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：2011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：2012年6月発行

日立グループは「優れた自主技術・製品の開発を通じて社会に貢献する」という企業理念のもと、創業以来100年以上にわたり、日本をはじめとして世界各地で様々な社会インフラシステムの構築に携わることで、安心・安全な社会の実現をめざしてまいりました。今後、この経験に基づいた知見を活かし、社会インフラと情報システムを融合した社会イノベーション事業を軸に、世界各地のパートナーとの協力による価値の創造を通じて、安心・安全で持続可能な社会の実現に向けさらに貢献してまいります。

情報セキュリテイに関しましては、お客様からお預かりした情報資産を適切に管理するため、全社一体となって取り組んでおります。日立グループとして定めた「情報セキュリティ方針」のもと、規則・体制の整備、最新IT技術を活用した安全対策の実施、従業員の教育、監査による点検、取引先のセキュリティ対策状況の確認・審査など、情報セキュリティマネジメントサイクルを推進することにより活動の有効性を評価し、取り組み内容の充実を図っております。

IT技術の進展とその利用拡大のスピードはめざましく、クラウドコンピューティング、スマートフォン、ソーシャルネットワーキングサービス（SNS）など、経済性や利便性を追究する新技術やサービスの活用が急速に進んできております。それに伴い、情報セキュリティに関する脅威もますます高度化・複雑化し、また日々変化しております。例えば、昨今、標的型メール等による情報搾取や重要設備へのサイバー攻撃が発生しており、官民連携した取り組みもスタートしております。日立グループはこのような活動にも積極的に参画し、これまで蓄積してきたノウハウと最新技術を駆使し、新たな脅威への対抗策を構築してまいります。そして、確立した成果をお客様に提供することで、情報セキュリティに関してより一層安心・安全な社会の実現に向けて一翼を担ってまいります。

今回で2回目の改定となる本報告書では、あらたに、日立のクラウドソリューションにおけるセキュリティへの取り組みやサイバー攻撃に対応したIT施策の多層防御の取り組みなどを盛り込みました。

情報セキュリティへの取り組みの重要性は益々高まってきております。本報告書でご紹介する私たちの取り組みが、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につながれば幸いです。

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

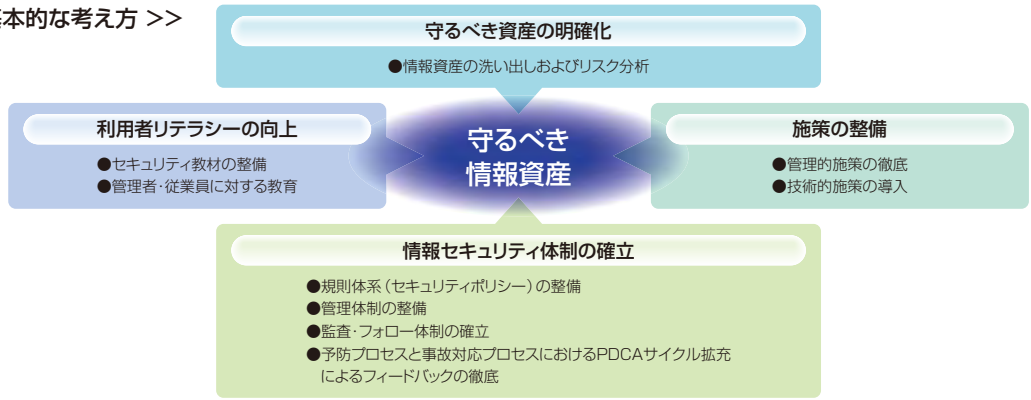
情報セキュリティガバナンスの取り組み方針

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

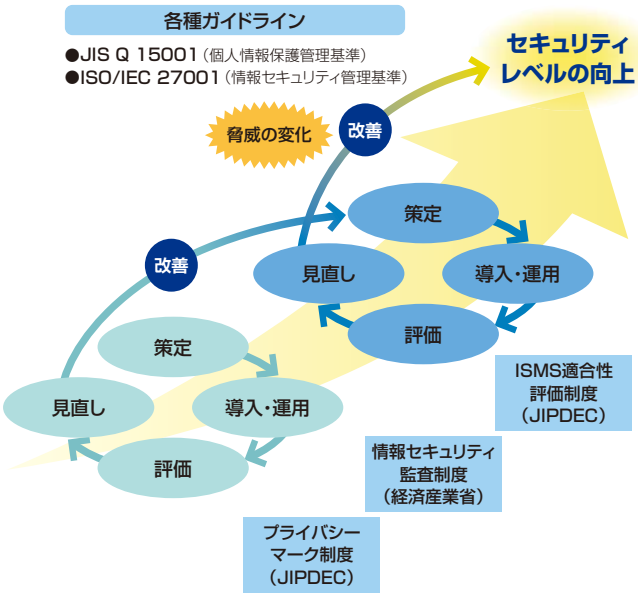
守るべき情報資産を明確にし、脆弱性評価とリスク分析に基づいて情報漏えい防止施策を実施しています。事故は「起きるかもしれない」という考え方を一歩進めて、「必ず起こるものだ」という前提に立って、緊急時のマニュアルを作成し、対応しています。

（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。

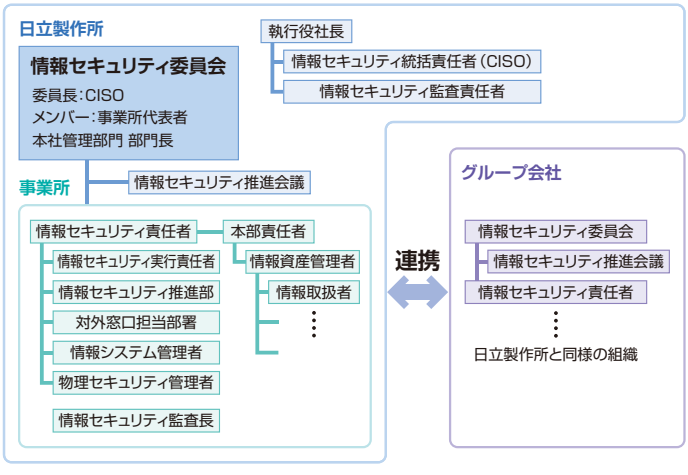
情報セキュリティ委員会の決定事項は、全事業所実務者が出席する情報セキュリティ推進会議を通じて、各事業所に徹底されます。

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

「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
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	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	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。

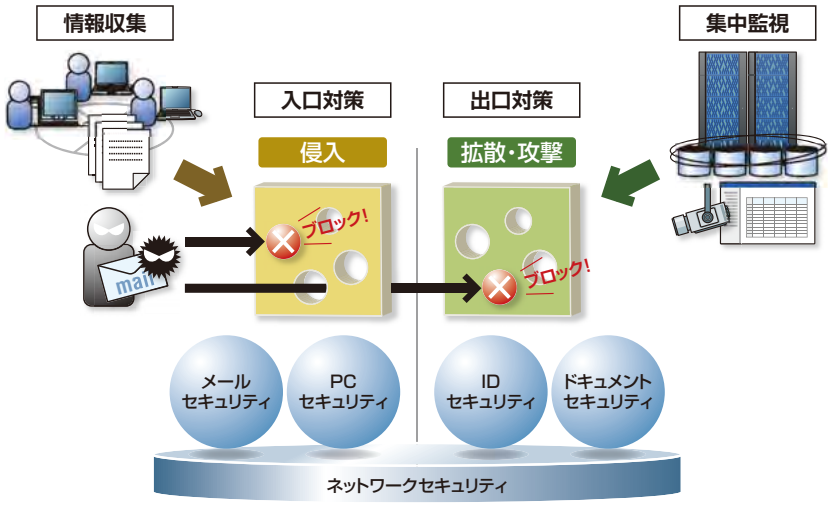
また、日立グループ製品を積極的に導入することで、その結果を製品設計部門にフィードバックし、日立グループ製品の更なる醸成に役立てています。

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として、以下の項目に取り組んでいます。

- 組織間IRT連携（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と迅速なインシデントレスポンス



情報セキュリティに対する技術面での取り組み

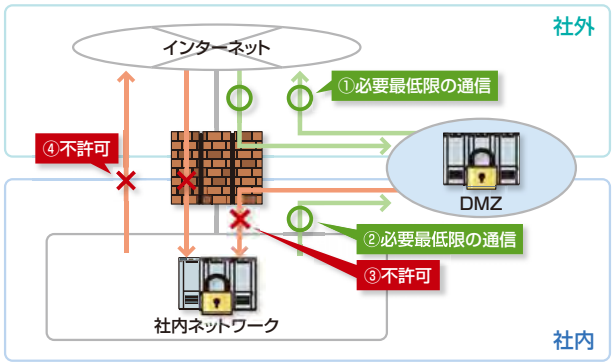
ネットワークセキュリティ

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。

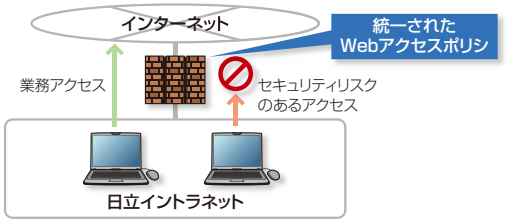
※1：DeMilitarized Zone　※2：Intrusion Prevention System



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。

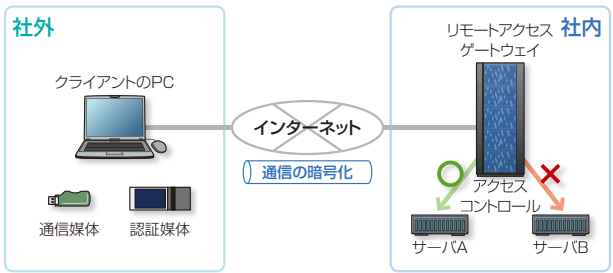
- 認証による、利用者の限定とログ保存およびログ監査
- 統一されたポリシーによる、URLフィルタリング
- Webウイルスチェック



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。

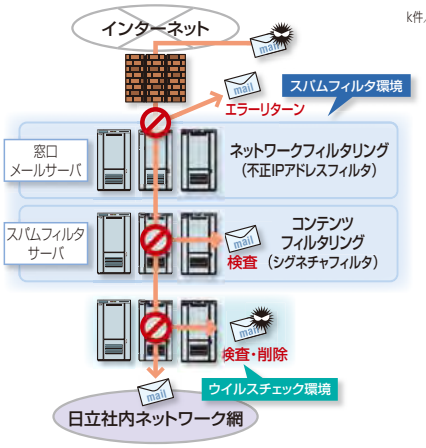
1. 外部からの脅威に対する対策

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。

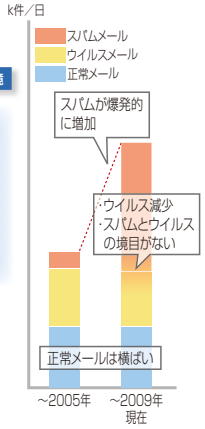
2. 内部で生じる脅威に対する対策

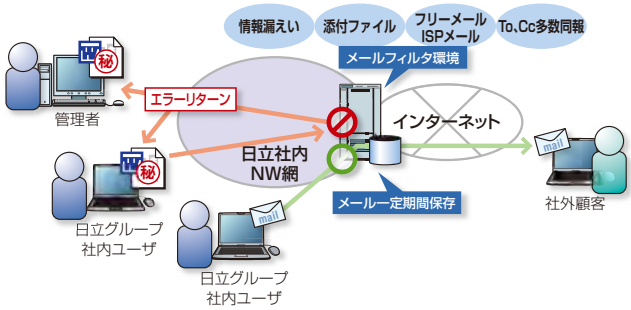
内部で生じる脅威については、①コンピュータウイルス拡散の脅威、②情報漏えいの脅威を考慮し、メール配送上にメールフィルタサーバを設置し、問題のないメールのみを配送しています。

〈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〉





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。

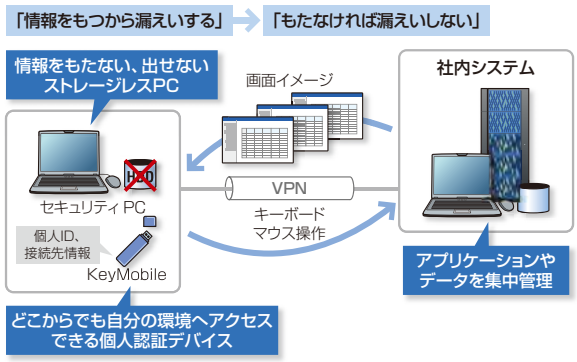
PCに関するリスクとして、以下が挙げられますが、内部・外部要因の組み合わせによってリスクが変化します。

（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

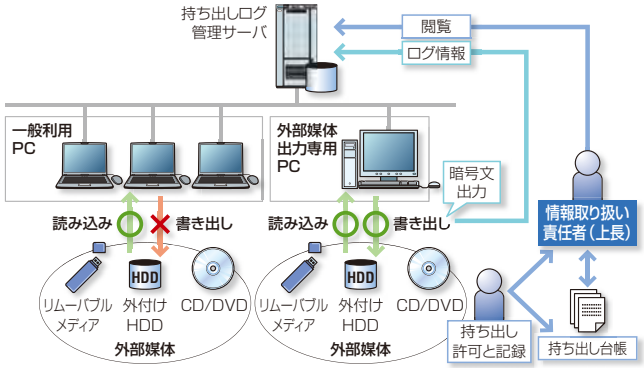


情報セキュリティに対する技術面での取り組み

●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。

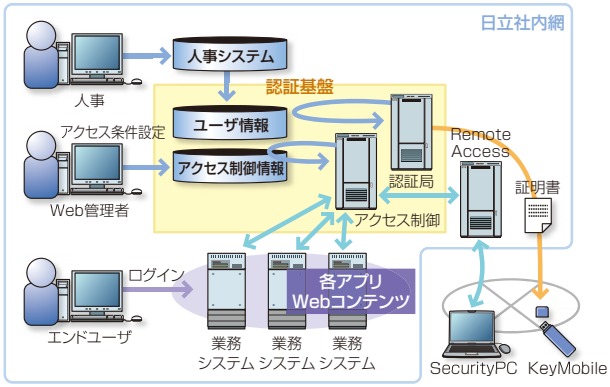
2. 個人単位での認証とアクセス制御

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。

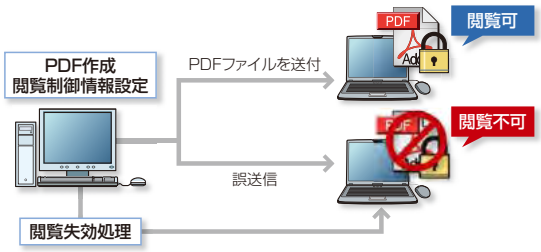
情報セキュリティに対する技術面での取り組み

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。

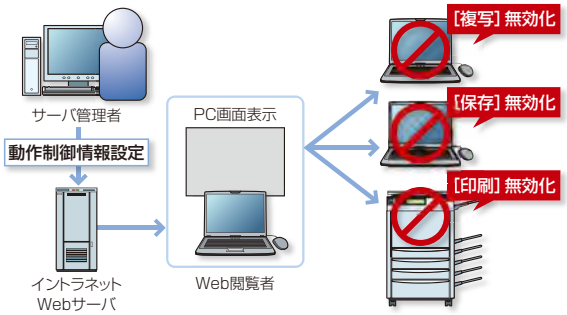
1. 電子ドキュメントの閲覧停止による情報漏えい防止

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。



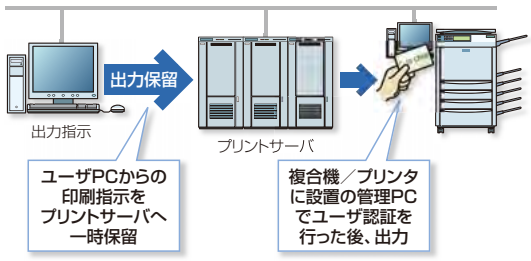
2. Webサーバコンテンツの情報漏えい防止

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。



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。

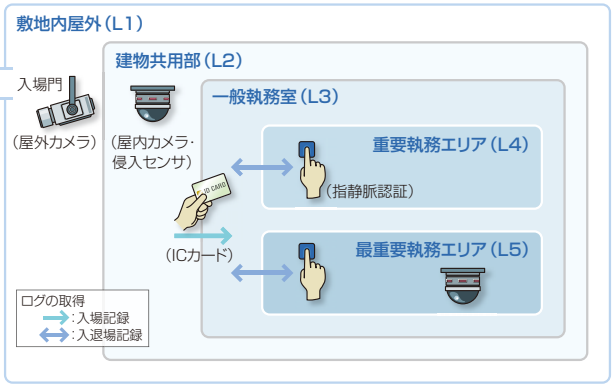
(2) 日立グループの製品と技術の活用

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。

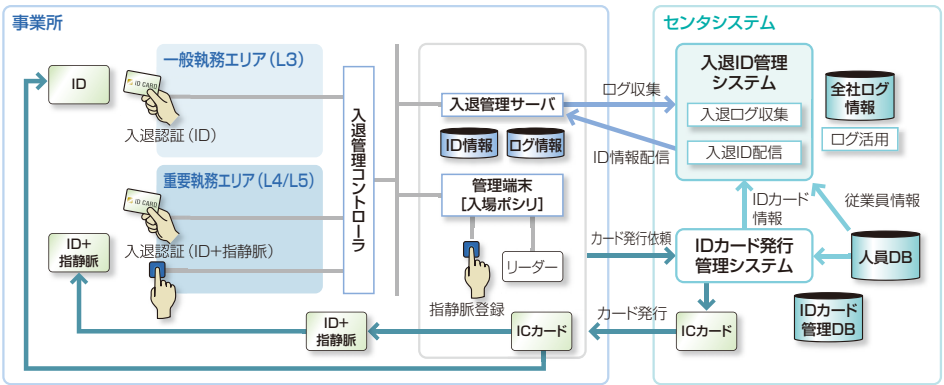
(3) センタシステムを活用した運用業務の効率化

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。

区域のセキュリティ対策レベルと対策方式 >>



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

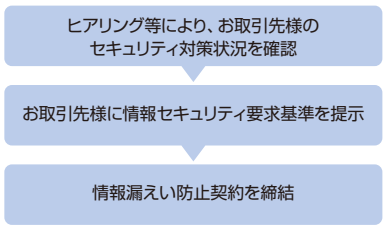
日立では、社会イノベーション事業を支える企業グループとして、お取引先様も日立と同じレベルの管理を実施していただき、情報セキュリティ事故の予防、再発防止に向けた取り組みを行っています。

(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。

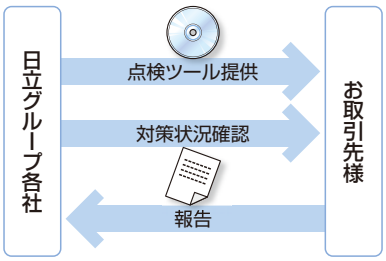
●情報漏えい防止契約書締結社数：約11，500社



(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：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。

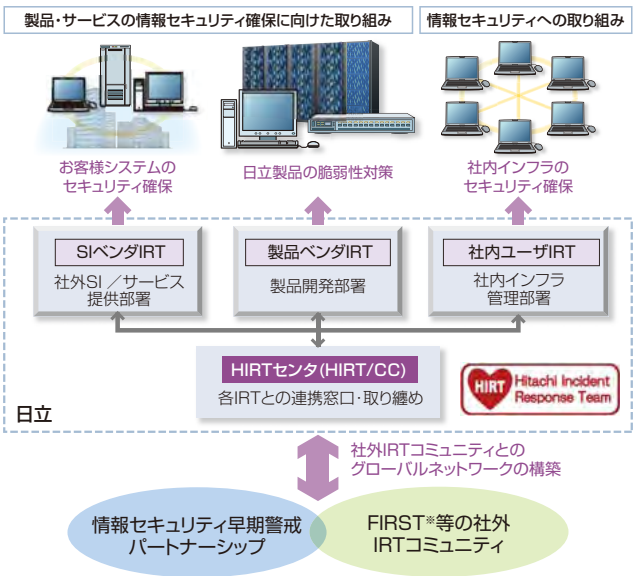
HIRTは、脆弱性対策とインシデント対応とを推進するために、下記のように、4つのIRT（Incident Response Team）という活動モデルを採用しています。4つのIRTとは、

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) 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

研究所との共同研究体制で、「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開発に取り組んでいます。

●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など脆弱性対策ならびにインシデント対応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、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/

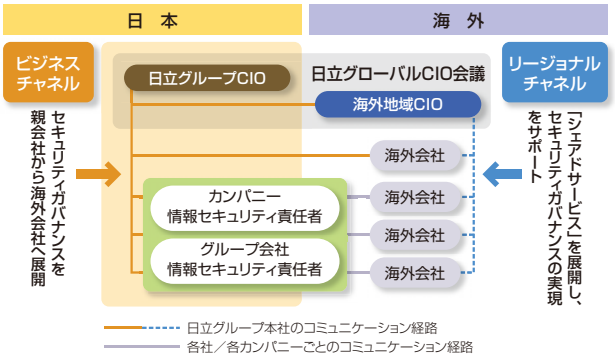
グローバル情報セキュリティの取り組み

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。

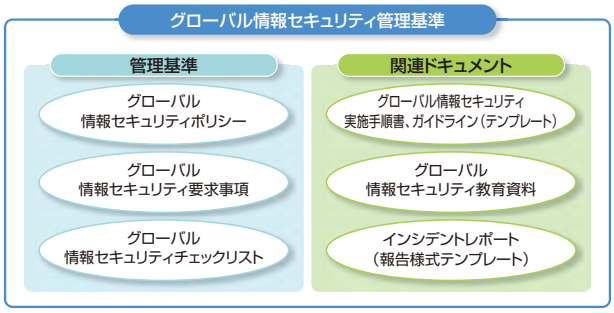
グローバル情報セキュリティ管理体制

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:一般財団法人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。現在、2013年3月の3回目の更新に向け継続的に取り組んでいます。

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

日立製作所　プライバシーマーク >>

(株)日立製作所　個人情報保護方針

1. **個人情報管理規則の策定および個人情報保護マネジメントシステムの継続的改善**
   当社は、役員および従業員に個人情報保護の重要性を認識させ、個人情報を適切に利用し、保護するための個人情報管理規則を策定し、個人情報保護マネジメントシステムを着実に実施します。更に、維持し、継続的に改善します。
2. **個人情報の収集・利用・提供および目的外利用の禁止**
   当社は、事業活動において、個人情報をお預かりしていることを考慮し、それぞれの業務実態に応じた個人情報保護のための管理体制を確立すると共に、個人情報の収集、利用、提供において所定の規則に従い適切に取扱います。また、目的外利用は行わない、およびそのための措置を講じます。
3. **安全対策の実施並びに是正**
   当社は、個人情報の正確性および安全性を確保するため、情報セキュリティに関する諸規則に則り、個人情報へのアクセス管理、個人情報の持ち出し手段の制限、外部からの不正アクセスの防止等の対策を実施し、個人情報の漏洩、滅失またはき損の防止に努めます。また、安全対策上の問題が確認された場合など、その原因を特定し、是正措置を講じます。
4. **法令・規範の遵守**
   当社は、個人情報の取扱いに関する法令、国が定める指針その他の規範を遵守します。また、当社の個人情報管理規則を、これらの法令および指針その他の規範に適合させます。
5. **個人情報に関する本人の権利尊重**
   当社は、個人情報に関して本人から情報の開示、訂正もしくは削除、または利用もしくは提供の拒否を求められたとき、および苦情、相談の申し出を受けたときは、個人情報に関する本人の権利を尊重し、誠意をもって対応します。

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

個人情報保護に対する取り組み

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〉

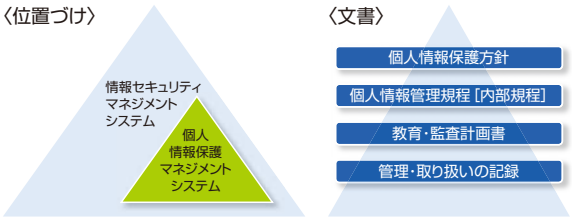
(1) 組織的安全管理措置:
　規程、体制の整備運用および実施状況の確認等
(2) 人的安全管理措置:
　非開示等契約の締結、教育・訓練等
(3) 物理的安全管理措置:
　入退館(室)の管理、盗難防止措置等
(4) 技術的安全管理措置:
　情報システムへのアクセス制御、不正ソフトウェア対策等

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 >>



個人情報保護に対する取り組み

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

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。

個人情報保護に対する取り組み

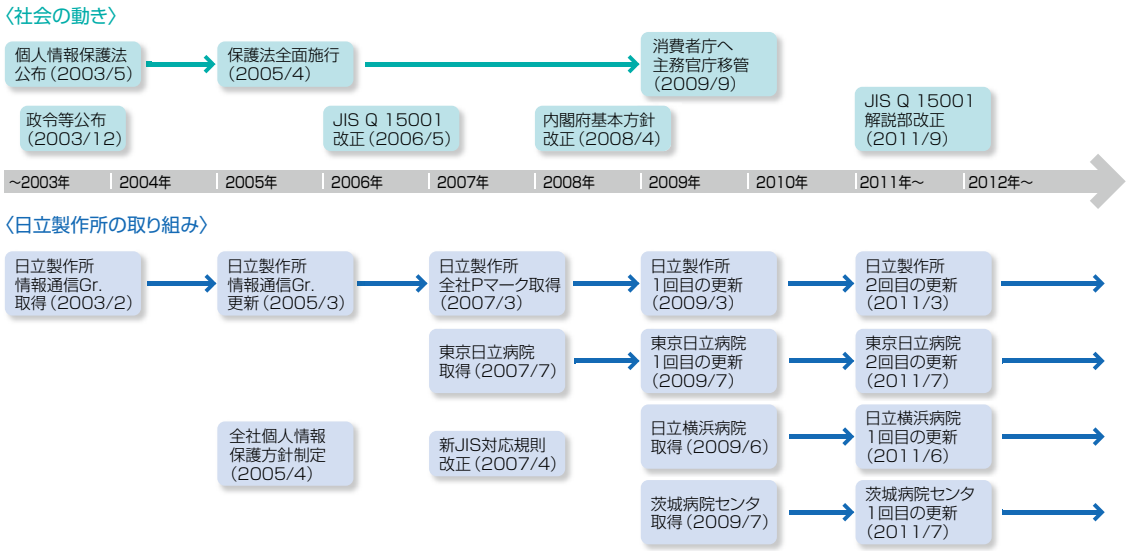
日立グループ全体の取り組み（プライバシーマーク取得推進状況）

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。2012年3月31日現在、70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続いて取得し、患者をはじめとする個人情報の保護に継続して努めています。

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 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。

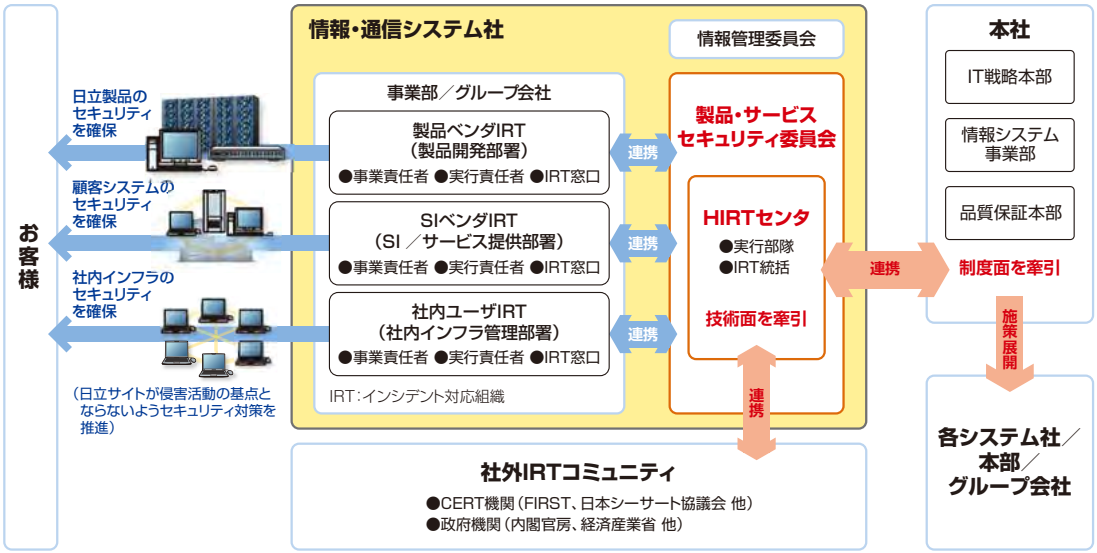
(3) セキュリティインシデントへの迅速な対応

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
(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継続的な検討・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。

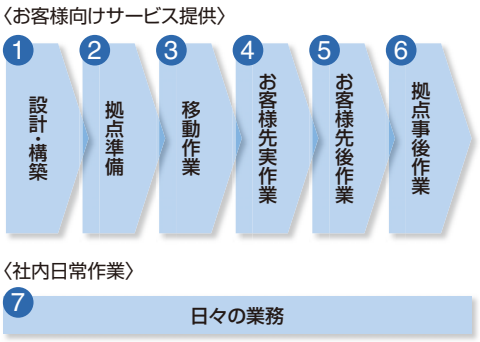
(3) 技術者向けセキュリティ教育

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、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、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、製品検査を行う担当者へのトレーニングなども実施しています。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。

ソフトウェアの脆弱性問題への対応の考え方

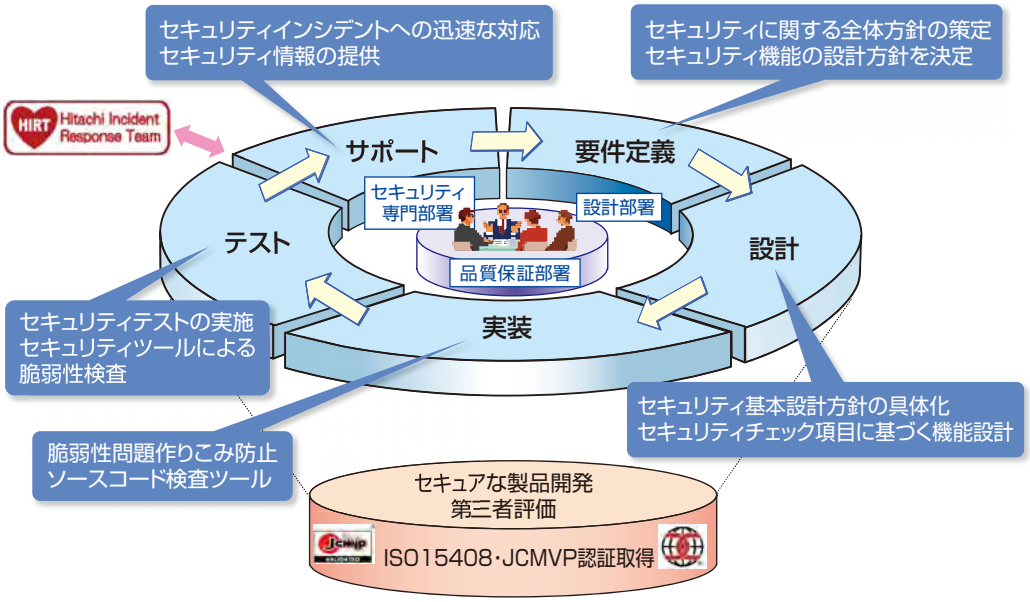
ソフトウェアの脆弱性問題は、設計、実装、テストフェーズで刈り取ることが基本ですが、新たな脆弱性が発見されたり、攻撃手法が登場することが考えられます。したがって、ソフトウェア製品の運用フェーズにおける対応も考慮しておく必要があります。

これらの取り組みは、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

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、P.39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

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セキュリティへの取り組み

日立クラウドソリューション Harmonious Cloud（プラットフォームリソース提供サービス）

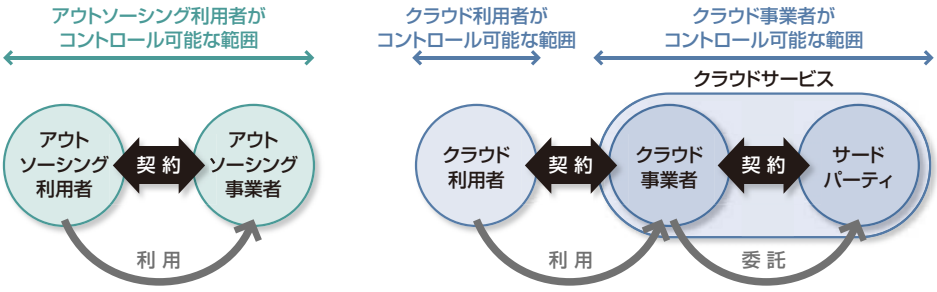
新たなITの提供形態であり、社会インフラの1つとなるクラウドにおいて、日立は種々のセキュリティに関する取り組みを行い、企業情報システムに適用可能な「安全・安心クラウド」を実現します。

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」）の普及が加速しています。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、クラウドで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、「共用」と「借用」というクラウド独特の特性に対応した情報セキュリティが必要となります。また、業務システムにおいて一部にクラウドを利用したような場合には、ITシステム全体として、従来システムと同等な情報セキュリティの確保が求められます。

従来の業務委託とクラウドとのコントロール範囲の違い>>



(a) 通常の業務委託時　　(b) クラウド利用時

クラウドコンピューティングの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。

このうち、経済産業省のガイドラインについては国際標準化に向けISO/IEC SC27に仕様案を提示するなど、国際標準検討の場においてもクラウドに関するセキュリティの議論が行われています。

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」を実現するセキュリティへの取り組み

日立クラウドソリューション Harmonious Cloud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なっています。Harmonious Cloud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. 2.1※が示す12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契約にて定め、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。

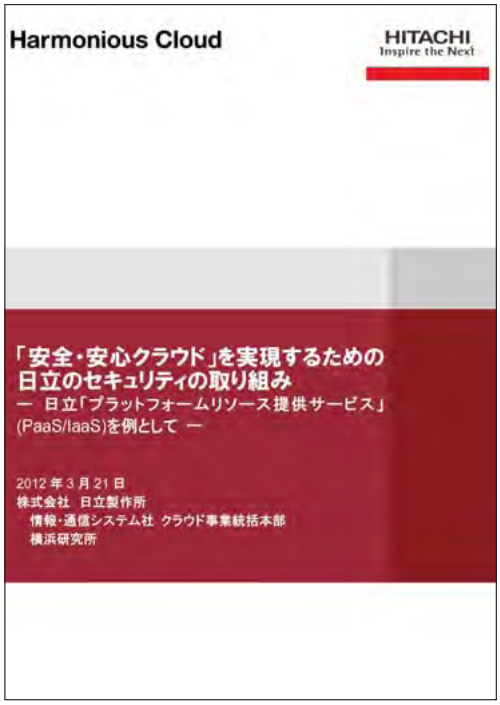
さらに、セキュリティに関する基準は、業種によっても異なることから、各業種の主要な基準に対する施策の整理を進めています。

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を広く公開しています。
http://www.hitachi.co.jp/cloud/solution/paas/platform.html

Harmonious 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。

※CSA: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1、https://cloudsecurityalliance.org/research/initiatives/security-guidance/（2009年12月）

ホワイトペーパ >>



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。

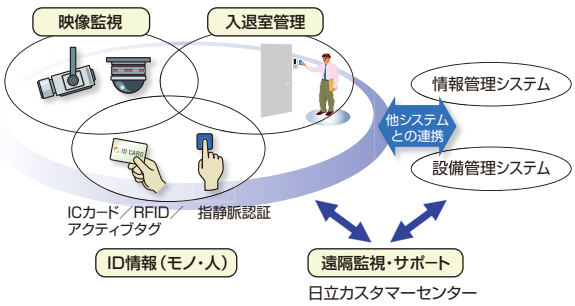
オフィスビルや工場では、各部署の役割や取り扱い情報のレベルに応じて、必要とされるセキュリティのレベルもさまざまです。物理セキュリティの導入にあたっては、守る場所、守るものを明確にしたうえで、適切なセキュリティレベルを設定し、そのレベルに応じたシステムを構築することが重要です。

(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 インフラシステム社は、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インフラシステム社の取り組みを以下に述べます。

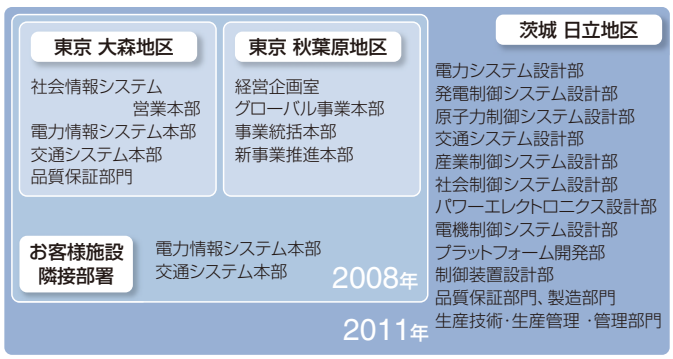
お客様の機密情報の管理（情報セキュリティマネジメントシステム（ISMS）の確立）

インフラシステム社は、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。インフラシステム社では、この要請に応えるため、トップマネジメント指揮のもと、情報セキュリティマネジメントシステム（ISMS）の国際規格（ISO/IEC 27001：2005）に基づくISMSを構築し、2010年1月に、情報制御システム部門の認証取得が完了しました。その後も、更新審査、継続審査を受査し、ISMS認証を継続しています。

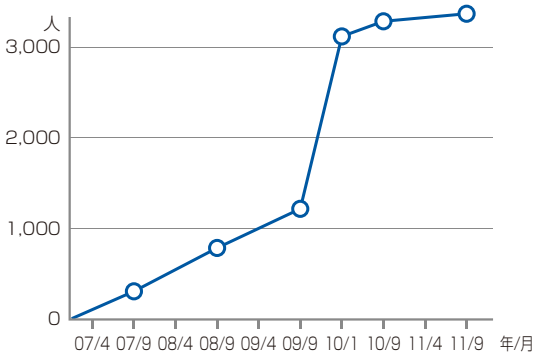
物理セキュリティ面では、全社統一基準に従った環境を構築中です。2008年度に日立地区に完成した新棟を始め、設計・品証・管理部門は、指静脈認証、ICカードを用いた入退室管理システムを適用し、防犯カメラを導入済です。現在、他の部門についても物理セキュリティ施設の構築、改築を計画的に推進しています。

インフラ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。

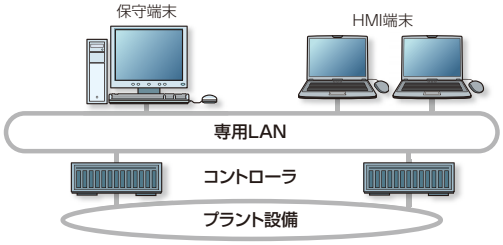
(1) 開発に着手した時点で、セキュリティリスクを洗い出します。
(2) 設計レビューで、セキュリティ設計（保護対象の設定、対策方針）を検証します。
(3) セキュリティ要件は、工場出荷時およびお客様に引き渡す前に、セキュリティ検査ツール等で全件確認します。

●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

情報系システムに対するコンピュータウィルスによるサイバー攻撃や組織内部からの情報漏えいは従来からありましたが、近年、ライフラインを狙った事案の発生、意図的な情報漏えいの増加、制御システムを狙ったマルウェアの登場など、これまでターゲットとなっていなかった制御システムに対するセキュリティ面の脅威が高まってきています。

さらに、制御システムのセキュリティについては、「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」等の動きがあり、今後の制御システムにおいては、これらへの対応が必須となりつつあります。

インフラシステム社は、国際規格への対応として、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、遵守すべき要件とその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ています。システム開発時にこのガイドラインを適宜参照することで、該当する国際規格に効率よく対応できるだけでなく、システムのセキュリティレベルを所定の水準にすることができます。さらに、国際規格の中で要求されているセキュリティ機能（例えば、暗号化や認証）についても、対応していきます。

セキュリティ認証は、装置のベンダ認証が規定されています。このベンダ認証は、専用装置により対象装置に対し不正パケットの送信やDoS（Denial of Service attack）攻撃などを実行することで、これらの攻撃に対する装置のタフネス性の十分性を評価するものです。コントローラをはじめとして制御サーバやネットワーク装置のベンダ認証取得も計画しています。

(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、進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

近年のICT技術の普及・進展と利用拡大に伴って、セキュリティはより一般的な技術へと変貌し、様々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、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採用されるとともに、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年ごろより、電子政府システムの構築が本格化したことから、電子署名に必要な公開鍵暗号基盤（PKI）の研究を加速し、「証明書検証サーバ（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。

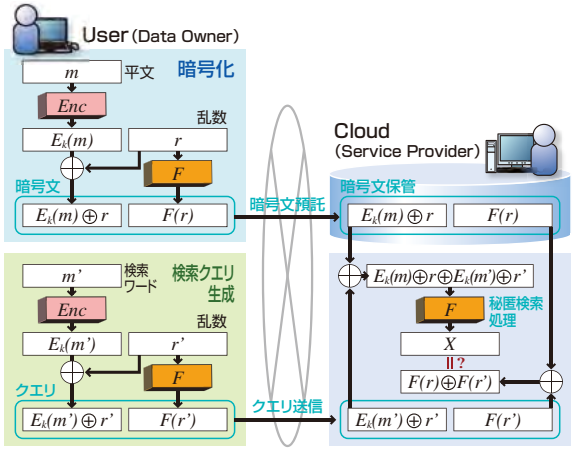
秘匿情報処理技術の開発

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。

本技術の適用先として、急速に進展が進むバイオインフォマティクス(生物情報科学)におけるゲノムデータ解析での応用が期待されています。今後、本技術をゲノムデータ解析向け秘匿検索処理技術へ応用し、既存のパブリッククラウドでも適用可能なセキュリティソリューションサービスとして、2013年度中の提供開始をめざします。

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

標的型攻撃対策への取り組み

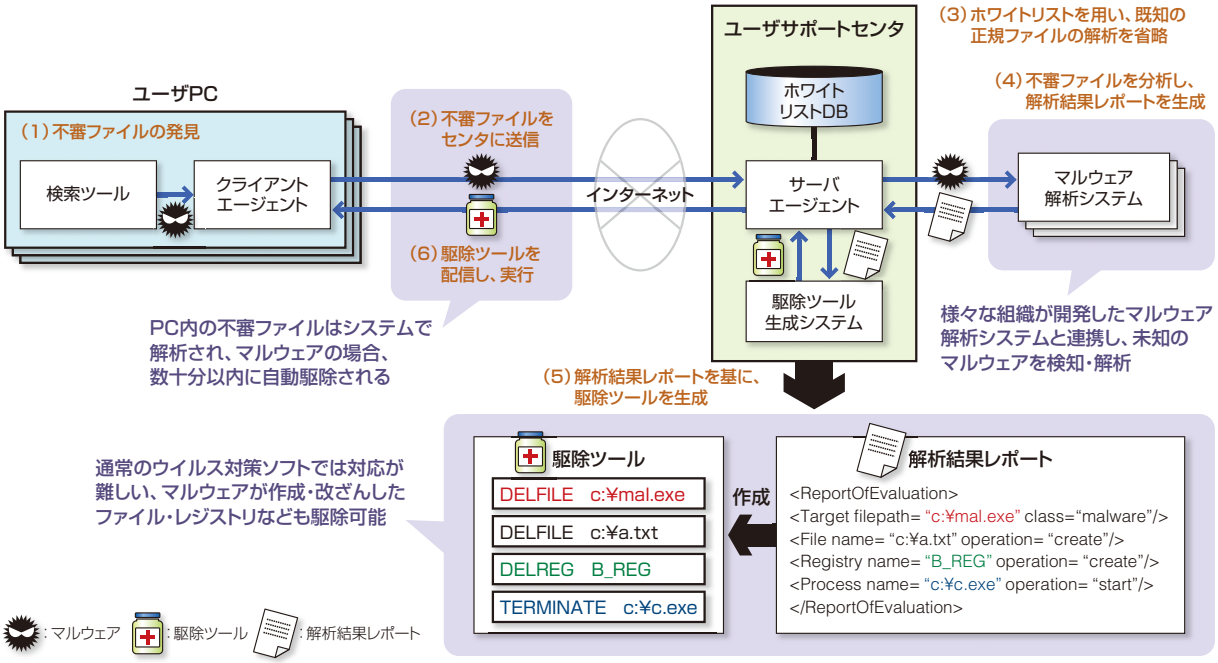
昨今、特定の企業の機密情報や社会インフラシステムを対象とした標的型攻撃の被害が大きな問題になっています。企業にとって顧客情報や機密情報の情報漏えいのリスクをいかに軽減するかが重要な課題となっており、情報漏えい事故を起こしたことによってブランドが棄損され、ビジネス機会が著しく減少した企業も少なくありません。

標的型攻撃では、マルウェアと呼ばれる、コンピュータやネットワークに害を及ぼす活動を行う、悪意あるプログラムが用いられます。従来、マルウェアの検知には、シグニチャと呼ばれる、各マルウェアのファイルの特徴を記述したデータを用いる方法が一般的でした。しかし、攻撃対象毎に特化したマルウェアが用いられる標的型攻撃では、従来の対策でマルウェアを検知することが困難になりつつあります。

日立では、PCで発見された不審ファイルの挙動を解析し、マルウェアと判断された場合は自動的に駆除するシステムの研究を行っています。実証実験において、本システムはマルウェアがPCで起動してからおよそ十分以内で、検知・駆除を完了することを確認しました。

上記には、総務省委託研究「大規模仮想化サーバ環境における情報セキュリティ対策技術の研究開発」、独立行政法人情報通信研究機構（NICT）委託研究「マルウェア対策ユーザサポートシステムの研究開発」の成果を含みます。

マルウェア対策システムの概要 >>



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、個人情報保護法や金融商品取引法をはじめとする法令の遵守など、（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

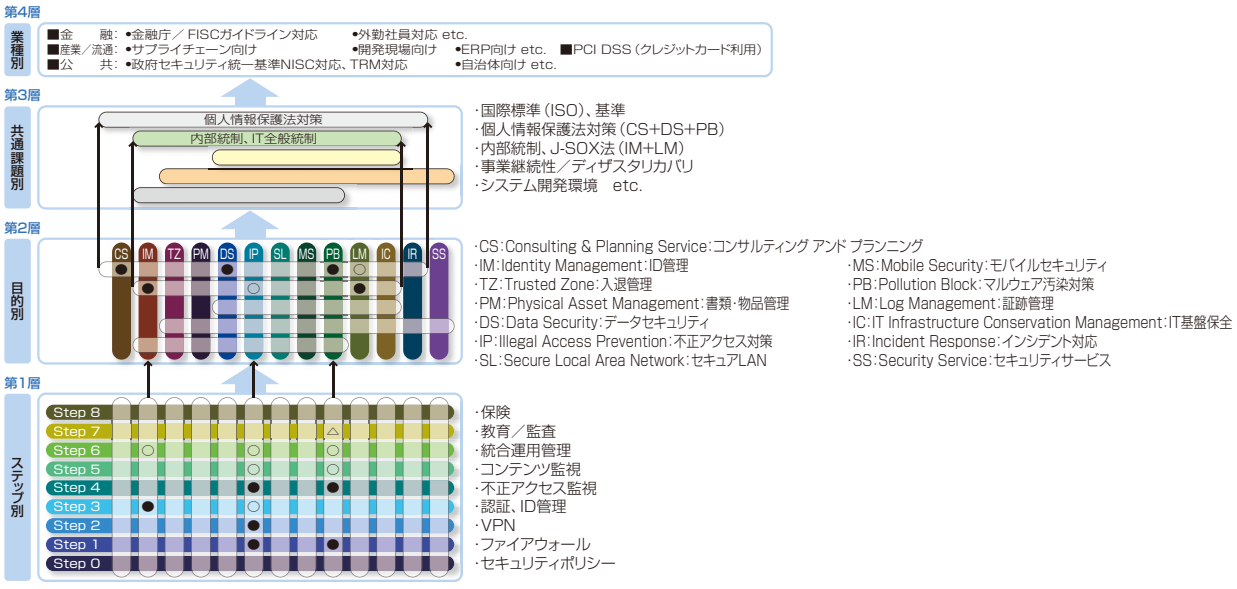
1996年頃より、IPプロトコルやWebシステムなどのインターネット技術を組織システムインフラで活用する動きが加速し始め、さらにPC端末の高機能化とも相まって、セキュリティへの対応が非常に重要な課題となってきました。

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、4階層のモデルによりカバーします。

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の全体体系は、前の頁に示す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層は不正アクセス対策や証跡管理などの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です。上位の層は下位の層を部分的に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。またこれらのソリューションを実現する300以上の商品群をラインアップしています。

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た、セキュリティポリシーの策定と実践、ファイアウォール、通信経路保護、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、保険などの9つのステップから構成されます。

第2層の目的別対策の全体像は下図のとおりです。Secureplazaは、7つのソリューションカテゴリ（組織的セキュリティ、ID管理、物理セキュリティ、データセキュリティ、ネットワークセキュリティ、セキュリティ基盤管理、サービス）と、各カテゴリを実現する13の目的別ソリューションから構成されます。

Secureplaza目的別ソリューション［第2層］>>

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
組織的セキュリティ	セキュリティ規則・ルールの不備	CS コンサルティング アンド プランニング Consulting and Planning Service
ID管理	情報システムの不正利用	IM ID管理 Identity Management
物理セキュリティ	外部からの不正侵入	TZ 入退管理 Trusted Zone Management
	書類・物品の盗難・紛失・誤廃棄	PM 書類・物品管理 Physical Asset Management
データセキュリティ	情報資産の保護	DS データセキュリティ Data Security
ネットワークセキュリティ	インターネットからの不正アクセス	IP 不正アクセス対策 Illegal Access Prevention
	組織内LANの不正利用	SL セキュアLAN Secure Local Area Network
	モバイル環境での脅威	MS モバイルセキュリティ Mobile Security
	マルウェア汚染	PB マルウェア汚染対策 Pollution Block
セキュリティ管理	内部不正・証跡不備	LM 証跡管理 Log Management
	脆弱性攻撃	IC IT基盤保全 IT Infrastructure Conservation Management
	インシデント対応不備	IR インシデント対応 Incident Response
サービス	セキュリティ診断運用・監視	SS セキュリティサービス Security Service

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、インターネットの活用へと発展してきました。また、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。一方、セキュリティ面を含むシステムのTCO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、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多数の業務システム群に対するユーザID管理
③不正利用を防止する厳格な認証
④システム全体の安全性を管理する統合運用管理
⑤利用者の正当性を担保する証跡管理
⑥執拗な攻撃に対する多層防御
⑦セキュリティの専門家による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などで構成されます。

②多数の業務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不正利用を防止する厳格な認証

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システム全体の安全性を管理する統合運用管理

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利用者の正当性を担保する証跡管理

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/LM（Log Management）があります。

⑥執拗な攻撃に対する多層防御

標的型攻撃の最終ターゲットとなる情報資産への対策として、異なるアーキテクチャを組み合わせたサイバー攻撃防御ソリューションであるSecureplaza/IP（Illegal Access Prevention）、Secureplaza/SL（Secure Local Area Network）があります。

⑦セキュリティの専門家による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/SS（Security Service）があります。

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。

●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、54カ国250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。

- 経済産業省 制御システムセキュリティ検討タスクフォース
- 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
- 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（2012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

愛宕産業株式会社
株式会社 エー・シー・エス
FSテクノサービス株式会社
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
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 四国日立システムズ
株式会社 DACS
株式会社 中国日立システムズ
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
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
日立健康保険組合
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 日立システム九州
株式会社 日立システムズ
日立システムズテクノサービス株式会社
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
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デザイン
株式会社 日立ソリューションズバリュー
株式会社 日立中国ソリューションズ
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
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 日立ブレーン
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 北海道日立システムズ
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（2012年4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（情報システム事業部 全国情報ネットワーク本部 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 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

アラクサラネットワークス株式会社
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）
日立SC株式会社（本社）
株式会社 日立ケーイーシステムズ（東京開発センタ）
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 日立国際電気サービス（サービス本部）
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（SHIELD セキュリティセンタ）
株式会社 日立システムズ（中国支社 岡山支店）
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（秋田・仙台センタ）
株式会社 日立システムズエンジニアリングアンドソリューション
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）
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

第三者評価・認証

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（2012年5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
HiRDB Server Version 9（Linux版）09-01	データベース管理システム	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	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 Command Suite Common Component 7.0.1-00	基盤モジュールソフトウェア	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 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	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	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
Finger Vein Authentication Device UBReader2 Hardware: D, Software: 03-00	生体認証装置	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EAL7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（2012年3月末日現在）。

製　品	認証取得レベル
HIBUN Cryptographic Module for User-Mode 1.0 Rev.2	レベル1（注1）
HIBUN Cryptographic Module for Kernel-Mode 1.0 Rev.2	レベル1（注1）
HIBUN Cryptographic Module for Pro-boot 1.0 Rev.2	レベル1（注1）
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

注1. この暗号モジュールは、IPAと米国NISTとの合意に基づく共同認証を取得。米国NISTとカナダCSEが運用するCMVP（Cryptographic Module Validation Program）の認証も同時に取得しています。

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（2012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

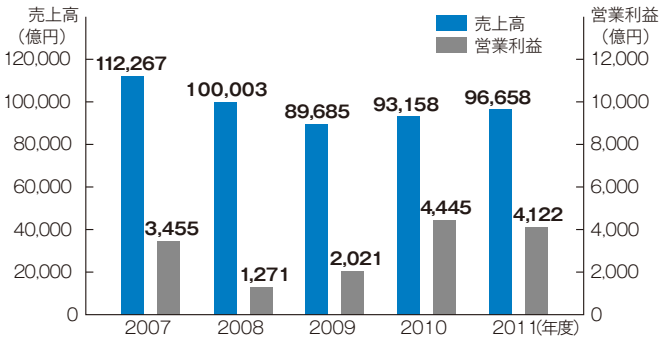
会社概要 (2012年3月末日現在)

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	427,775百万円
従業員数	(個別)32,908名 (連結)323,540名
連結子会社数	939社(国内340社、海外599社) (含む、変動持分事業体)
持分法適用関連会社数	183社(国内78社、海外105社)

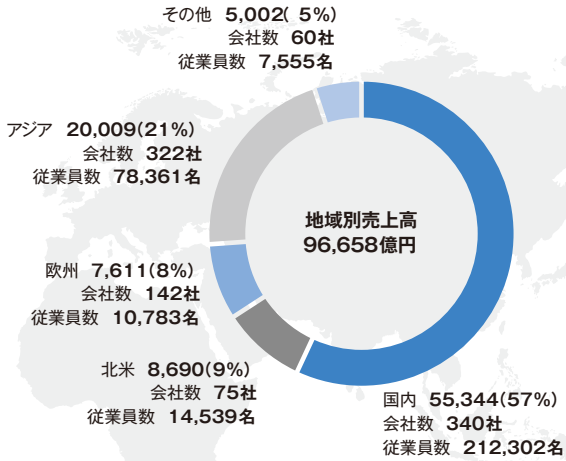
事業概要と業績 (2012年3月期)(連結)

売　上　高	96,658億円(前期比104%)
営業利益	4,122億円(前期比93%)
設備投資額	6,492億円(前期比117%)
研究開発費	4,125億円(前期比104%)
連結売上高に占める海外生産高比率	26%

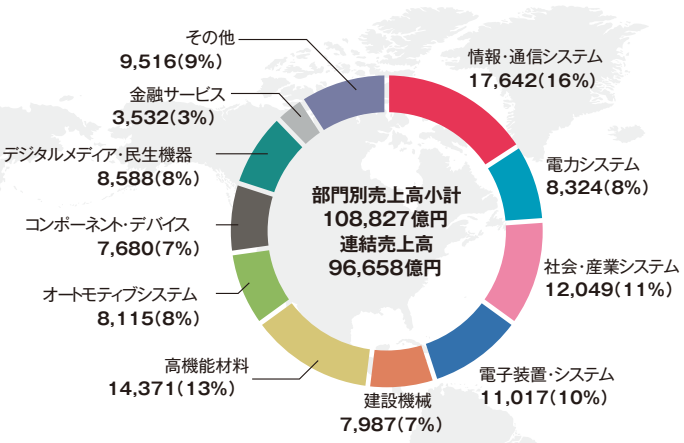
●売上高および営業利益推移



●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

Printed in Japan (H) (2012.00)