HITACHI
Inspire the Next

情報セキュリティ報告書
Information Security Report

日立グループ

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：2010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：2011年6月発行

東日本大震災は未曾有の災害となりましたが、被災された皆様には、心よりお見舞いを申し上げます。

日立グループの被災した拠点においては、サプライチェーンの関係で一部ご迷惑をおかけしているところもございますが、早期の生産再開にこぎつけることができました。これからも、震災によるお客様への影響を最小限に抑える努力を継続し、お客様への製品の安定供給に取り組んでいくとともに、日立グループの力を結集し、被災地の復旧・復興にできるかぎり貢献していきたいと考えています。

日立グループは、「優れた自主技術・製品の開発を通して社会に貢献する」という創業以来の企業理念のもと、ITで高度化された社会インフラを提供する、社会イノベーション事業のグローバル展開を通じ、持続可能な社会の実現に貢献していきます。

情報セキュリティに関する取り組みは、情報セキュリティ方針のもと、規則・体制の整備、技術的・管理的施策の整備および従業員教育を軸として、PDCA（継続的改善活動）を推進し、一連の活動が有効に機能しているかを検証し、内容の向上を図っています。

また、「機密情報漏えい防止3原則」を定め、従業員に徹底すると共に、お客様からお預かりしている情報の適切な管理に努めています。

〈機密情報漏えい防止3原則〉

原則1：機密情報については、原則、社外に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。

情報セキュリティにおける脅威は日々変化しており、この度の大震災や、最近頻発しているサイバー攻撃などのように、広範囲化、高度化、複雑化してきています。日立はこうした新たな脅威に対し、従来から定めていた事業継続計画（BCP）の内容やICTシステムにおけるセキュリティ対策の見直しなどを通じて、対策内容の有効性評価に努めています。この対策強化に際しては、日立グループ内に蓄積されている知識と先進技術を最大限に活用し実現するとともに、その成果は、お客様のシステムや情報資産を守る先進ソリューションとして提供し、社会に貢献して参ります。

「情報セキュリティ報告書」は、昨年、創業100周年を機に、初めて刊行しましたが、この度、2010年度までに実施してきた内容を盛り込み、改訂いたしました。

本報告書で述べている私たちの活動が、日立グループに対する信頼につながり、結果として皆様のお役に立てれば幸いです。

株式会社 日立製作所
代表執行役　執行役副社長兼日立グループCISO
中島 純三

情報セキュリティガバナンスの基本的な考え方

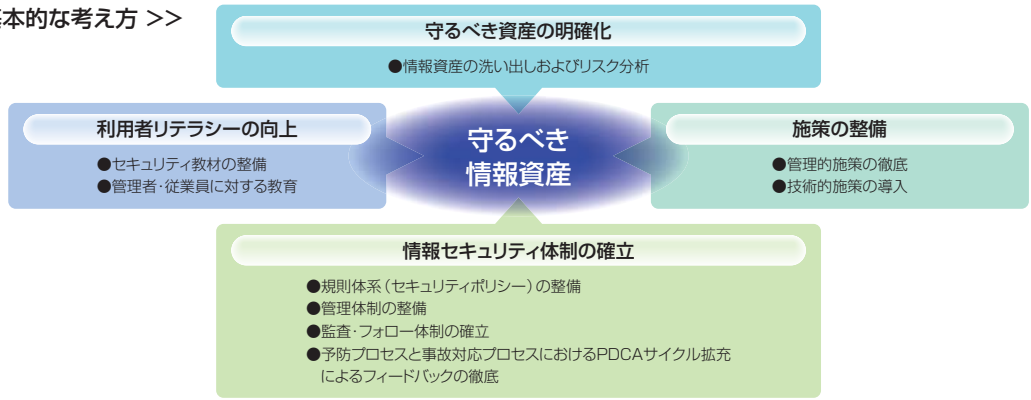
情報セキュリティガバナンスの取り組み方針

情報漏えいは、企業の信用失墜、株価への影響、ブランド価値の毀損など、企業経営の根底を揺るがしかねません。日立は、これらの経営リスクを顕在化させない「情報漏えい対策」として、情報セキュリティの取り組み方針を定めています。

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は、情報セキュリティポリシーに則り、情報資産保護の施策を下図の4つの視点から確実に講じることを基本的な考えとしています。

情報資産保護の基本的な考え方 >>



なかでも次の2点を重視しています。

（1）予防体制の整備と事故発生時の迅速な対応

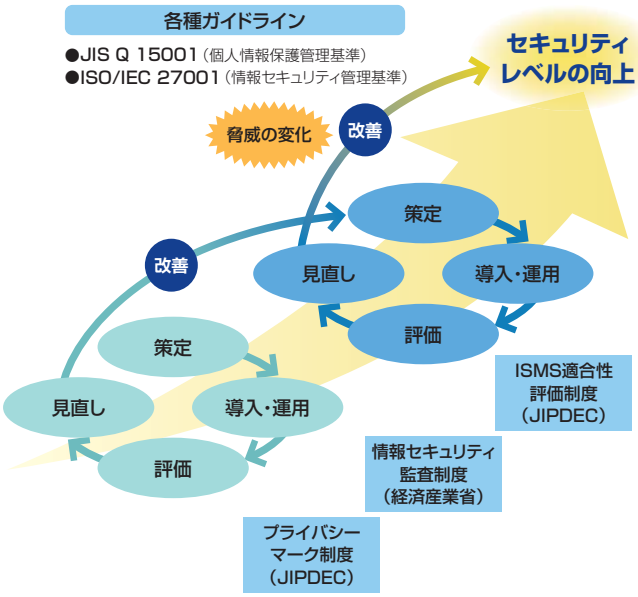
守るべき情報資産を明確にし、脆弱性評価とリスク分析に基づいて情報漏えい防止施策を実施しています。事故は「起きるかもしれない」という考え方を一歩進めて、「必ず起こるものだ」という前提に立って、緊急時のマニュアルを作成し、対応しています。

（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。

また、基本的な考え方に基づき、情報セキュリティ対策における継続的な運用、維持・改善といったPDCA（継続的改善活動）を推進し、全社を挙げてセキュリティレベルの向上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。

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、各種施策を決定します。

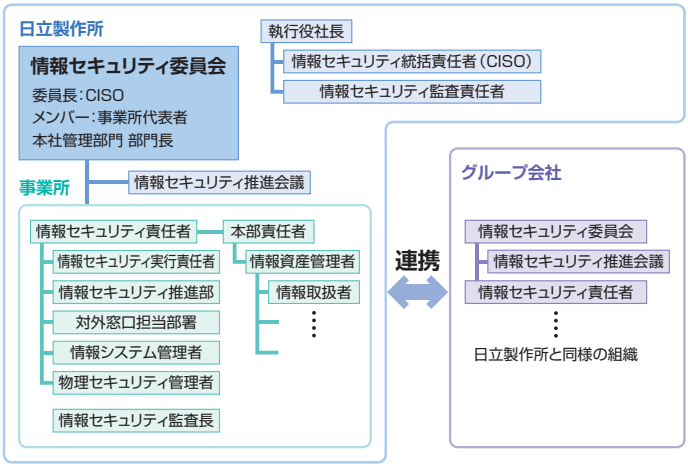
情報セキュリティ委員会の決定事項は、全事業所実務者が出席する情報セキュリティ推進会議を通じて、各事業所に徹底されます。

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、営業秘密、秘扱い文書、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 >>



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、建物への入退館に関する規定など、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。

●その他の支援

情報の取り扱いに関する社内規則を周知するために「情報の取扱及び管理ハンドブック」を全従業員に配布しています。またイントラネットにも掲載し、情報の取り扱い方法に疑問が生じた場合、すぐに参照できるようにしています。

また「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
全員教育	演習形式	実例に基づいたケーススタディを教材として、その原因、対策を考えることにより、情報の取り扱いに関する実践知識を授ける教育
管理職教育	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	宿泊研修形式	個人情報保護、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
情報資産管理者	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

情報の取扱及び管理ハンドブック >>

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

日立は年々増大する情報報漏えい、コンピューターウイルス感染、不正アクセス等の防止に取り組み、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。

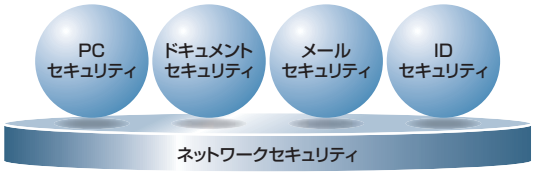
安全・安心な日立のITセキュリティ

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ITインフラ環境を構築しています。情報セキュリティと利便性は一般的にトレードオフの関係にありますが、日立では利便性を考慮しながら情報セキュリティの強化を図っています。

また国内、海外のグループ会社とも日立グループが開発した情報セキュリティ製品を積極的に導入しています。その結果を製品設計部署にフィードバックし、日立グループ製品のさらなる開発に役立てています。

日立のITセキュリティ体系

日立のITによる情報セキュリティ体系は、ネットワークセキュリティ、PCセキュリティ、ドキュメントセキュリティ、メールセキュリティ、IDセキュリティから成り、それぞれ各種IT施策を整備し、万全な情報セキュリティ対策を講じています。



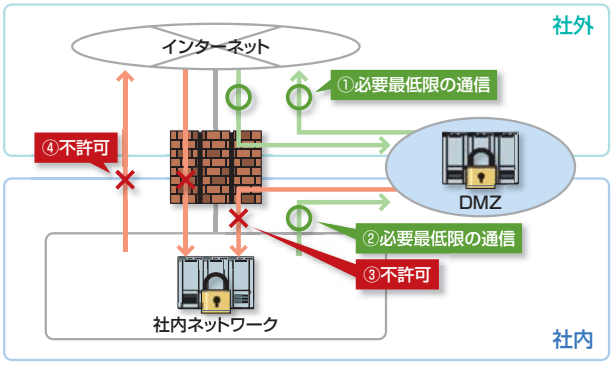
ネットワークセキュリティ

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IDS※2が不正アクセスを監視しています。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。

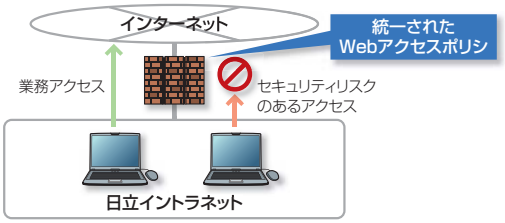
※1：DeMilitarized Zone　※2：Intrusion Detection System



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
- 統一されたポリシーによる、URLフィルタリング
- コンピュータウイルスチェック

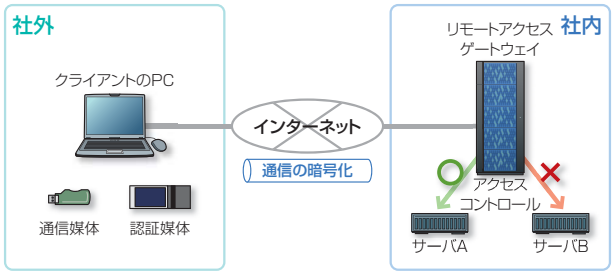


情報セキュリティに対する技術面での取り組み

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



PCセキュリティ

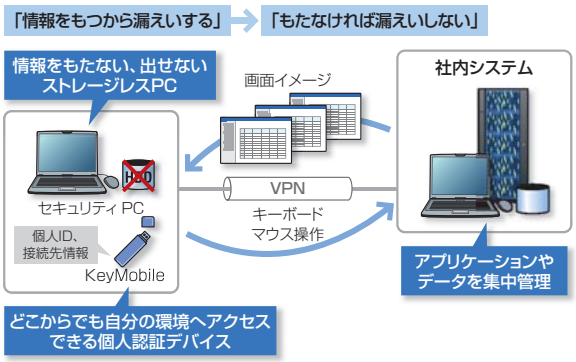
情報を取り扱う道具・器であるPCのセキュリティ対策は、社内システム環境の末端（エンドポイント）に位置づけられ、最後の砦と考えられています。

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

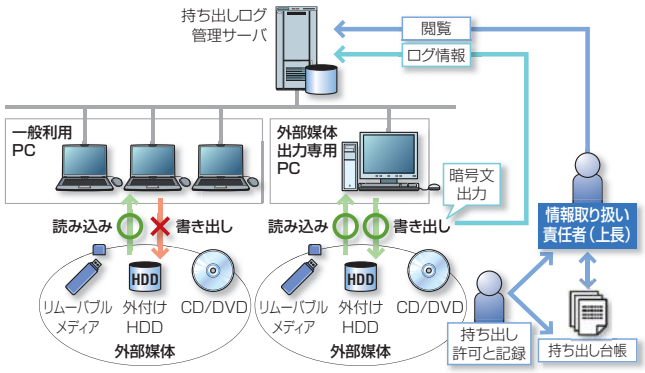
（1）については、次の2点に重点を置いて防止対策を講じています。

●モバイルPCのシンクライアント化



●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。

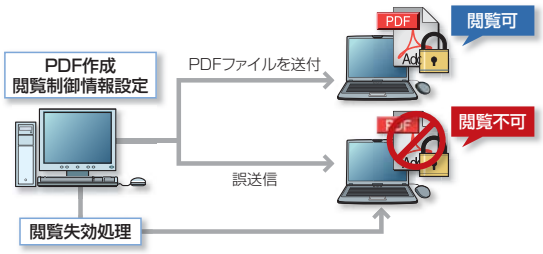
情報セキュリティに対する技術面での取り組み

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。

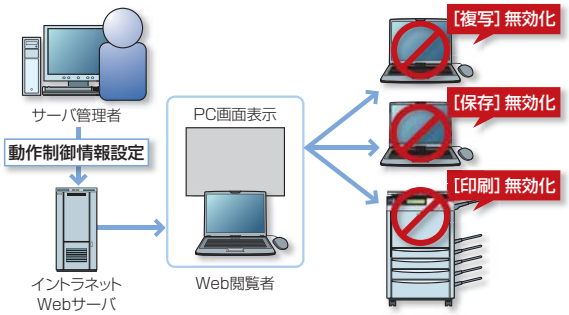
1. 電子ドキュメントの閲覧停止による情報漏えい防止

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、所持者の指示により、当該ドキュメントを失効できるようにしています。



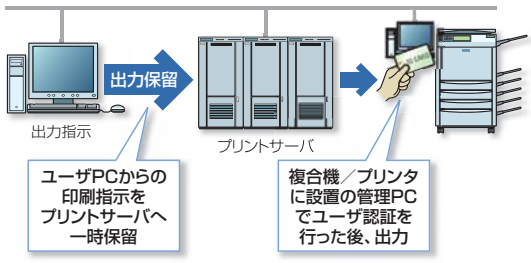
2. Webサーバコンテンツの情報漏えい防止

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。



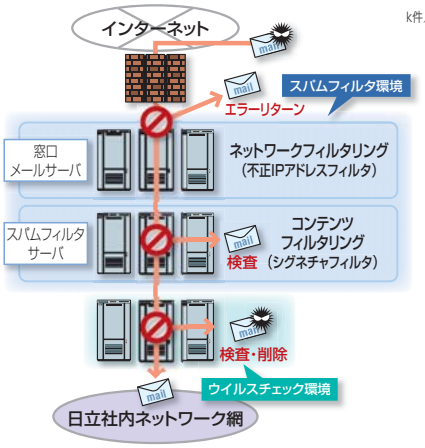
情報セキュリティに対する技術面での取り組み

メールセキュリティ

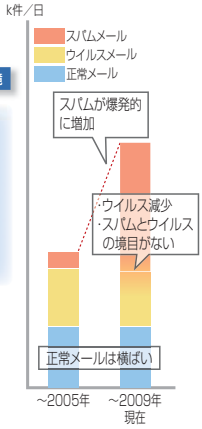
メールについては、外部からの脅威と内部で発生する脅威に備えて対策を講じています。

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〉



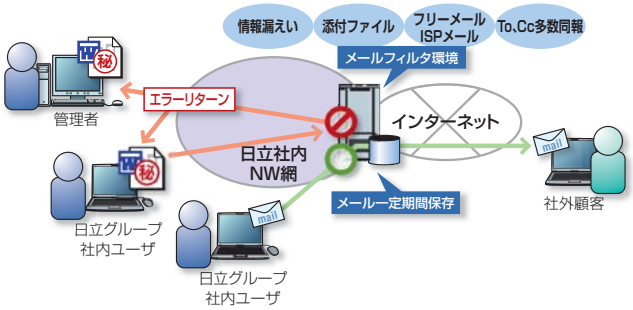
〈外部からの脅威の変遷〉



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。



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。

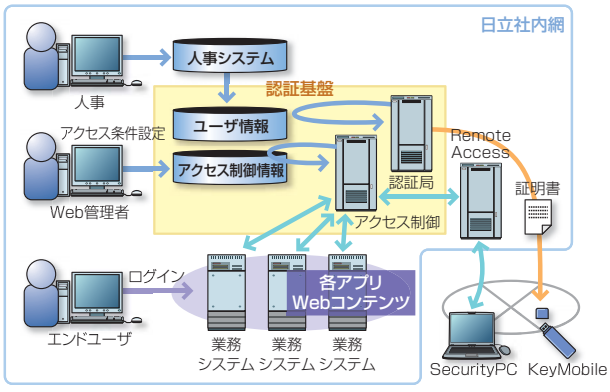
2. 個人単位での認証とアクセス制御

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。

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

③2011年度の整備完了に向け、4カ年計画を策定し推進※

※：日立製作所の推進計画、グループ会社は順次展開

物理セキュリティ整備の概要

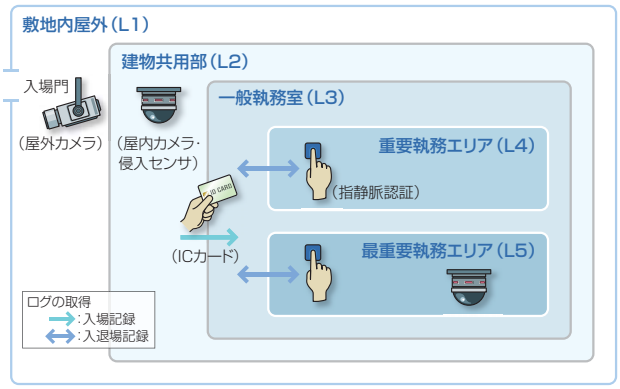
(1) 管理区域のセキュリティレベルの設定と整備の統一化

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。

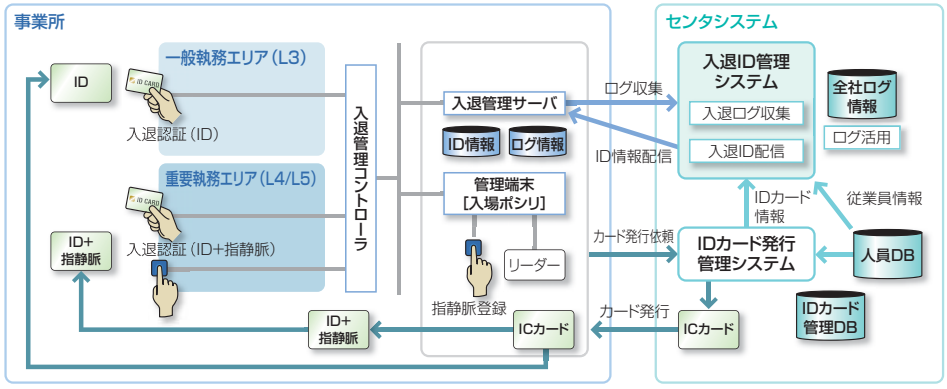
区域のセキュリティ対策レベルと対策方式 >>



(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。将来は、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

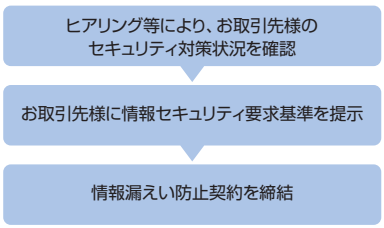
日立では、社会イノベーション事業を支える企業グループとして、お取引先様も日立と同じレベルの管理を実施していただき、情報セキュリティ事故の予防、再発防止に向けた取り組みを行っています。

(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。

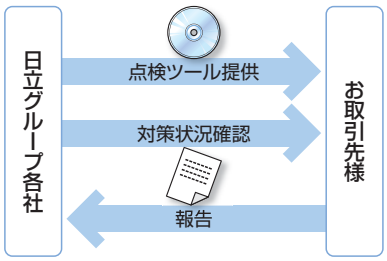
●情報漏えい防止契約書締結社数：約11，500社



(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。

情報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、日立の情報セキュリティ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

コンピュータ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、コンピュータ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、「インシデントオペレーション」を通じて、インシデントの予防と解決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：情報セキュリティに関する脆弱性を除去するための活動」と「インシデント対応：発生している侵害行為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を対象とする『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』」の視点から、日立の情報セキュリティ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。

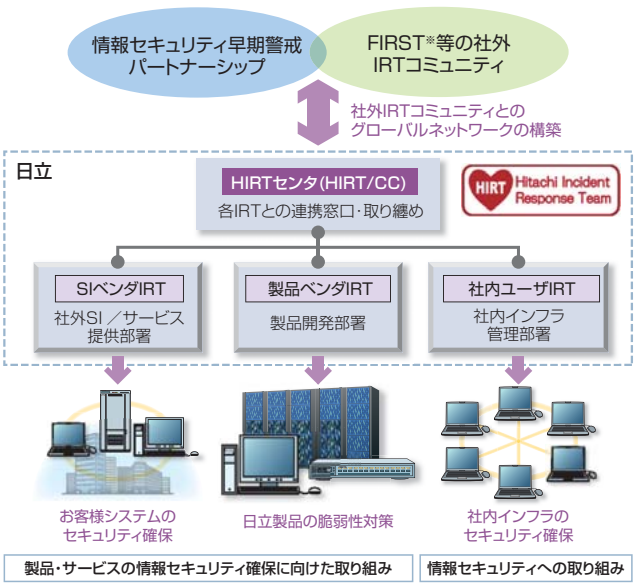
HIRTは、脆弱性対策とインシデント対応とを推進するために、下記のように、4つのIRT（Incident Response Team）という活動モデルを採用しています。4つのIRTとは、

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：Computer Emergency Response Team/Coordination Center
SI：System Integration

情報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・技術両面での情報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連携による情報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) 情報利活用基盤の整備

統合Webサイトを活用したセキュリティ情報の発信など、セキュリティ情報の収集～調査分析～展開のための情報利活用基盤を確立しています。

(3) 製品・サービスのセキュリティ技術の向上

Webアプリケーションセキュリティの強化、情報家電・組み込み系製品・制御系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（開発～検査～運用管理のための各種ガイドラインなど）を推進しています。

(4) 研究活動基盤の整備

「次の脅威のキャッチアップ」と早期の対策展開を図るための技術開発に向け、研究所との共同研究体制を整備しています。

●組織間IRT活動

組織間IRT活動では、複数のIRTが協調して、予兆や被害を隠ぺいする侵害活動などの新たな脅威に立ち向かうための組織間連携、互いのインシデント対応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）が共同で運営するJVN※2を用いた情報利活用基盤の整備、情報セキュリティ早期警戒パートナーシップに基づく脆弱性対策活動の推進、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・海外製品ベンダーIRTとの連携体制の整備、英国WARP※4活動の推進、ITU-T SG17 Q.4を通じたCVE※5、CVSS※6など脆弱性関連の標準化への対応を推進しています。

※3 FIRST：Forum of Incident Response and Security Teams
※4 WARP：Warning, Advice and Reporting Point
※5 CVE：Common Vulnerability and Exposures（共通脆弱性識別子）
※6 CVSS：Common Vulnerability Scoring System（共通脆弱性評価システム）

(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、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/

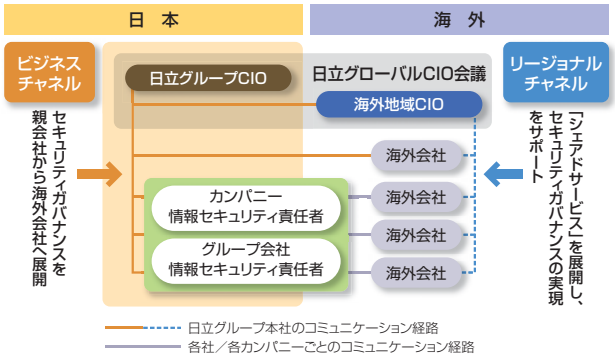
グローバル情報セキュリティの取り組み

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基準を定め、PDCAサイクルを推進し取り組んでいます。

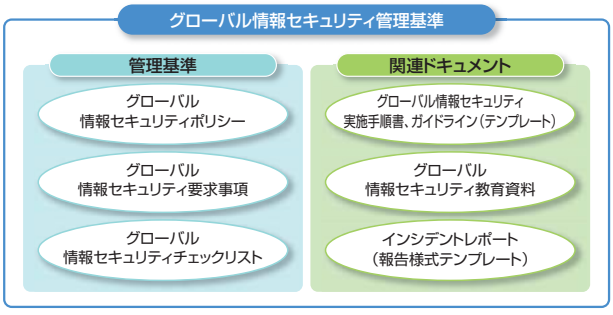
グローバル情報セキュリティ管理体制

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基準の制定

セキュリティガバナンスを推進するために、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 27001:2005）に準拠した「グローバル情報セキュリティ管理基準」を定めています。この管理基準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基準」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、「セキュリティセルフチェック」および「セキュリティ施策実施状況調査」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：日本情報経済社会推進協会）を取得し、2011年3月に2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 >>

日立製作所　個人情報保護方針 >>

http://www.hitachi.co.jp/utility/privacy/index.html

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。

〈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

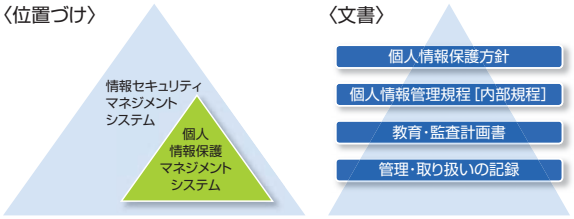
個人情報保護に対する取り組み

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の基本要素を書面として記述した「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。

個人情報保護／情報セキュリティカード >>

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」と「機密情報管理リーフレット」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

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）

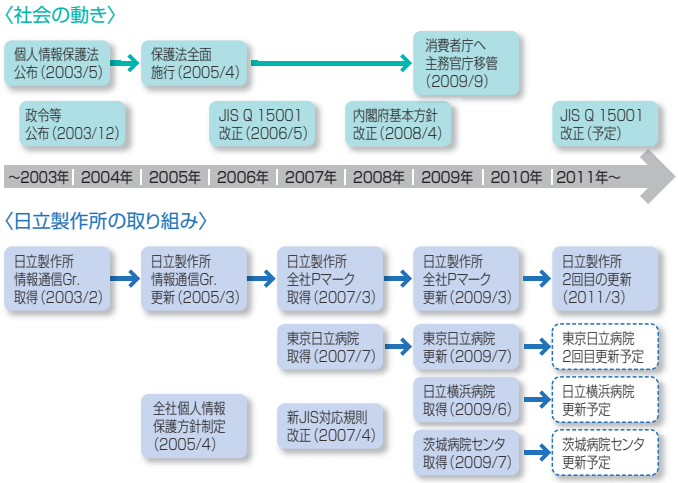
日立グループでは、グループ一体となり、個人情報保護に取り組んでいます。2011年3月31日現在、72事業者が「プライバシーマーク」を取得し、法令より管理レベルの高い個人情報の保護と取り扱いを行っています。また、プライバシーマーク取得会社を主体として、「日立グループPマーク連絡会」を組織し、定期的に情報交換会、勉強会、外部有識者を招いての講演会等を実施するほか、グループ全体として、個人情報保護に関する情報共有化および研鑽を重ねています。

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。

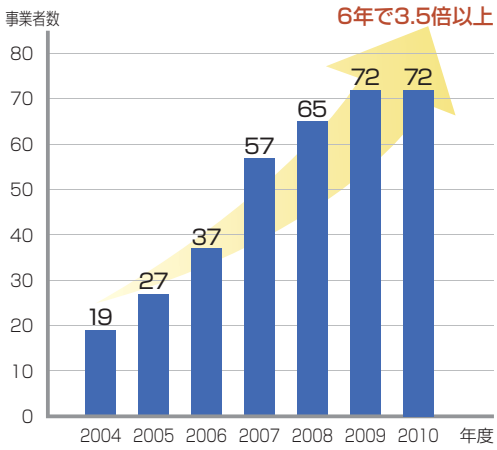
日立では、2007年7月に小平記念東京日立病院が、企業立病院として全国初のプライバシーマークを取得しました。2009年6月には、日立横浜病院、同年7月には茨城病院センタが新規に取得しており、患者をはじめとする個人情報の保護に努めています。

各医療施設とも、2011年に認定更新を予定しています。

日立製作所プライバシーマークへの取り組み >>



日立グループのプライバシーマーク取得事業者数推移 >>



※ 数値は、各年度の3月31日現在の調査数値

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 情報・通信システム社では、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を推進しています。その中心となるのが、製品・サービスセキュリティ委員会です。委員会は、日立製作所本社、情報・通信システム社以外の各システム社／本部／グループ会社とも連携して推進しています。

製品・サービスセキュリティ委員会の活動

●委員会の特徴

安全で信頼できるユビキタス情報社会の実現は、情報システム基盤を支える製品やサービスを提供する情報・通信システム社の使命です。情報・通信システム社が提供する製品・サービスは、情報セキュリティが確保され、これを利用するお客様およびユビキタス情報社会の安全に寄与するものでなければなりません。

製品・サービスセキュリティ委員会は、次の役割を担って活動しています。

(1) セキュリティマネジメントシステムの確立

セキュアな製品・サービスの提供およびセキュリティインシデントへの迅速な対応のために、セキュリティマネジメントシステムを確立し、維持・改善します。

(2) セキュアな製品・サービスの提供

製品・サービスの一連の開発プロセスにおいて、そのセキュリティ要件を設計・実装し、セキュアな製品・サービスを提供します。

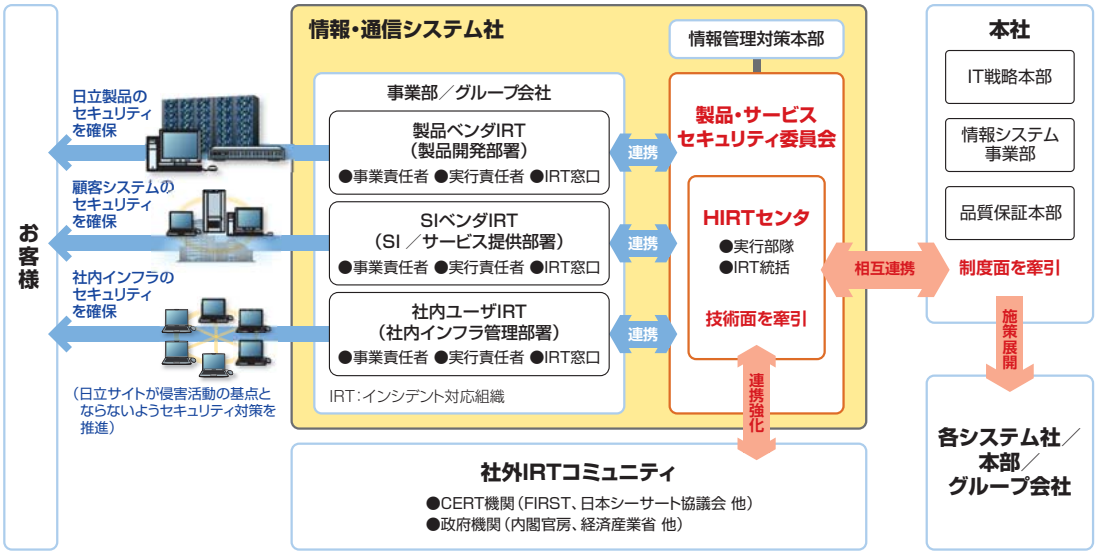
(3) セキュリティインシデントへの迅速な対応

社内外のセキュリティインシデント情報をモニターし、提供する製品・サービスにかかわるセキュリティ脆弱性について速やかに対策を講じます。インシデント情報は利用者に開示して、セキュリティ事故の予防に努めます。

●推進内容

(1) 製品・サービスのセキュリティ確保（脆弱性排除、問題点対応等）の基本方針の策定
(2) 製品・サービスのセキュリティ確保のための体制の確立・技術開発・教育実施
(3) セキュリティを考慮したシステム構築・維持運用が可能な製品・サービス開発方法の検討・実施

●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・通信システム社グループ会社においても、製品・サービスセキュリティ委員会と連携して、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。

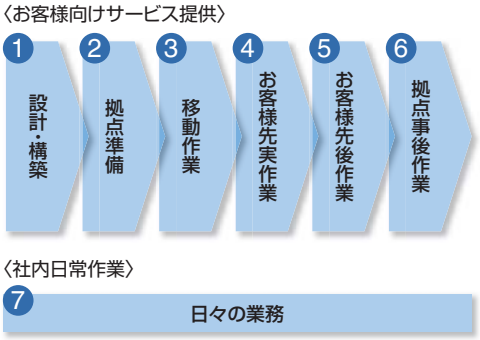
(3) 技術者向けセキュリティ教育

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 >>



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、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

日立の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ソフトウェア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ける、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、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 セキュリティを考慮した製品設計
② セキュアな実装（セキュアプログラミング）
③ 運用開始後に発見された脆弱性問題への迅速な対応と情報提供
④ 第三者評価・認証の活用

これらの取り組みを「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、世界水準のセキュリティの確保に努めています。

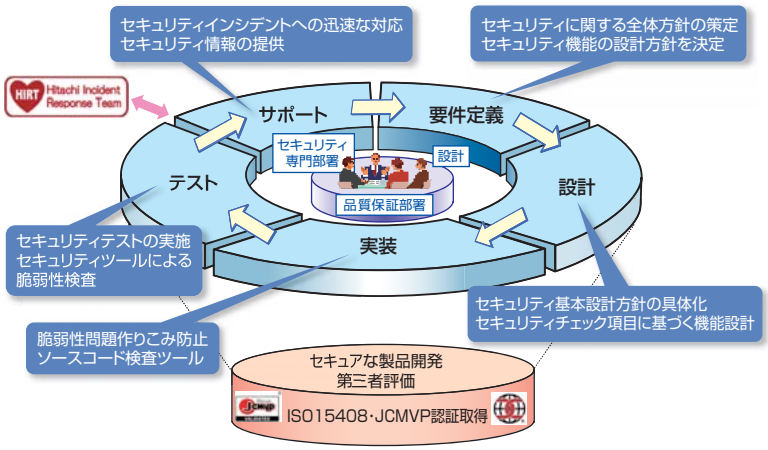
「製品セキュリティライフサイクル」の確立

製品の要件定義から始まって、設計、実装、テスト、サポートといった従来の開発プロセスの各フェーズにおいてセキュリティ確保のための施策を取り入れており、セキュリティを考慮した設計、ツールを活用したセキュアな実装とテスト、脆弱性問題への対応を行っています。また、設計者に対してセキュアプログラミング教育を実施し、脆弱性問題の発生を防止するために、情報の共有、検査担当者へのトレーニングなどにも力を入れています。これらを確実に実行していくことで、セキュリティを確保した製品開発に取り組んでいます。

製品セキュリティ・ライフサイクルの取り組み内容 >>

フェーズ	実施内容
要件定義	製品のセキュリティに関する全体方針、セキュリティ機能の設計方針を決定。
設計	セキュリティチェック項目に基づく機能設計を実施。セキュリティ機能設計方針を具体化。
実装	ソースコードレベルでの脆弱性問題作り込みを防止。セキュアプログラミングの実施。ソースコード検査ツールによる検証。
テスト	セキュリティツール（脆弱性検出ツール）による脆弱性検査。セキュリティチェック項目に基づいたテストの実施。
サポート	セキュリティインシデントへの迅速な対応。対策版の作成／提供。セキュリティ情報の提供。HIRTと連携して最新の脆弱性問題を追求。

製品セキュリティライフサイクル図 >>



情報系製品・サービスへの取り組み

ソフトウェアの脆弱性問題への対応と情報公開

ソフトウェア製品の脆弱性問題についても、「製品セキュリティライフサイクル」の取り組みの一環として対応しており、問題が発見された場合は迅速に対応するとともに、お客様への情報公開を積極的に進めています。

ソフトウェアの脆弱性問題は、設計フェーズ、実装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もあるので、運用フェーズでの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、経済産業省告示第235号「ソフトウエア等脆弱性関連情報取扱基準」にも対応しており、脆弱性発見の連絡から、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

第三者評価・認証制度の活用

セキュリティを確保する取り組みを客観的に示す指標、ISO/IEC 15408（国際セキュリティ評価基準）やJCMVP（暗号モジュール試験および認証制度）による第三者評価・認証にも積極的に対応しています。

これらは、主に「政府機関の情報セキュリティ対策のための統一基準」等でも活用されていますが、お客様のニーズに合わせてこれらの認証を活用すれば、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、ISO規格で規程されているセキュリティ保証要件は、認証を取得する製品だけではなく、製品共通の開発プロセスとして確立すれば、他の製品においても同等水準のセキュリティを確保することができます。

日立のオープンミドルウェア製品は、ISO/IEC 15408で規定されているセキュリティ欠陥への対応プロセスの評価についても国内ではいち早く対応しています。また、ISO規格で規定されるEAL（評価保証レベル）に対して、「ALC_FLR.1（基本的な欠陥修正）」の保証を追加した認証を取得しており、ソフトウェアの脆弱性への対応プロセスについての客観性が証明されています。

ISO/IEC 15408およびJCMVPの認証については、HiRDB、JP1/Base、uCosminexus Application Server、Hitachi Command Suite、uCosminexus DocumentBroker Server、Keymate/Crypto JCMVPライブラリといった主要なオープンミドルウェア製品等で取得しています（取得製品は、P.36の表に掲載）。

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

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

日立製作所 都市開発システム社では、オフィスや工場における物理セキュリティ向けの製品・サービスとして、①ネットワーク対応の映像監視システム、②拡張性の高い入退室管理システム、③ミューチップや指静脈認証など日立独自のID情報管理、④センターからの常時遠隔監視・サポートシステムなどを提供し、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の普及で企業が取り扱う情報量が激増したことに伴って企業情報や顧客情報などのデジタル化が進み、また業務システムがネットワーク化したことで利便性が高まった半面、情報漏えいのリスクも高まっています。このリスクを低減するため情報セキュリティの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の制限、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といった物理セキュリティの必要性も高まっています。

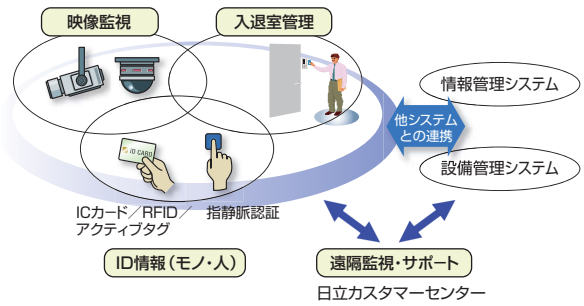
オフィスビルや工場では、各部署の役割や取り扱い情報のレベルに応じて、必要とされるセキュリティのレベルもさまざまです。物理セキュリティの導入にあたっては、守る場所、守るものを明確にしたうえで、適切なセキュリティレベルを設定し、そのレベルに応じたシステムを構築することが重要です。

(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代表的な物理セキュリティシステムとしては、フラッパーゲートによるビルへの入退場管理システム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、顔写真入りの認証カード、ICカード、さらには指静脈などの生体情報を使った認証装置といった個人認証技術と組み合わせることができます。

さらに個人認証結果を、PCや業務システムへのアクセス管理や、印刷文書のセキュリティ性を高めるプリンター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求められています。また近年は、物理セキュリティを目的とするだけでなく、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なされています。

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



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。

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、下記のような特徴のある製品・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（遠隔監視、集中監視）システムを提供しています。これによりセキュリティレベルが高く、高画質の映像を撮りたい場所にはメガピクセル対応ネットワークカメラを、通常画質でよい場所にはプログレッシブ対応アナログカメラを使い分けて導入でき、既存のシステムから容易に拡張できます。

(2) 入退室管理

日立の入退室管理システムは、コンパクトなフロアコントローラを中心に、各種非接触ICカード、RFID（超小型無線自動認識ICチップ）、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、入退室管理の情報に、PCログイン、プリンター出力、キャビネット施解錠管理を連携させることができ、オフィス内業務におけるセキュリティの向上を図ることができます。なお、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。また、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。

(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を追加できるミューチップ、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。

このような特徴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

制御系システムを開発するためにお客様の重要な情報を組み込む場合も多くあり、その情報の漏えいは直ちに社会インフラの脅威となります。内部プロセスとしての機密情報管理を厳格に行い、機密情報の漏えいを防止することが重要です。日立製作所 情報制御システム社は、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保持することにより、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、原則として物理的に他系を遮断することで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。このような動きのなかで、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情報制御システム社の取り組みを以下に述べます。

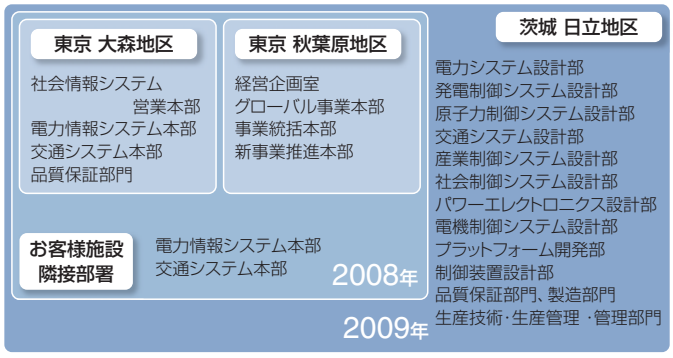
お客様の機密情報の管理

情報制御システム社は、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ます。また、お客様の情報とそれに基づいて設計する結果のお客様関連情報の機密保持が特に重要です。情報制御システム社では、この要請に応えるために、トップマネージメントの指揮のもと、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）に規定された要求事項に基づく情報セキュリティマネジメントシステムの確立、導入、運用、維持、監視、レビュー、および改善を実施しています。

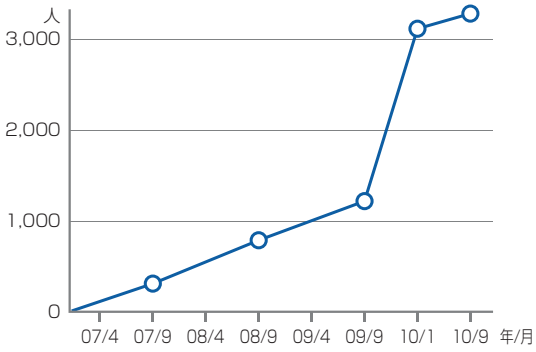
2010年1月には、全部門のISMS認証を受けました。その後、更新審査を受査し、2010年9月に全部門ISMS認証を更新しました。

情報制御システム社情報セキュリティ基盤の構築 >>

●ISMS認証取得の経過



●ISMS適用人員推移



制御系製品・システムへの取り組み

システム開発

●セキュリティを考慮した製品開発プロセスの整備

2005年に以下のプロセスを制定して以来、すべてのシステム開発に適用しています。

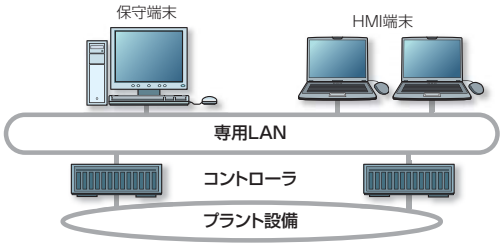
(1) 開発に着手した時点で、セキュリティリスクを洗い出します。
(2) 設計レビューで、セキュリティ設計（保護対象の設定、対策方針）を検証します。
(3) セキュリティ要件は、お客様に引き渡す前に、セキュリティ検査ツール等で全件確認します。

●セキュアなシステム開発

(1) システム設計面での取り組み

設備制御に使われるコントローラシステムの一般的な構成を下図に示します。コントローラは、設備制御の重要な部分に適用されるため、セキュリティが問題となるような運用はしないのが原則です。一般的には、物理的にオープンネットワークに接続しない構成としてセキュリティを確保し、他システムとの連携部にはファイアウォール（以下FW）を設置して、外部からの脅威に対して安全なシステム構成としています。

設備制御用コントローラシステム >>



(2) 技術面での取り組み

これまでは、制御装置専用のFWを自主開発し、これを適用することで対応してきました。製品の信頼性を確保するためには、内部の作りまで検証できるホワイトボックス製品であることが重要であるからです。今後もFWの自主開発は継続して行っていきます。

しかし、オープン化の進展により社会環境、事業環境は変化しており、それに伴って発生する情報セキュリティの脅威の多様性に対応するには、汎用製品を組み込むことも求められます。この場合には、導入時に制御の観点から徹底的に評価し、ブラックボックス度を限りなく低減しホワイトボックス化したうえで適用することにより信頼性を確保しています。さらに、HMI（Human Machine Interface）では、FWを越えて不正アクセスを試みようとしても、アクセス元の端末やログイン名などで不正操作を検出し、不正操作を行えないようにして、システムの安全性を確保しています。

コントローラは、完全にクローズした環境で動作することが原則ですが、保守端末やHMIからのアクセスも受けます。情報制御システム社では、安全に関する国際規格IEC61508に準拠する機能安全コントローラを開発し、2010年3月に認証機関TÜV Rheinland社より認証されました。機能安全コントローラは、主としてコントローラ自身の自己診断を強化することにより、非安全状態（故障を検知せずに運転継続するような状態）を極力少なくします。機能安全コントローラは、従来保守端末上で行っていたユーザ認証を、安全規格の観点から、機能安全コントローラ自身が認証する仕組みに変え、さらに暗号による強化を行い、外部からのアクセスに対する安全性を向上させています。この仕組みにより、なりすまし等による不正アクセスからコントローラを守り、プラント設備への不正出力を防止しています。制御システムのセキュリティについては、現在北米を中心に規格化が進められており、今後はこうした規格への対応も行っていきます。

(3) 人的要素、設備面での取り組み

社会インフラシステムは重要施設であり、テロ対策が求められます。施設従業員や納入・施工業者になりすまして現場に直接入り込む「侵入者」によるシステムの改ざん、消去、不正運用などの脅威が想定されます。確実に個人認証を行い、一人ずつしか入れない特殊なゲートの設置と、情報制御システムにアクセス可能な運用者の個人認証が必要です。これらの取り組みは、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最適なソリューションを提案し、情報制御システムの安全を確保していきます。

製品・サービスのセキュリティを支える研究開発

安全・安心な社会を実現するセキュリティ研究開発

ITの普及による昨今の社会環境、事業環境の変化がもたらした新たなリスクに対処するため、先進的なセキュリティ技術が求められています。信頼性・安全性の高い製品・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への取り組み

近年のITの普及・進展とビジネスへの利用拡大に伴い、セキュリティ技術はより一般的な技術へと変貌し、さまざまな事業領域でその利用が進んでいます。日立では、社会インフラ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つの柱として研究開発に取り組んできました。

1988年に開発した「MULTI2暗号」は、大型計算機用暗号装置や暗号ライブラリなど多くの日立製品に利用されるとともに、1994年にはデジタル衛星放送の国内標準暗号となり、現在もBS、CS、ケーブルテレビなどの標準暗号として、日本全国で広く利用されています。

認証技術では、画像処理技術を応用して、指静脈認証などの生体認証技術を開発するとともに、電子透かし技術の開発にも取り組み、動画配信サービスの著作権保護に利用できる「リアルタイム動画透かし技術」を世界に先駆けて製品化しました。また、2000年頃より、電子政府システムの構築が本格化し始めたことから、電子署名に必要な公開鍵暗号基盤（PKI）の研究を加速し、「電子政府向け証明書検証システム（CVS）」を実用化しました。

評価技術では、1970年代に電力分野で利用されていた「フォールトツリー分析」を情報システムに適用した独自の安全性評価手法を確立し、セキュリティ評価サービスなどで活用しています。

安全で安心して生活できる社会を実現するのは、社会インフラ企業としての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。

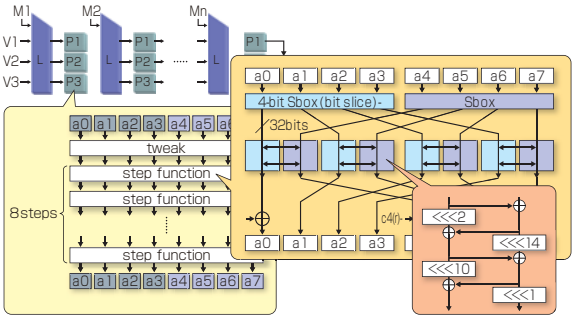
次世代標準ハッシュ関数の開発

電子政府やオンラインバンキング等のシステムでは、ネットワークを介して送受信される情報を保護したり、端末・ユーザを認証したりするうえで、暗号技術が重要な役割を果たしています。ハッシュ関数とはそのような暗号技術のひとつで、デジタル情報を圧縮して特徴値（ハッシュ値）を算出する関数です。このハッシュ値はデータの指紋とも呼ばれ、異なるデータから算出されたハッシュ値が一致する可能性は極めて低く、また、元の情報がわずかでも変わるとハッシュ値が大きく異なるといった性質をもっています。この意図的な操作が困難であるという特徴から、ハッシュ関数はデータの真正性確認手段として幅広く利用されています。

しかし2005年に、最も普及しているハッシュ関数「SHA-1」に脆弱性が発見され、期待される安全性を確保できないことが明らかになりました。「SHA-1」の急激な安全性の低下を受け、米国国立標準技術研究所NISTは、次世代の標準ハッシュ関数を選定するコンペを2007年11月に開始しました。本コンペで選定されたハッシュ関数は、事実上の世界標準としてあらゆる情報システムに利用されると予想されています。

日立は、これまでの暗号研究で培った技術・ノウハウを結集し、このコンペに2つのアルゴリズムを提案しました。そのひとつである「Luffa」は、2009年7月に51方式の応募案のなかから、日本からは唯一、他の13方式とともに第2次選考に進出することになりました。残念ながら、2010年12月に発表された最終候補5方式には選ばれませんでしたが、高速性、小規模実装が可能な軽量性などは世界中の暗号研究者から高く評価されました。今後は、国内標準化等をめざす予定です。

ハッシュ関数「Luffa」の構造 >>



製品・サービスのセキュリティを支える研究開発

情報漏えい対策への取り組み

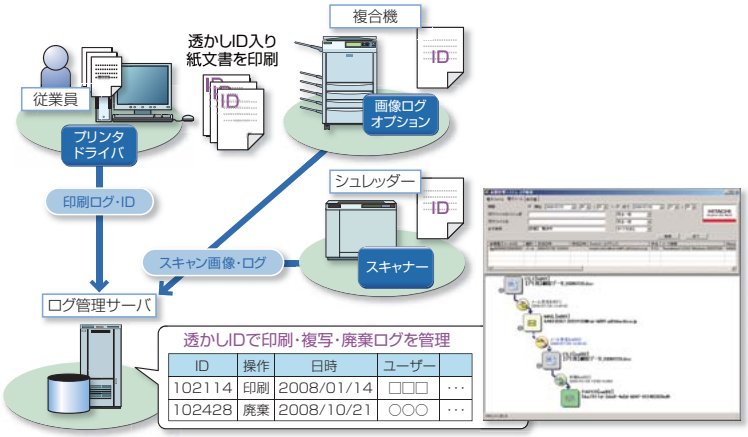
ここ数年、企業にとって情報漏えいリスクをいかに軽減するかが重要な課題となっています。情報漏えい事故を起こしたことによってブランドが棄損され、ビジネス機会が著しく減少した企業も少なくありません。暗号化やアクセス制御など、電子文書に対する情報漏えい対策は進んでいますが、紙文書に対する情報漏えい対策は遅れているのが現状です。その結果、情報漏えい事故全体に占める紙媒体経由の漏えいの割合は年々増加しており、2007年度には59.5%が紙媒体経由で、損害賠償額は1,884億円に上ったとの報告もあります。特に、一度に10万人以上の顧客情報を持ち出す事故が2008年度だけで11件（可搬媒体による持ち出しは1件のみ）あり、紙媒体といえども大量の情報漏えいの危険性を否定できない状況にあります。

このような状況に対応するため、以下のような特徴をもつ「来歴管理技術」を開発しました。

（1）情報漏えい事故が発生した場合に、漏えい元の特定等にかかる手間をできるだけ削減し、二次被害を防止するために迅速に対応できるよう、パソコンやサーバに格納されている電子文書に対する操作ログ、メールの送受信ログ、可搬媒体の読み書きログ、印刷ログ、さらには複合機の操作ログなどをそれぞれ関連づけながら一元的に管理します。これにより、メディアをまたがった迅速な追跡調査が可能となりました。特に、紙文書に関しては、日立独自の「二値透かし技術」を利用して紙一枚一枚にIDを付与し、どの紙が印刷、複写、スキャン、廃棄されたかを管理することができます。

（2）文書操作に関するログだけを選別して管理するため、他のログ収集／管理製品と比較してログの容量を抑えることができます。例えば、ファイルを新規作成しただけで、ファイルシステムのイベントログは20個近く発生しますが、これを1つの新規作成ログにまとめる、といった工夫をしています。また、検索結果がグラフィカルに表示され、電子文書や紙文書を正確かつ直感的に追跡できるようにしています。さらに、ファイル圧縮などにより、操作元ファイルが複数になる場合も、ファイルを正しくトレースすることができます。

来歴管理技術の概要 >>



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個人情報保護法や金融商品取引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。日々移り変わるこれらに継続的に対応できる組織セキュリティの実現を、Secureplazaはめざしています。

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、充分な情報セキュリティ対策が不可欠な時代となっており、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）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）は、個人情報保護法や金融商品取引法をはじめとする法令の遵守など、（3）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（セキュアプラザ）です。

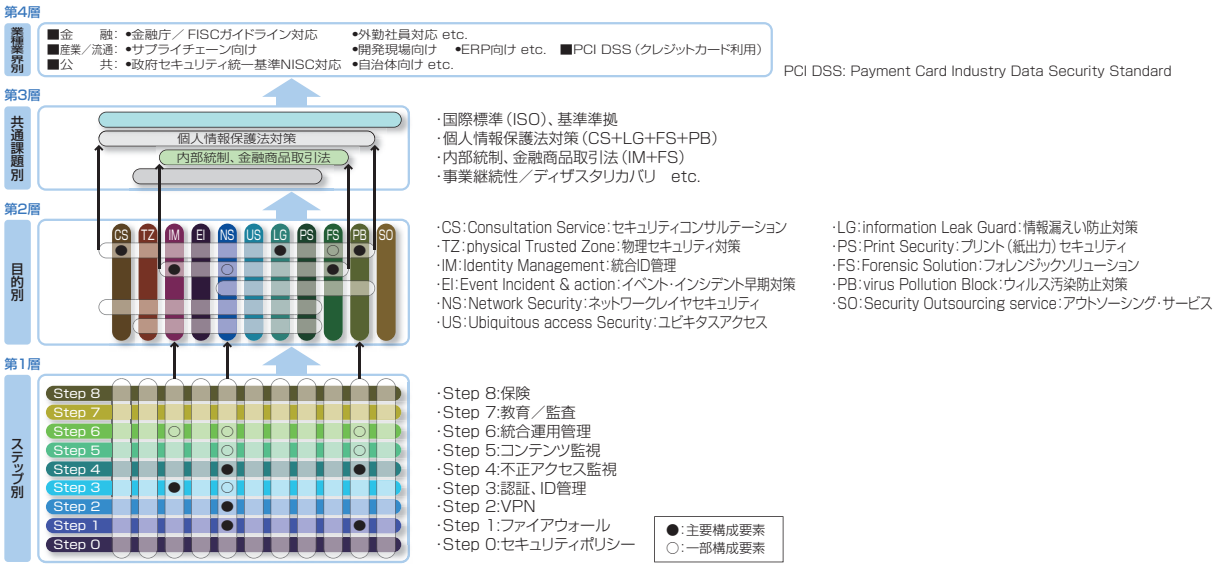
トータルセキュリティソリューション：Secureplaza

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縦横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、組織が直面するセキュリティ対策の実現に向け、ソリューションを継続的に拡張しています。このソリューションは以下の特徴を備えています。

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、4階層のモデルでトータルに包含しています。

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）に縦横に対応できる体系となっています。

Secureplazaのソリューション全体体系［4階層モデル］>>



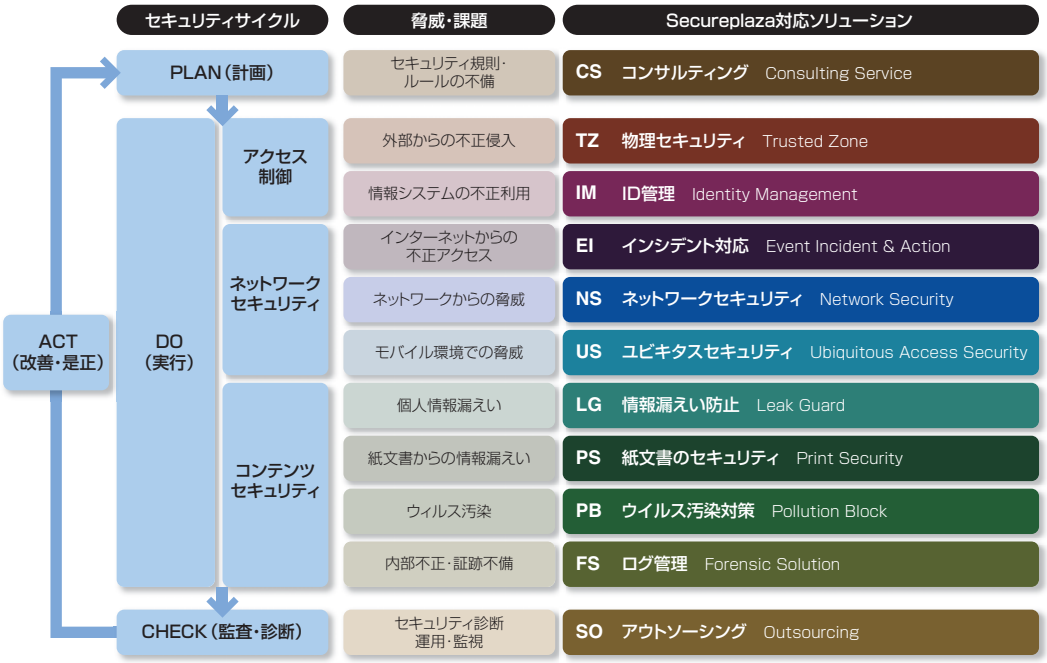
お客様のセキュリティを実現する トータルセキュリティソリューション Secureplaza

Secureplazaの体系

Secureplazaの全体系は、P29に示す4階層のモデルで構成されています。第1層は、システムやサービスの広がりに応じて顕在化してくる脅威に対するセグメントごとのステップ別対策群、第2層は、情報漏えい防止から証跡管理まで個々の目的に沿った対策群、第3層は、法令遵守や国際標準化への対応など、組織としての共通課題に対する対策群、第4層は、業種や業界、あるいは公的機関に固有の基準やガイドラインに対する対策群から成ります。上位の層は下位の層の部分を組み合わせて実現しており、システムおよび組織におけるあらゆるセキュリティ対策に縦横に応えられるトータルソリューションとなっています。また各層ごとに、その対策を実現する300以上の商品群がマッピングされています。

第1層のステップ別対策は、システムやサービスの広がりに応じて、セキュリティポリシーの策定と実践、ファイアウォール、通信路保護、認証、不正侵入検知、コンテンツ監視、統合運用管理、教育、監査、保険など9ステップから成っています。第2層の目的別対策の全体像は下図のとおりです。PDCA（Plan-Do-Check-Act）のサイクルに沿って、セキュリティポリシーをはじめとする全体のマネジメントシステムの策定から、実行フェーズはアクセス制御、ネットワークセキュリティ、コンテンツセキュリティ、監査・診断フェーズはセキュリティ診断やアウトソーシングなど、11のソリューション群から成っています。

Secureplaza目的別ソリューション［第2層］>>



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、ネットの活用へと発展してきました。そのなかで、さまざまな新しい脅威が顕在化、増大化し、さらにコンプライアンスの課題なども浮上し、それらに対して、後付けとなる形でさまざまなセキュリティ対策が講じられてきました。一方、セキュリティ面を含むシステムの運用管理コストの増大が、新たな問題として浮上してきています。

現行システムへの対策は今後も重要な課題ですが、中長期的には、次期の組織システムを視野に入れていくべき時期を迎えています。セキュリティの抜本的な改善と、運用管理の効率化を含めた、組織にとってより好適なシステムの構築を実現するための主要な要件としては、以下が挙げられます。

①セキュアかつ効率的なプラットフォーム構造
②多数のシステム群に対するユーザID管理
③厳格な認証
④統合運用管理
⑤証跡管理
⑥クラウド型セキュリティサービス

Secureplazaは、これらの要件にも対応しています。

①セキュアかつ効率的なプラットフォーム構造

情報やリソースの管理と処理を中央でするサーバベースコンピューティング、仮想化によるサーバ統合、シンクライアント化が鍵で、Blade Symphonyサーバ、仮想化ソフトウェアVirtage、ディスクレスのセキュリティPCなどが挙げられます。

②多数のシステム群に対するユーザ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管理システムの構築ソリューションとして、Secureplaza/IM（Identity Management）があります。

③厳格な認証

システム全体のセキュリティのレベルを向上させるのに非常に効果的で、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があります。

④統合運用管理

組織システム全体の統合運用管理基盤として、JP1シリーズがあります。

⑤証跡管理

証跡ログの取得、管理、分析、証跡保管に至るトータルな証跡管理ソリューションとして、Secureplaza/FS（Forensic Solution）があります。

⑥クラウド型セキュリティサービス

初期投資や運用管理コストを低減し、最新の技術・人材・設備を提供するサービスとして、Secureplaza/SO（Security Outsourcing service）があります。

注力する取り組み事例：クラウドコンピューティングへの取り組み

日立クラウドソリューション Harmonious Cloud

「安全・安心」、「スピード・柔軟」、「協創」をコンセプトとしたHarmonious Cloudを企業情報システムに適用することにより、IT投資リスクを軽減し、業務変化に柔軟かつ迅速に対応するビジネス環境を確立します。

企業が利用するクラウド形態への対応

企業が利用するクラウドには，社外事業者のITサービスをネットワーク経由で利用する「パブリッククラウド」と、社内にクラウド基盤を構築して各部門が必要なときに利用する「プライベートクラウド」の二つの形態があります。Harmonious Cloudは、両形態のソリューションの強化を推進しています。

〈パブリッククラウド〉

- PaaS（Platform as a Service）：
  ITリソースをサービスとして提供
  高信頼・高セキュリティを備えたITリソース（仮想マシン：サーバ/OS、ストレージなど）をサービスとして提供します。
- SaaS（Software as a Service）：
  アプリケーション機能をサービスとして提供
  各業種/業務に対応した幅広いアプリケーションをサービスとして提供します。セキュリティについても、ウィルス対策機能やWebアプリケーション脆弱性対策機能、また、クラウド環境下での確実な本人認証を可能とする指静脈認証を、SaaS型セキュリティサービスとして提供します。

〈プライベートクラウド〉

高信頼なプライベートクラウドの構築・運用をトータルで支援します。

ハイブリッドクラウドへの取り組み Harmonious Cloud Framework

クラウドの普及は、システムの形態にも大きな変化をもたらします。企業は、通常の日々の業務処理に必要なIT能力のみを社内にプライベートクラウドとして保持して業務を実行し、一時的、あるいは試行的に必要な機能・システムはパブリッククラウドを利用するという「ハイブリッドクラウド」が主流になっていくと考えられます。

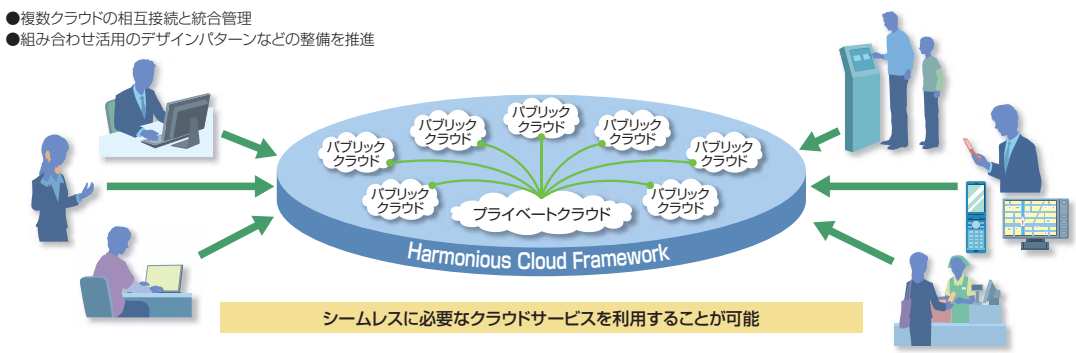
この新たな形態において、プライベートクラウドとパブリッククラウドのシームレスな連携、パブリッククラウド上のSaaSを組み合わせたシステム構築を可能とするフレームワークが「Harmonious Cloud Framework（HCF）」です。

HCFでは、次に示すような各種フレームを用意します。

- プライベートクラウドから、SaaSを組み合わせた業務を開発・実行するためのアプリケーション連携フレーム
- パブリッククラウド上の計算機資産を利用するリソース連携フレーム
- プライベートクラウドを効率的に管理・運用するためのフレーム
- 業務の機密性、保全性、可用性を確保するためのセキュリティフレーム

HCFは、処理の分散、ソフトウェアのサービス化と流通が進むクラウドにおいて、安全で効率のよい業務システムを実現する枠組みです。

ハイブリッドクラウドを牽引するHarmonious Cloud Framework >>



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 TC223

国際標準化機構（ISO）のテクニカルコミッティ（TC）223では、社会セキュリティ（Societal Security）をテーマとしており、緊急事態準備および事業継続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。

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、48カ国200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。

- 安心・安全インターネット推進協議会
- （独）情報処理推進機構（IPA）
  10大脅威-執筆者会
  情報システム等の脆弱性情報の取扱いに関する研究会 など
- 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
- （社）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
- 情報セキュリティ教育事業者連絡会（ISEPA）
- 日本セキュリティ・マネジメント学会ITリスク学研究会

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（財）日本情報処理開発協会（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（2011年3月末日現在）。

株式会社 日立製作所
株式会社 日立製作所 茨城病院センタ
株式会社 日立製作所 小平記念東京日立病院
株式会社 日立製作所 日立横浜病院

株式会社 エー・シー・エス
沖縄日立ネットワークシステムズ株式会社
株式会社 九州日立情報システムズ
株式会社 九州日立ソリューションズ
クリエイティブソリューション株式会社
株式会社 国際電気テクノサービス
株式会社 コンピュータシステムエンジニアリング
株式会社 四国日立情報システムズ
株式会社 中国日立情報システムズ
株式会社 でんさテクノ
東京エコリサイクル株式会社
株式会社 日情秋田システムズ
株式会社 日情システムソリューションズ
日誠コンピュータサービス株式会社
バブ日立ビジネス株式会社
日立アイ・エヌ・エス・ソフトウェア株式会社
株式会社 日立アイシーシー
株式会社 日立ICTビジネスサービス
株式会社 日立インスファーマ
日立インターメディックス株式会社

日立SC株式会社
株式会社 日立インフォメーションアカデミー
株式会社 日立エンジニアリング・アンド・サービス
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
日立建機ビジネスフロンティア株式会社
日立公共システムエンジニアリング株式会社
日立公共システムサービス株式会社
株式会社 日立国際ビジネス
日立コミュニケーションネットワークス株式会社
株式会社 日立四国ソリューションズ
株式会社 日立システム九州
株式会社 日立システムバリュー
株式会社 日立情報システムズ
株式会社 日立情報制御ソリューションズ
日立情報通信エンジニアリング株式会社
日立製作所健康保険組合
株式会社 日立総合計画研究所
株式会社 日立ソフテック

日立ソフトシステムデザイン株式会社
株式会社 日立ソリューションズ
株式会社 日立中国ソリューションズ
日立電子サービス株式会社
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
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 日立東日本ソリューションズ
日立ビジネスソリューション株式会社
日立フィールドアンドファシリティサービス株式会社
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
日立物流オリエントロジ株式会社
日立物流ソフトウェア株式会社
株式会社 日立プレーン
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
株式会社 日立メディコ
ファイナンシャルブリッジ株式会社
株式会社 北海道日立情報システムズ
株式会社 北海道日立電子サービス
マクセル精器株式会社

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（2011年3月末日現在）。

株式会社 日立製作所（ITサービス事業部）
株式会社 日立製作所（情報制御システム社）
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（ネットワーク営業統括本部）
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

沖縄日立ネットワークシステムズ株式会社（沖縄サポートセンター）
株式会社 コンピュータシステムエンジニアリング
日立SC株式会社（本社）
日立公共システムエンジニアリング株式会社（全社）
日立公共システムサービス株式会社（全社）
株式会社 日立国際電気（情報ソリューション本部　フィールドサポート部、関西支社 情報営業所）
株式会社 日立情報システムズ（アウトソーシングセンタ事業部）

株式会社 日立情報システムズ（アウトソーシングセンタ事業部 第三DC本部）
株式会社 日立情報システムズ（関西支社）
株式会社 日立情報システムズ（SHIELD セキュリティセンタ）
株式会社 日立情報システムズ（東北支社）
株式会社 日立情報システムズ（西日本支社）
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（エンタープライズコンピューティングセンタ）
日立電子サービス株式会社（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）
日立電線ネットワークス株式会社
日立ビジネスソリューション株式会社
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

日立が提供する、国際規格（ISO/IEC 15408）に基づきセキュリティ機能・品質が評価・認証された代表的なIT製品は、以下のとおりです（2011年3月末日現在）。

製　品	TOE種別※1	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	EAL4+ALC_FLR.1
HiRDB/Single Server Version 8 08-04	データベース管理システム	EAL4+ALC_FLR.1
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	EAL4
Enterprise Certificate Server Set（01-01-A）	認証局機能	EAL3
JP1/Base 認証サーバ 08-10（Windows版）	システム運用管理	EAL2+ALC_FLR.1
uCosminexus Application Server 08-00	アプリケーションサーバ	EAL2+ALC_FLR.1
EUR Form Client　05-07	帳票データ作成支援ソフトウェア	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	EAL2+ALC_FLR.1
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	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	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	EAL2
証明書検証サーバ 03-00	PKI	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	EAL2
DocumentBroker Server Version 3 03-11	文書管理	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	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	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。

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「暗号モジュール試験および認証制度（JCMVP）」によって以下の認証取得した製品は、次のとおりです（2011年3月末日現在）。

製　品	認証取得レベル
Keymate/Crypto JCMVP ライブラリ04-00（Solaris版、Windows版）	レベル1
Keymate/Crypto JCMVP ライブラリ04-00	レベル1

機能安全認証の取得状況

安全に関する国際規格IEC61508に基づいて評価・認証された下記の機能安全コントローラを提供しています（2011年3月末日現在）。

製　品	規格
R800FS/HSC800FS	IEC61508、Part1-7:1998-2000 SIL2

日立グループの概要

会社概要 (2011年3月末日現在)

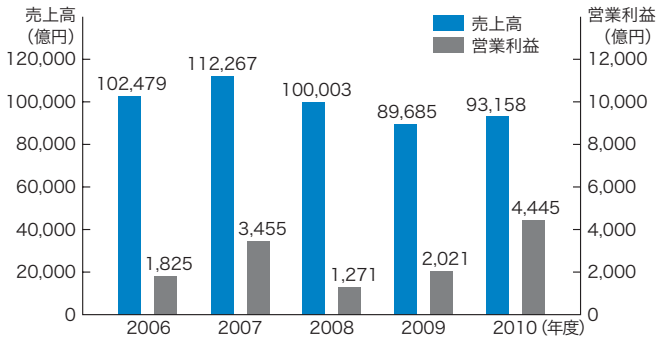
商　　号　株式会社日立製作所
Hitachi, Ltd.
設立年月日　大正9年(1920年)2月1日
(創業明治43年(1910年))
本店の所在地　東京都千代田区丸の内一丁目6番6号
代　表　者　代表執行役　執行役社長　中西 宏明

資　本　金　409,129百万円
従業員数　(個別)32,926名
(連結)361,745名
連結子会社数　913社(国内351社、海外562社)
(含む、変動持分事業体)
持分法適用関連会社数　164社(国内72社、海外92社)

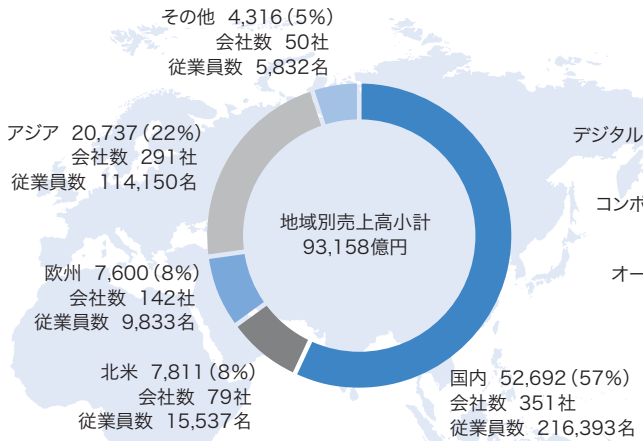
事業概要と業績 (2011年3月期)(連結)

売　上　高　93,158億円(前期比104%)
営業利益　4,445億円(前期比220%)
設備投資額　5,568億円(前期比102%)
研究開発費　3,951億円(前期比106%)
連結売上高に占める海外生産高比率　27%

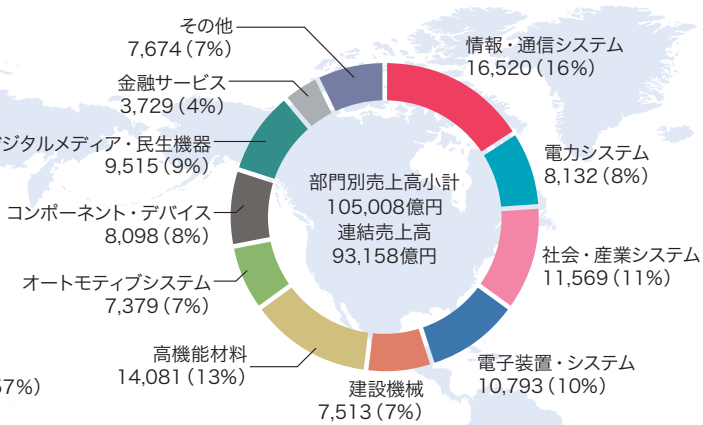
●売上高および営業利益推移



●地域別売上高(億円)



●部門別売上高(億円)



株式会社 日立製作所
IT統括本部　IT戦略本部　情報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