureplaza/GR（Governance and Risk Management）です。

②ユーザ認証・ID管理

人事DBを源泉情報とし、各システムへのアカウントを自動配布（プロビジョニング）する統合ID管理システムや不正利用を防止する厳格な認証を実現するICカードや生体情報（指静脈など）を活用した認証ソリューションを、Secureplaza/IM（Identity Management）で提供します。

③人や物（書類・物品等）の物理的管理

セキュリティレベルに応じたゾーニングに基づく入退室管理や、物品や書類・印刷物のライフサイクルに沿ったセキュリティ管理を、Secureplaza/TZ（Trusted Zone Management）で提供します。

④情報（データ）自体のセキュリティ確保

組織の情報資産を破壊や改ざん漏えいなどから保護するとともに、安全に活用するための仕組みを提供するのがSecureplaza/DS（Data Security）です。

⑤ネットワーク利用におけるセキュリティ対策

標的型攻撃を含む組織外からの不正なアクセス・攻撃に対して、クラウドセキュリティサービスの活用を含む遮断や検知などのネットワークレイヤでの対策をSecureplaza/NS（Network Security）で提供します。

※1 CSIRT：Computer Security Incident Response Team
（セキュリティインシデント対応組織）
※2 SIEM：Security Information and Event Management
（セキュリティイベント監視）
※3 SOC：Security Operation Center
（セキュリティ監視センタ）

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

セキュリティに関する次の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

国際標準化機構（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を含むセキュリティ分野の標準化が検討されています。

●ISO TC262

国際標準化機構（ISO）のテクニカルコミッティ（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を規格化しています。

●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

国際電気標準会議（IEC）のテクニカルコミッティ（TC）であるTC65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。

FIRST（Forum of Incident Response and Security Teams）への参加

FIRSTは、信頼関係に結ばれた、世界におけるコンピュータインシデント対応チームの国際コニュニティです。現在では、70カ国350チーム以上が加盟しています。日立からもHIRT（HItachi Incident Response Team）が加盟しています。

その他活動

例えば次に示すようなさまざまなセキュリティに関する研究・検討や普及・啓発などの活動に参画しています。

- 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）
  情報セキュリティマネジメントシステム適合性評価制度 技術専門部会
  CSMS（Cyber Security Management System）技術専門部会
- Telecom-ISAC Japan
- フィッシング対策協議会
- 日本シーサート協議会
- 日本セキュリティ監査協会（JASA）
- 日本ISMSユーザグループ
- 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）

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（2016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

沖縄日立ネットワークシステムズ株式会社
株式会社 九州日立システムズ
国際電気テクノサービス株式会社
株式会社 四国日立システムズ
東京エコリサイクル株式会社
日立アイ・エヌ・エス・ソフトウェア株式会社
株式会社 日立ICTビジネスサービス
株式会社 日立アーバンサポート
株式会社 日立インスファーマ
株式会社 日立インフォメーションアカデミー
株式会社 日立インフォメーションエンジニアリング
日立SC株式会社
株式会社 日立オートサービス
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 日立技術情報サービス
日立キャピタル株式会社
日立キャピタルNBL株式会社

日立キャピタルサービス株式会社
日立キャピタル債権回収株式会社
株式会社 日立ケーイーシステムズ
日立健康保険組合
株式会社 日立公共システム
株式会社 日立国際ビジネス
株式会社 日立コンサルティング
株式会社 日立産業制御ソリューションズ
株式会社 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
日立システムズ・テクノサービス株式会社
株式会社 日立システムズネットワークス
株式会社 日立システムズパワーサービス
株式会社 日立システムズファシリティサービス
株式会社 日立情報通信エンジニアリング
株式会社 日立総合計画研究所
株式会社 日立ソフテック
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・サービス

株式会社 日立ソリューションズ西日本
株式会社 日立ソリューションズ東日本
株式会社 日立テクニカルコミュニケーションズ
日立電線ネットワークス株式会社
株式会社 日立トラベルビューロー
株式会社 日立ドキュメントソリューションズ
日立トリプルウィン株式会社
株式会社 日立ハイシステム21
株式会社 日立ハイテクソリューションズ
株式会社 日立パワーソリューションズ
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 日立物流
日立物流コラボネクスト株式会社
日立物流ソフトウェア株式会社
株式会社 日立保険サービス
株式会社 日立マネジメントパートナー
日立メディカルコンピュータ株式会社
株式会社 北海道日立システムズ

ISMS認証取得状況

日立で、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JIPDECから取得した会社、および組織をもつ会社は、以下のとおりです（2016年3月末日現在）。

株式会社 日立製作所（インフラシステム社）
株式会社 日立製作所（クラウドサービス事業部）
株式会社 日立製作所（ITビジネスサービス本部 e-プラットフォーム本部 データセンタ部）
株式会社 日立製作所（情報・通信システム社 公共システム事業部）
株式会社 日立製作所（情報・通信システム社　スマート情報システム統括本部ヘルスケア本部
ヘルスケアサービス第1部、ヘルスケアソリューション第1部）
株式会社 日立製作所 ディフェンスシステム社および株式会社日立アドバンストシステムズ

株式会社 アイシーエス
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）
日立SC株式会社（本社）
日立アイ・エヌ・エス・ソフトウェア株式会社
アラクサラネットワークス株式会社
日立SC株式会社（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 日立ケーイーシステムズ（東京開発センタ）
株式会社 日立公共システム（全社）
株式会社 日立国際八木ソリューションズ（ソリューション本部）

株式会社 日立システムズ（アウトソーシングセンタ事業部）
株式会社 日立システムズ（秋田・仙台センタ）
株式会社 日立システムズ（金融プラットフォーム事業部サービス本部 ATMクラウドサービス部）
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（日立ソリューションサポートセンタ 日立統合管制センタ）
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 日立システムズパワーサービス（ITサービス事業部）
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西日本（クラウドビジネス推進センタ）
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）
日立電線ネットワークス株式会社
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 日立パワーソリューションズ
株式会社 日立ファルマエヴォリューションズ
株式会社 日立物流
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セキュリティ評価及び認証制度」によって認証された主な製品は、次のとおりです（2016年3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	認証取得レベル※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
Enterprise Certificate Server Set 01-01-A	認証局機能	C0013	EAL3
JP1/Base 認証サーバ 08-10（Windows版）	システム運用管理	C0114	EAL2+ALC_FLR.1
uCosminexus Application Server 08-00	アプリケーションサーバ	C0234	EAL2+ALC_FLR.1
EUR Form Client　05-07	帳票データ作成支援ソフトウェア	C0068	EAL2+ALC_FLR.1
Hitachi Command Suite Common Component 7.0.1-00	基盤モジュールソフトウェア	C0303	EAL2+ALC_FLR.1
Hitachi Storage Command Suite Common Component 6.0.0-01	基盤モジュールソフトウェア	C0199	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
Hitachi Unified Storage 150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	C0419	EAL2
Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500用制御プログラム 70-02-05-00/00（R7-02-06A）	ストレージ装置制御ソフトウェア	C0315	EAL2
Hitachi Adaptable Modular Storage用マイクロプログラム 0862/A Hitachi Adaptable Modular Storage 2300 用マイクロプログラム 0862/ A-M	ディスクアレイ装置制御ソフトウェア	C0220	EAL2
Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform H24000, Hitachi Universal Storage Platform VM, Hitachi Universal Storage Platform H20000用 制御プログラム 60-02-32-00/00（R6-02A-14）	ストレージ装置制御ソフトウェア	C0200	EAL2
SANRISE Universal Storage Platform用CHA/DKAプログラム（日本国内） TagmaStore Universal Storage Platform CHA/DKA Program（海外） SANRISE Network Storage Controller用CHA/DKAプログラム（日本国内） TagmaStore Network Storage Controller CHA/DKA Program（海外） SANRISE H12000用CHA/DKAプログラム（日本国内） SANRISE H10000用CHA/DKAプログラム（日本国内） 50-04-34-00/00	ストレージ装置制御ソフトウェア	C0102	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
アプリポーター Security Kit バージョン 01-00	電子申請基盤ソフトウェア	C0025	EAL2
DocumentBroker Server Version 3 03-11	文書管理	C0158	EAL1+ASE_OBJ.2、 ASE_REQ.2、ASE_SPD.1
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

※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の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、利用者からの報告受付けと利用者への通知手続きが求められます。

第三者評価・認証

暗号モジュール試験・認証の取得状況

（独）情報処理推進機構（IPA）が運用するISO/IEC 19790に基づく「暗号モジュール試験及び認証制度（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製品は、次のとおりです（2016年3月末現在）。

製　品	認証番号	認証取得レベル
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	J0015【CMVP#1696】	レベル1（注1）
HIBUN Cryptographic Module for Kernel-Mode 1.0 Rev.2	J0016【CMVP#1697】	レベル1（注1）
HIBUN Cryptographic Module for Pre-boot 1.0 Rev.2	J0017【CMVP#1698】	レベル1（注1）
Keymate/Crypto JCMVP ライブラリ04-00（Solaris版、Windows版）	J0007	レベル1
Keymate/Crypto JCMVP ライブラリ04-00	J0005	レベル1

注1. この暗号モジュールは、JCMVPとCMVPの認証を同時に取得（共同認証）しています。
JCMVPが適用するISO/IEC 19790は、CMVPが適用する米国連邦情報処理標準FIPS140-2をベースとしており、規格の内容は等価です。

制御機器向けセキュリティ認証の取得状況

技術研究組合制御システムセキュリティセンタ（CSSC）が運用する国際的な制御機器向けセキュリティ認証制度であるISCI※1の「ISASecure® EDSA 認証」※2によって認証された製品は、次の通りです。（2016年3月末日現在）。

製　品	認証番号	認証取得レベル
制御用コントローラ　HISEC 04/R900E	CSSC-C00002	EDSA 2010.1 Level 1

※1.ISCI（ISA Security Compliance Institute）：ISAセキュリティ適合性協会
※2.EDSA（Embedded Device Security Assurance）：制御機器のセキュリティ認証制度

日立グループの概要

会社概要 (2016年3月末日現在)

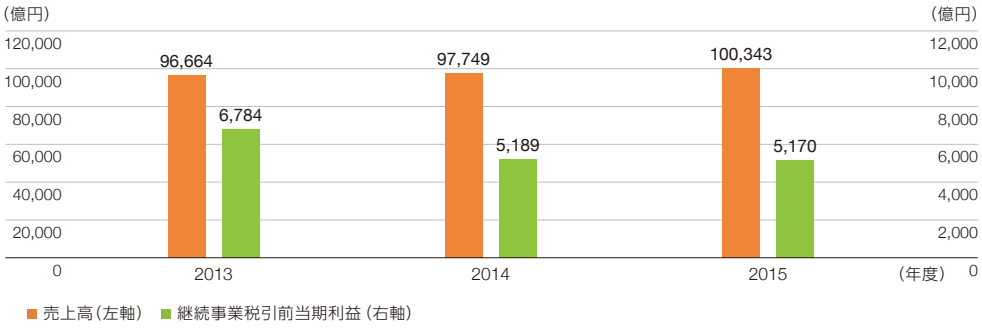
商号	株式会社 日立製作所 Hitachi, Ltd.
設立年月日	大正9年(1920年)2月1日 (創業 明治43年(1910年))
本店の所在地	東京都千代田区丸の内一丁目6番6号
代表者	代表執行役 執行役社長兼CEO 東原 敏昭
資本金	458,790百万円
従業員数	(個別)37,353人 (連結)335,244人
連結子会社数	1,056社(国内262社、海外794社)
持分法適用関連会社数	249社

財務ハイライト (2016年3月期 連結 IFRS)

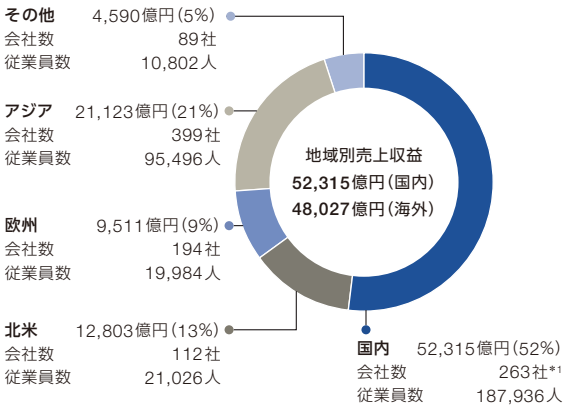
売上収益	100,343 億円 (前期比103%)
EBIT※1	5,310 億円 (前期比99%)
継続事業税引前当期利益	5,170 億円 (前期比100%)
設備投資額※2	5,285 億円 (前期比123%)
研究開発費	3,337 億円 (前期比100%)
総資産額	125,510 億円
売上収益に占める海外生産高比率	26%

※ 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

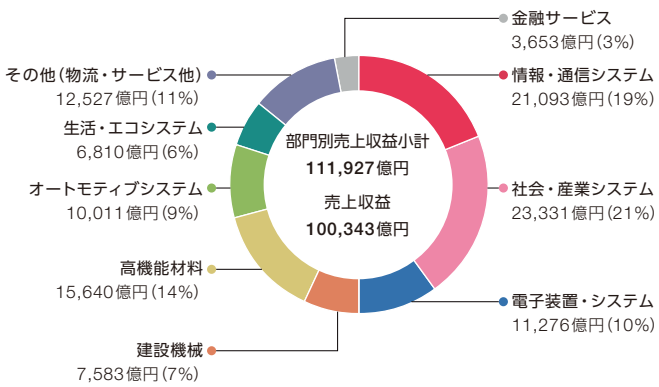
●売上収益／継続事業税引前当期利益の推移



●地域別売上収益／売上収益比率
(2016年3月期 連結 IFRS)



●事業部門別売上収益／構成比
(2016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262社、計263社

* 2015年4月1日より、「電力システム」を「社会・産業システム」へ統合しています。
*「その他(物流・サービス他)」に含まれる(株)日立物流は、2016年5月19日付けで(株)日立製作所の持分法適用関連会社となりました。
*「金融サービス」を構成する日立キャピタル(株)は、2016年10月以降、関連規制および許認可などへの対応が完了次第、(株)日立製作所の持分法適用関連会社となる予定です。

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