日立グループのセキュリティソリューションへの取り組み

Hitachi's Latest Security Solutions

田村 祐二 Yuji Tamura　　増田 亮太 Ryota Masuda

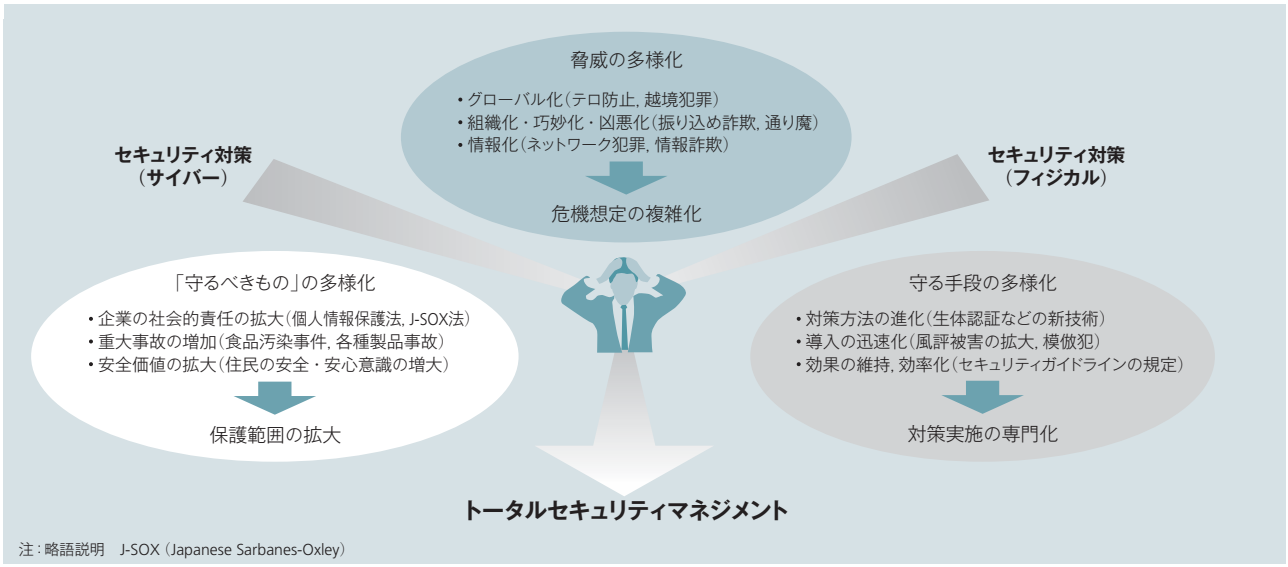


図1　セキュリティをめぐる動向
技術の進展，対応すべき事項の増加などにより，被害をもたらす脅威の内容，守るべき対象の範囲，守る手段の選択肢が増え，従来にも増して，フィジカルとサイバーのバランスをとったトータルセキュリティマネジメントが求められている。

セキュリティをめぐる動向

近年，テロや越境犯罪に見られる犯罪のグローバル化や，いわゆる「振り込め詐欺」などの巧妙で組織化された犯罪が増える[1)]など，日々新たな脅威が発生していると考えられる。また，通り魔事件のような，従来にない突発的な被害も多くなっている。企業活動においては，**個人情報保護法**[(a)]や**J-SOX法**[(b)]に見られる企業責任の拡大や，企業事故発生時における情報公開の迅速化，風評被害対策など，物的（フィジカル）および情報（サイバー）セキュリティ対策が，ますます重要となっている。そのため，発電所や空港・鉄道などの重要施設・社会インフラにおける対策はもとより，工場・事業者やオフィスなど企業におけるセキュリティ対策も重要性が高まっている（**図1**参照）。

脅威の多様化

インターネットを通じたグローバルな取引は，個人・企業とも増加の一途をたどり，十数年前に比べると，現在は誰でも，どこでも，簡単に売買ができる状況となっている。また，電子マネーやIC（Integrated Circuit）カード乗車券などの普及により，現金を持ち歩くことなく快適に生活できる社会が実現しつつある。

このような情報通信技術の進展は，便利な一方でクレジットカード番号や口座番号などの個人情報を盗み出す「フィッシング」など，ネットワーク犯罪や情報詐欺といった新たな犯罪の機会をつくり出している[2)]。こうしたことが犯罪のグローバル化と相まって，見知らぬ人間が悪意を持って近づく機会をつくっている。

このように，快適さの一方で従来にない新たな脅威が発生していることから，企業に求められるセキュリティ対策の危機想定は，ますます複雑化している。

(a) 個人情報保護法
一定数以上の個人情報（特定の個人を識別することができる情報）を扱う事業者を対象に，本人の了解なく個人情報の流用，売買，譲渡を規制する法律。2005年4月から施行された。個人情報について，利用目的を本人に明示すること，本人の了解を得て取得すること，常に正確な個人情報に保つこと，流出や盗難，紛失の防止に努めること，本人による閲覧，訂正，目的外利用の停止が可能であることを原則とし，個人情報の有用性に配慮しつつ，個人の権利利益を保護することを目的としている。

(b) J-SOX法
日本版SOX法とも言う。米国の企業改革法であるSOX（Sarbanes-Oxley）法にならって設けられた法制度で，「金融商品取引法」の内部統制に関する規定部分を指し，上場企業とその関連会社に，内部統制の整備や公認会計士による監査を義務づけている。米国版と比べ，ITによる内部統制の重要性が強調されているのが日本版の特徴である。

「守るべきもの」の多様化

大規模な個人情報流出事故が続出したことを受けて，2005年に個人情報保護法が施行され，個人情報に関するセキュリティが厳しく問われるようになった。その後J-SOX法が2007年に施行されたことにより，内部統制の構築と，その有効性の評価が義務づけられ，企業活動全般にわたってのIT統制のあり方が問われている。

また，食品汚染事件や各種製品事故などに見られるように，情報公開の重要性もますます高まり，対応の迅速性がいっそう求められている。そのため，企業がセキュリティ対策を行って保護すべき対象（守るべきもの）も，人命・人権・財産など人に直接かかわるものに加えて，企業活動の情報そのものへと範囲が拡大している。

生活者個々人の感覚としても，事件報道などを通じて安全・安心への意識が高まっており，社会の不安を払拭（ふっしょく）するため，セキュリティ対策の必要性がますます高まってきている。

守る手段の多様化

セキュリティ対策は，大別してフィジカル対策とサイバー対策があり，「守るべきもの」の価値に合わせた費用対効果の検証や，対策を必要とする時期や導入する規模に合わせた段階的導入など，セキュリティ計画を総合的に立案・実施しなければならない。

また，導入後に実施する対策の修正・効率化見直しなど，セキュリティ対策の知識と経験は専門化してきている。そのため，トータルセキュリティマネジメントを適切に，また効率よく実現する方法は，ますます難しくなってきており，先進事例を基にした最新技術の適用や多様なシステムの経験者による設計の実施など，従来にも増して専門家チームの設立が必要となっている。

日立グループが考えるセキュリティ対策

セキュリティ設計・実施の流れ

情報セキュリティの分野では，評価基準の標準規格**ISO/IEC15408**[c]が制定されている。トータルセキュリティマネジメントの構築においても，脅威の想定や保護する対象の設定，対策方針の立案など，全体運用の設計手順は，そのセキュリティ設計仕様書（ST：Security Target）を策定する流れを参考とすることができる。フィジカルやサイバーに限らず，一般的にセキュリティ対策の設計，実施は**図2**の手順で行われており，日立グループもこの手順で行っている。

対象設定プロセスでは，「守るべきもの」や脅威の多様化により，事象発生時の影響度もさまざまであるため，その影響の度合い，実現の可能性を考慮して保護対象を設定する。

また，対策立案プロセスでは，守る手段の選定，組み合わせ（機能要件，保証要件の選択と具体化）を検討し，その仕様をまとめ，セキュリティ対策の全体運用の方法を決定する。

企業活動では，関係する環境の変化が常に発生している。そのため，運用プロセスでは，定期的な監査の実施や，変更した対

(c) ISO/IEC15408
ITセキュリティ評価基準の国際規格であり，ITセキュリティ製品およびシステムの開発・製造・運用に関するセキュリティ保証レベルを評価，格付けする国際基準。情報システムの安全性を統一基準の下で評価可能にすることを目的に策定された。ITSEC（Information Technology Security Evaluation Criteria）やCC（Common Criteria）もITセキュリティの評価基準を示す名称としては同義で扱われる。

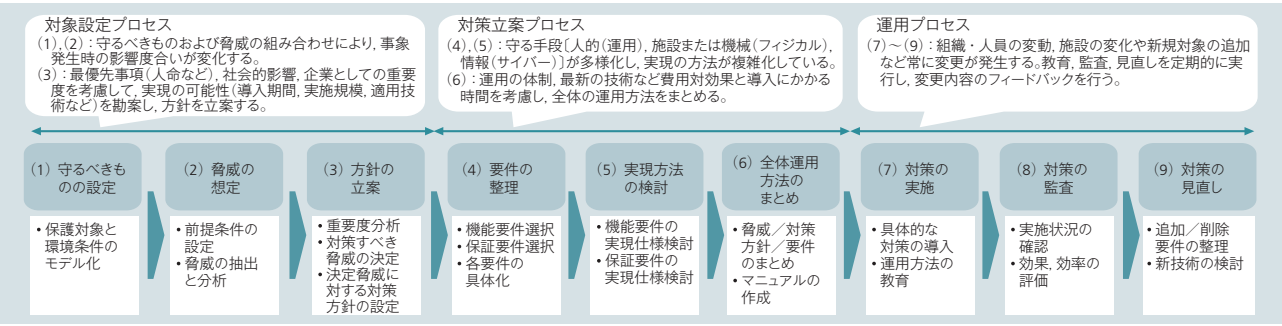


図2　一般的なセキュリティ設計・実施の流れ
守るべきもの，脅威，守る手段の多様化により，効果的で効率的なセキュリティ対策の設計が難しくなっている。

策の運用教育を行い，セキュリティ対策を最新状況に保つことで，確実な効果が期待できる。

オフィスにおけるセキュリティの実現事例

効果的でかつ効率的なセキュリティ対策を実現するには，サイバー要素と，フィジカル要素を融合させた「トータルセキュリティ」を構築することが重要である。日立グループの考えるオフィスにおけるトータルセキュリティの実現事例を**図3**に示す。

オフィスにおける「守るべきもの」は，財務，人事など会社の経営にかかわる企業情報や，製品の仕様などの製品情報，納入実績などの顧客情報，従業員・顧客の個人情報といった情報資産が中心となる。これらは執務室の書類や電子媒体，計算機室に電子データとして存在しており，情報セキュリティ管理の対象となる。

「脅威」は，従業員による自宅や取引先への情報持ち出し時に起こる(1)「紛失，盗難」や，ネットワーク経由でのハッカーやウイルスの(2)「侵入」，外注業者や顧客になりすましてオフィスへ直接入り込む(3)「侵入者」によって起こされる情報資産の改ざん，消去，不正持ち出しなどの(4)「不正アクセス」などが挙げられる。近年では「不正アクセス」はハッカーや侵入者によるものだけでなく，悪意を持った従業員による内部犯行も懸念され，重大な「脅威」と認識されつつある。

これらの「脅威」から情報資産を守るためには，人間の行動をサイバー，フィジカル両面で管理する必要がある。日立グループはユーザーIDをキーに，利用者のサイバー，フィジカルの利用権限と行動履歴をトータルで管理することでこの課題に対応している。さらに指静脈による個人認証や監視カメラを組み合わせることで，他者のなりすましや共連れを防止し，より強固なトータルセキュリティを実現している。対策の詳細を以下に示す。

(1) 持ち出しとそれに伴う紛失，盗難

「情報資産を持ち出さない」という対策が有効となるが，業務上著しく効率が低下する可能性がある。そのため日立グループはHDD（Hard Disk Drive）を持たないセキュリティPCを開発し，外部からセキュアに情報資産へアクセスすることで紛失，盗難の防止を図りつつ効率的な業務を実現した。

また，やむをえず情報資産を外部へ持ち出す場合には，暗号化技術を用いることで，紛失，盗難時の被害を最小限とすることが可能である。

(2) ウイルス，ハッカーの侵入

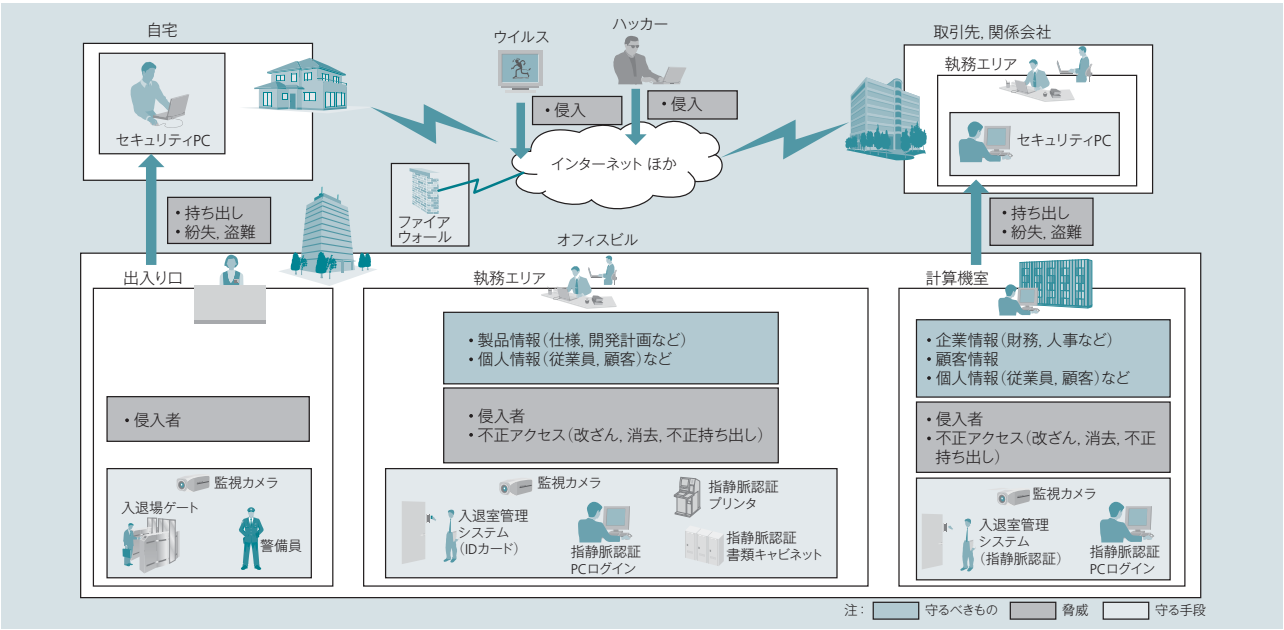
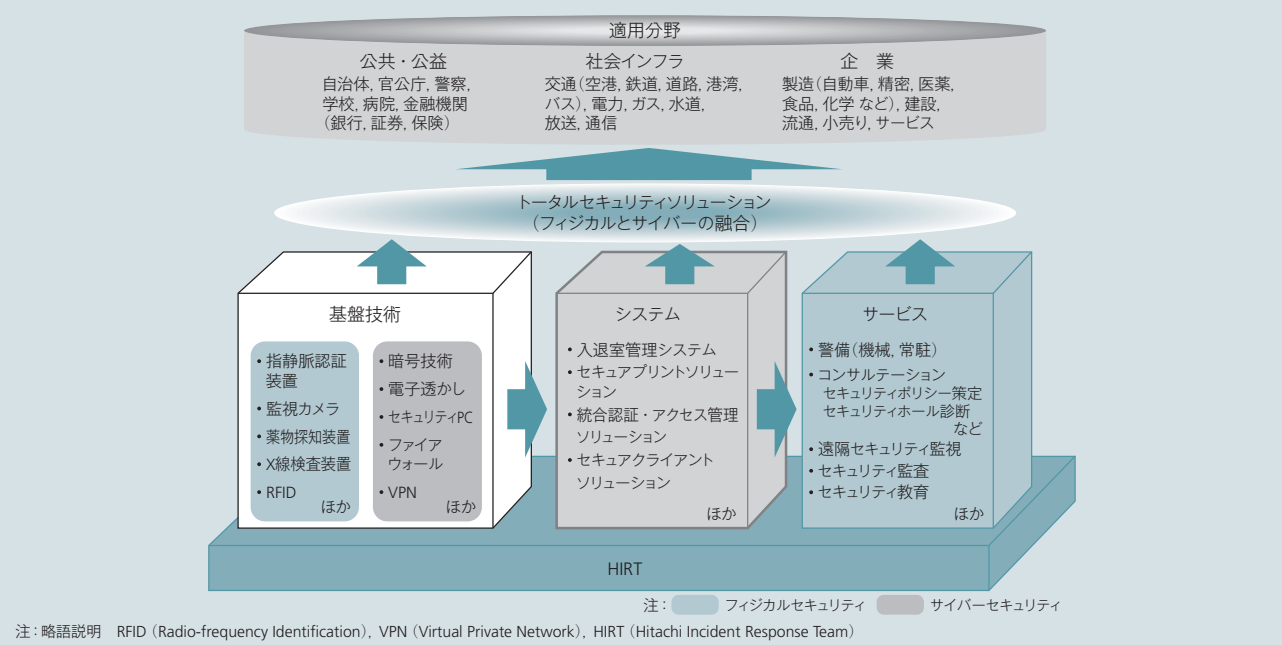


図3　オフィスにおけるトータルセキュリティソリューションの構築事例
フィジカルセキュリティとサイバーセキュリティを融合させることで，オフィスを取り巻くさまざまな脅威から守ることが可能となる。



注：略語説明　RFID（Radio-frequency Identification），VPN（Virtual Private Network），HIRT（Hitachi Incident Response Team）

図4　日立グループのセキュリティソリューション全体像
日立グループは，フィジカルとサイバーを融合したトータルセキュリティソリューションに注力しており，社会インフラ，公共・公益，企業各社の幅広いセキュリティニーズに応えている。

重要施設においては，完全に外部から遮断することで情報を守ることも行われている。しかし，一般的な企業では顧客や関係会社との情報交換にはインターネット網を利用することが前提であるため，ファイアウォールの設置や，アンチウイルスソフトウェアにより対策を行う。

(3) 侵入者

重要施設などテロ対策が求められる場所では，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により対策を行う。一方，一般的な企業では効率的な運用を目的に，IDカードで開く入退場ゲートや入退室管理システムで，侵入者を抑制する。また，重要な情報を扱う計算機室の入り口では，**指静脈認証**[d]装置による確実な個人認証を行うことで他人のIDカードでのなりすまし侵入を防止している。

しかし，IDカードを持った人が開けた扉から続けて入る「共連れ」を防ぐことは困難なので，監視カメラや無線タグにより，不携帯者・不許可者の侵入を検知するハンズフリーセキュリティシステムも併用する。

(4) 不正アクセス

情報資産の改ざん，消去への対策は，指静脈認証による確実な個人認証により，権限のない他者のなりすまし防止を実現している。また，プリンタや書類を保管するキャビネットを指静脈認証機能付きのものにすることで，不正な持ち出しを防止できる。

さらに，悪意を持った従業員へは，情報資産への来歴管理や**電子透かし**[e]を導入することで，迅速な事故対応が可能となるため，犯行の抑止効果が期待できる。

日立グループの取り組み

前章では，オフィスにおける日立グループのセキュリティソリューションの適用事例を述べたが，「守るべきもの」，「脅威」，「事象発生時の影響度」は企業により異なる。セキュリティシステムの設計，実施の手順を前述したが，この検討には，セキュリティ対策に関する幅広い経験と専門知識が必要である。また，システム導入後も，対策の見直し，社員の教育など種々の施策を講ずる必要があり，セキュリティシステムの導入・運用は一般企業にとって大きな負担となっている。

日立グループは，このような課題を解決するため，自社および多くの顧客で構築・運用したセキュリティシステムのノウハウを活用し，トータルセキュリティソリューションを立ち上げた。本ソリューションの全体像を**図4**に示す。システム導入時のサービスとしてはセキュリティポリシーの

(d) 指静脈認証
近赤外線を指に透過させて得られる指の静脈パターンの画像によって個人認証を行う技術。指画像から静脈の存在する部分を人工知能手法で鮮明な構造パターンとして検出し，あらかじめ登録した静脈の構造パターンとマッチングさせて個人認識を行う。生体内の静脈パターンを認証するため，かすれや乾燥肌による影響を受けず，偽造もきわめて困難であることから，高精度な認証が可能である。

(e) 電子透かし
文書や画像，音声などの電子データに，著作権者の名前やデータ作成日などの特定の情報を埋め込む技術。埋め込んだ情報を専用のソフトウェアで検出することで，不正コピーによる著作権侵害や改ざんを判別できる。

策定やリスク分析，個人情報保護法対策などの多くのコンサルティング業務を提供している。また運用時には一般社員から専門技術者までの幅広い人材を対象とした教育研修や，エレベーターなどのビル施設の遠隔監視，警備員を派遣する常駐警備など多様なセキュリティサービスを提供している。

このように，基盤技術から対策の実施計画，構築段階におけるシステム提供，運用サービスに至るトータルセキュリティソリューションを提供することで，社会インフラ，公共・公益，企業各社など幅広い顧客のニーズに対応している。

また，日立グループが提供する製品・サービスの脆（ぜい）弱性対策とインシデント対応（発生している侵害行為の回避ならびに解決のための活動）を推進するため，「HIRT（Hitachi Incident Response Team）[3)]」を組織し，日立グループ製品の脆弱性を迅速に解決することで．顧客システムのセキュリティ向上に日々努めている。

今後のセキュリティシステムに向けた研究開発

現在，その利便性の高さから**クラウドコンピューティング**(f)に注目が集まっている。しかし利便性が高い反面，インターネット経由でサービスを利用することから，ビジネスへの適用にはセキュリティに課題があると指摘されている。これに対し，日立グループは次世代暗号技術やP2P（Peer to Peer）での情報漏洩（えい）対策技術を研究中で，クラウドコンピューティングの信頼性を，電力・交通などの社会インフラと同等にまで高めることをめざしている。また，従来のセキュリティ対策は「高セキュリティ」＝「煩わしさが増える」という傾向にあった。これに対し，利用者にはセキュリティ対策をしていることを感じさせず，監視する側には業務負担をかけない「人に優しい」セキュリティ技術の開発にも力を入れている。

例えば，防犯対策では，街中に監視カメラが設置されるようになってきているものの，膨大なカメラ映像の中から，犯罪や事故の発生を人の目で特定するのはきわめて困難である。これを解決すべく，100台の監視カメラの映像から人が写っていたり，人や物の動きのあったりするものだけを大画面で表示する広域ネットワークシステムを研究しており，「人に優しい」監視システムの実現をめざしている。

社会イノベーションへの貢献

科学技術の進展により，われわれは快適で便利な社会生活を手にすることができた。しかし科学技術の進展は同時に，今まで考えてもいなかった多くの脅威を生み出し，社会はその対策に悩まされ続けている。今後は社会インフラにも，より高い利便性や効率が求められるようになり，それに伴った新たな脅威が現れるものと思われる。

日立グループは，今後も社会インフラの「安全・安心」の実現に不可欠なセキュリティ技術やシステム，サービスを開発し，トータルセキュリティソリューションで社会イノベーションに貢献していく。

(f) クラウドコンピューティング
ITインフラやアプリケーション，データなどのIT資源を，インターネットなどのネットワークを通じてサービスとして利用可能にするコンピューティングの考え方，または利用環境を指す。「クラウド」は，システム構成図などでネットワークを表現する際に，しばしば雲（クラウド）のイメージが用いられることに由来する。

参考文献

1） 警察庁：振り込め詐欺被害発生状況・被害額，http://www.npa.go.jp/safetylife/seianki31/1_hurikome.files/Page386.htm
2） 警察庁：平成21年上半期のサイバー犯罪の検挙状況等について，http://www.npa.go.jp/cyber/statics/h21/pdf50.pdf
3） Hitachi Incident Response Team，http://www.hitachi.co.jp/hirt/about/

執筆者紹介

田村 祐二
1982年日立製作所入社，トータルソリューション事業部 公共・社会システム本部 社会システム部 所属
現在，電力，交通システムなどの社会インフラ事業向けトータルソリューションの開発に従事

増田 亮太
1991年日立製作所入社，トータルソリューション事業部 公共・社会システム本部 社会システム部 所属
現在，社会セキュリティ事業の取りまとめに従事