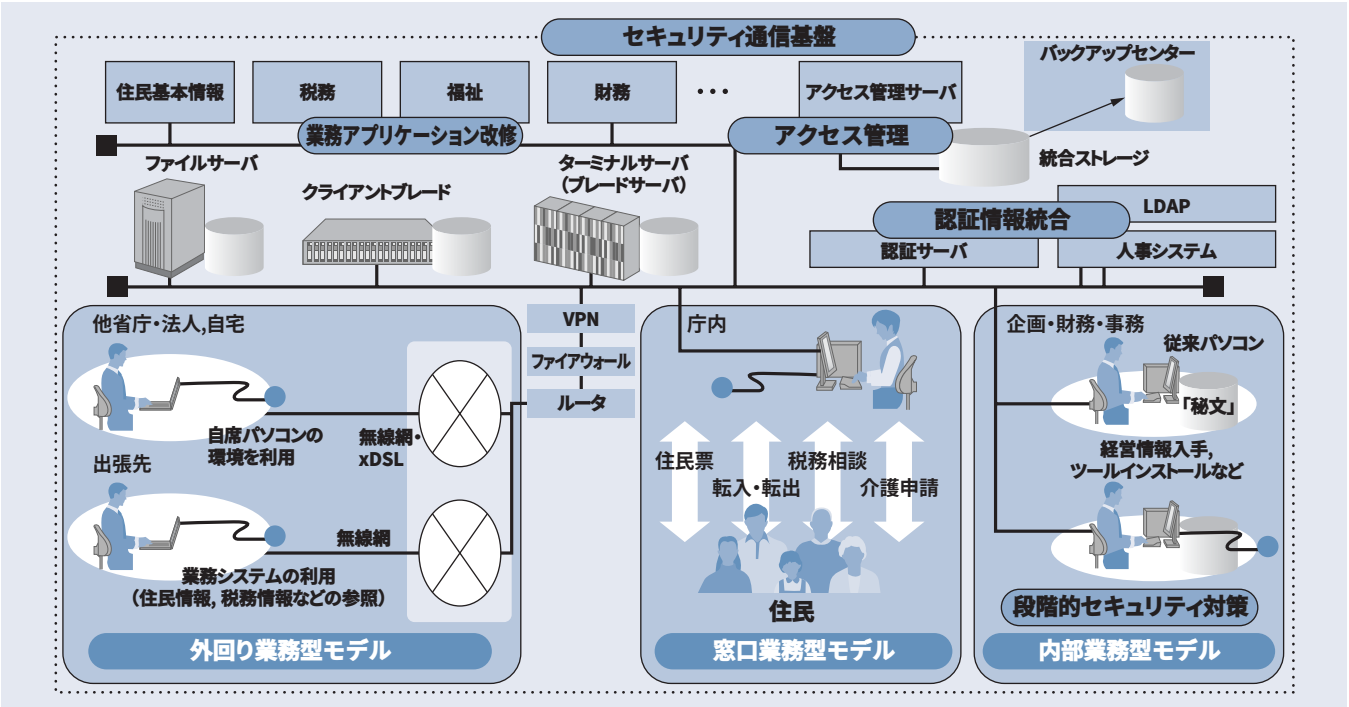
Vol.87 No.12

情報漏えい対策を強固にする「公共向けセキュアソリューション」

Ensuring Information Security for Public Institutions

■ 太田 慶一 *Keiichi Ôta*　■ 梅木 市朗 *Ichirô Umeki*　■ 田中 雅子 *Masako Tanaka*
■ 菊地 輝治 *Kôji Kikuchi*　■ 佐藤 衣子 *Maiko Satô*　■ 田島 主成 *Kazunari Tajima*



注:略語説明　LDAP(Lightweight Directory Access Protocol), VPN(Virtual Private Network), xDSL(Generic Digital Subscriber Line)

公共向けセキュアソリューションが提供する「業務別セキュリティ対策モデル」の適用イメージ

「外回り業務」,「窓口業務」, および「内部業務」を業務モデルとし, これらの構築支援サービスとして「業務アプリケーションの改修」,「セキュリティ通信基盤の構築」,「アクセス管理」,「認証情報の統合」,「段階的セキュリティ対策」の五つを組み合わせて提供する。

高度情報化社会が進展する中で, 近年, 情報漏えい防止, 文書の原本性や真正性の保証, 証拠保全といった観点から, 強固な情報セキュリティ対策が求められている。

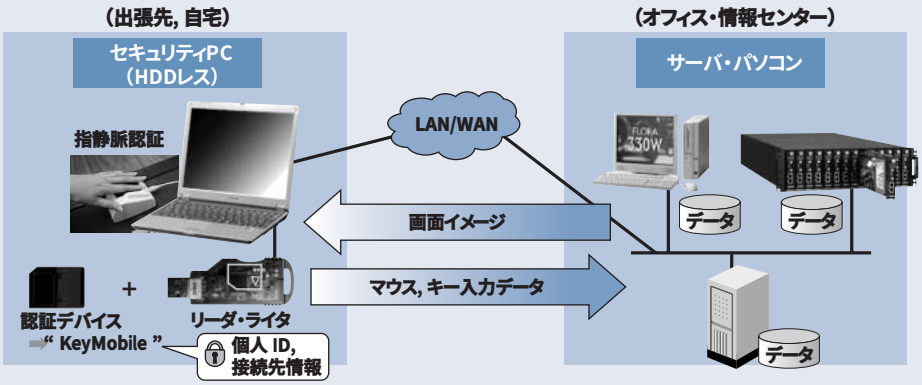
日立製作所は, セキュアな情報システムの構築を容易にするため,「セキュリティPC」や「指静脈認証」などを用いて, 官公庁や自治体向けの業務別セキュリティ対策モデルを提案する「公共向けセキュアソリューション」を提供している。これにより, 公共分野の各種業務に求められる, 住民・企業の個人情報や機密情報などの漏えい防止対策を迅速に実現する。

さらに, 公共分野向けに特化したセキュリティに関するコンサルティングからシステム構築, 運用・監視までを支援している。

1 はじめに

2005年4月の個人情報保護法の全面施行により, 個人情報を守ることへの関心とともに, 各種業務情報が保存, 蓄積された情報システムの安全対策へのニーズも高まっている。特に, 情報漏えい問題は, 民間企業や公共分野で組織活動に多大な影響を与えることなどにより, 当面の課題として最も注目を集めている分野の一つである。情報漏えいが発生しやすい場面を考えてみると, 主な原因としては, USBメモリ, CD-ROMなどの可搬記録媒体, さらにパソコンそのものの盗難・紛失があげられる。

官公庁・自治体・医療・教育機関などの公共分野で扱われている情報は, 国の機密情報, 住民情報や入札情報などの重要情報であるため, いったん情報が漏えいすると, 損害賠償の発生もさることながら, 情報の悪用や国民からの信頼の失墜など, 民間企業に比べてその影



注：略語説明　HDD（Hard Disc Drive），LAN（Local Area Network），WAN（Wide Area Network），ID（Identification）

図1｜**「セキュリティPC」の利用イメージ**
いつでも，どこでも自席パソコンを利用できる「利便性」を損なわず，セキュリティを強化して安心して利用できる安全な環境を実現する。

響は計り知れないものと考えられる。

ここでは，公共分野が扱う重要情報を漏えいなどのリスクから守る「公共向けセキュアソリューション」と，情報漏えい対策を実現するための具体的な業務への適用について述べる。

2 情報漏えいに対する日立製作所の取り組み

2.1 求められる公共分野のセキュリティ対策

従来のセキュリティ対策は，データをいかに漏えいさせないかなど，防御することを中心に実施されてきた。

例えば，情報がデータベースから抜き出された場合に，抜き出されたデータベースにふたを閉めることで対策するなどである。これからは，このような対処療法的な対策ではなく，情報にかかわる信頼・安心を損なうリスクをいかに管理するかに主眼を置く必要がある。そのために，潜在リスクの低減や，将来のリスクを予測したうえでのリスクの回避，移転，保有といった対応が求められる。これらは「e-Japan戦略」でも推進されているように，安全・安心な対策をいかに強化するかを中心とする取り組みである。

特に，公共分野では国民から信頼されることが重要であり，セキュリティに対しても厳格な取り組みが期待，要求されている。しかし，公平さを厳しくチェックされる透明性とセキュリティ確保という相反する要件を満たすことは，公共分野の情報管理での一種のジレンマになっている。一方で，新分野への予算・人材が確保しにくいという事情もある。このようなさまざまなニーズや背景の下では，確実で安全なセキュリティ環境の構築が必要になってくる。そして，これらの対応によって情報の有効な活用が促進されるだけでなく，行政への信頼感，安心感が向上するという付加価値が期待できる。

日立製作所は，これまで，セキュリティ関連ソリューションとして「日立セキュリティソリューションSecureplaza（セキュアプラザ）」を提供している。この中で，「セキュリティPC」や「指静脈認証」などの製品・サービスをベースとし，公共分野での情報漏えい防止をはじめとした強固なセキュリティ対策を提供する「公共向けセキュアソリューション」を整備した。

2.2 「セキュリティPC」

日立製作所は，情報漏えい防止対策について，「事故は起きるかもしれない」という考えからではなく，「事故は必ず起こる」という立場で推進するアプローチを取っている。これを原点にして，業務データを保持しない「セキュリティPC」を開発した（**図1**参照）。「セキュリティPC」は，「情報を持つから漏えいする，持たなければ漏えいしない」というシンプルな開発コンセプトを基に，いつでも，どこでも自席のパソコンを利用できる利便性を確保したうえでセキュリティを強化し，安心して利用できる環境を実現したハードディスクレスのパソコンである。

「セキュリティPC」は，情報漏えいを防止するためにハードディスクレスであるだけでなく，USBメモリやCD-ROMなど可搬記録媒体の接続や紙への印刷を抑止する。また，他のシンクライアント製品とは異なり，認証デバイズ“ KeyMobile ”を装着しなければパソコンの起動やネットワークの接続ができない仕組みとしており，高度なセキュリティ環境を実現している。さらに，「指静脈認証」を使った個人認証を追加することで，成り済まし防止に対するセキュリティレベルのいっそうの強化を提供している。

3 「公共向けセキュアソリューション」の概要

「公共向けセキュアソリューション」は，これまで日立製作所が提供してきた情報システムのセキュリティ対策ソリューション群に，公共分野での業務システム構築ノウハ

ウを加えて，官公庁や自治体など公共分野向けに特化し，セキュリティに関するコンサルティングからシステム構築，運用・監視までを体系化したものである。

今回は，システム設計・構築の迅速化を図るために，各種窓口業務向けや拠点を移動するような外回り業務向けなど，業務別に想定されるセキュリティ対策を実現するハードウェア・ソフトウェア・サービスを組み合わせてパッケージ化した「業務別セキュリティ対策モデル」を新たに開発した。さらに，ユーザー認証情報の統合管理や，既存の業務アプリケーションの修正，段階的なセキュリティ対策の導入などを支援する「セキュアプラットフォーム構築支援サービス」や，システムの安定稼動を維持する「運用・監視支援サービス」も提供する。

3.1 「業務別セキュリティ対策モデル」

「業務別セキュリティ対策モデル」は，官公庁や自治体の業務ごとに想定されるセキュリティリスクについて，日立製作所が考える標準的なセキュリティ対策としてハードウェア・ソフトウェア・サービスを組み合わせてパッケージ化したものである。

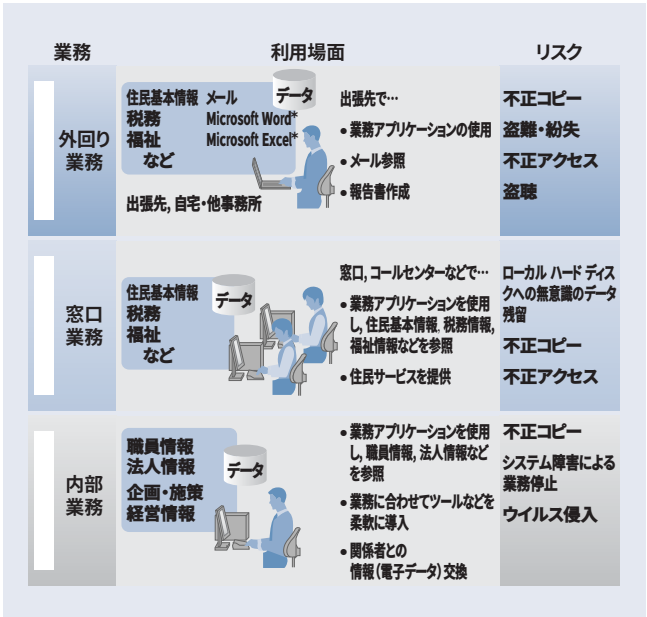
モデルは，住民・企業からの申請窓口，コールセンターや各種相談業務などの定型的な業務に対応する「窓口業務型モデル」，企画書・りん議書の作成などOA用のソフトウェアを使った非定型な業務に対応する「内部業務型モデル」，および出張相談所や外出先での報告書作成など出張先のモバイル環境での業務に対応する「外回り業務型モデル」の三つがあり，公共分野のニーズや既存の業務システムに合わせてカスタマイズし，提供していく(図2参照)。3モデルの特徴は以下のとおりである。

(1)「窓口業務型モデル」

個人情報のやり取りの場である申請窓口でのセキュリティ強化を支援する。窓口で「セキュリティPC」を利用することにより，データの残留を防ぎ，さらに安心な窓口業務環境を提供する。担当者の離席時には画面がロックされ，「のぞき見」ができなくなるなどの機能も備えている(図3参照)。

(2)「内部業務型モデル」

作成した企画書，りん議書などの不正コピーやウイルス侵入など，庁内での危険防止対策を支援する。内部業務で「セキュリティPC」を利用することにより，個人所有



注:* Microsoft Word，Microsoft Excelは，米国Microsoft Corp.の商品名称である。

図2 セキュアソリューションの利用場面とリスク
各業務(外回り・窓口・内部)でのソリューションの利用場面と潜在するセキュリティリスクを示す。

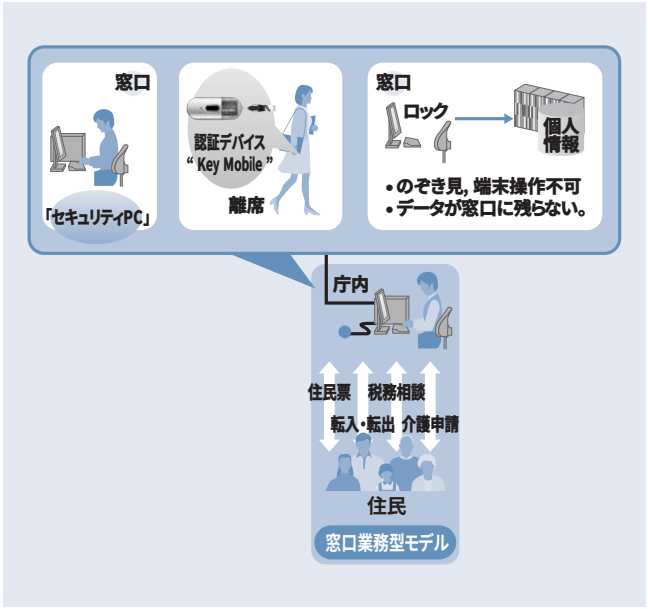


図3 「窓口業務型モデル」の適用イメージ
窓口業務への適用により，個人情報のやり取りの場である申請窓口でのセキュリティの強化を支援する。

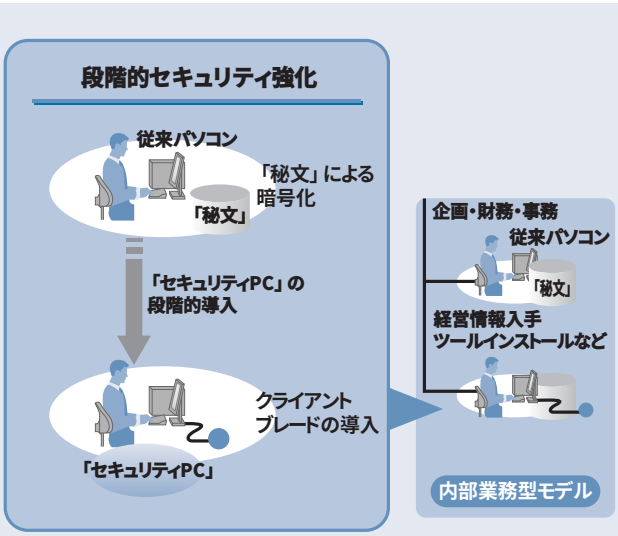
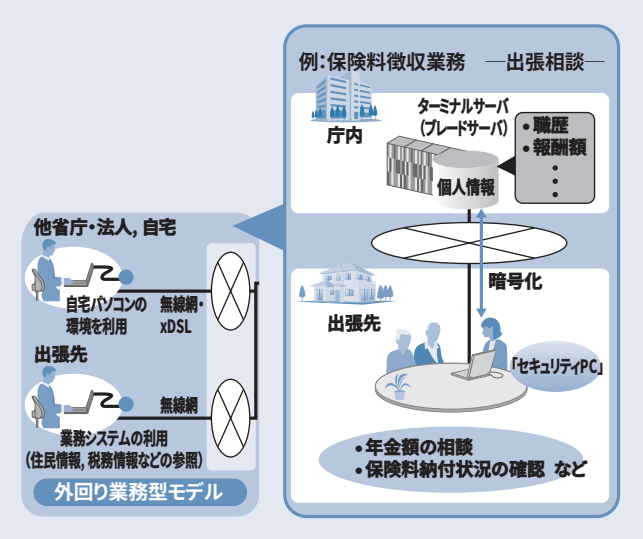


図4 「内部業務型モデル」の適用イメージ
内部業務への適用により，作成した企画書などの不正コピーやウイルス侵入など，庁内での危険防止対策を支援する。



注:略語説明　xDSL(Generic Digital Subscriber Line)

図5｜**「外回り業務型モデル」の適用イメージ**
出張相談所や外出先といった庁外で庁内と同等の業務が行える環境を提供し，盗難・紛失時の情報漏えいを防止する。

のデータや，企画書・統計情報などの基となる個人情報データ，内部機密データの残留・不正コピー・持ち出しが防止でき，庁内環境の安全性の向上が図れる(**図4**参照)。

(3)「外回り業務型モデル」

出張相談所や外出先といった庁外でも，庁内と同等の業務ができるセキュアな環境を提供する。庁外では，「セキュリティPC」を利用することにより，盗難・紛失が起こってもパソコンから情報が漏えいすることはないため，これまでセキュリティ上の問題で，実施に制限のあった庁外での業務が可能となり，出張先での業務報告や，個人情報を閲覧しながら相談業務を行うなど，住民サービスの向上や庁外業務の拡張化，効率化を図ることができる(**図5**参照)。

3.2　「セキュアプラットフォーム構築支援サービス」

「セキュアプラットフォーム構築支援サービス」は，公共分野の顧客の要望に合わせ，「業務別セキュリティ対策モデル」をさらにセキュアな環境にカスタマイズするための構築支援サービスである。

このサービスでは，以下のような，顧客の既存のインフラ環境・資産の有効活用や，さらに高度なセキュア環境の構築を実現する。

(1) アクセス管理機能構築支援

端末へのログインやログアウト，およびファイルへのアクセスログ(作成，削除，更新，参照)を収集し，自動的にチェックして，不正アクセスを監視する環境を提供する。

(2) 認証情報統合化支援

追加・削除・異動などで更新される人事システムのデータを基に，既存のLDAP(Lightweight Directory Access Protocol)と認証サーバとを連動させ，ユーザーのデータ登録の運用・管理を総合的にサポートする。これにより，ユーザーのシステムアクセス権限設定の省力化を図ることができる。

(3) セキュリティ通信基盤統合化支援

既存のネットワーク製品や業務アプリケーションなどに変更を加えることなく，ネットワーク上のすべてのデータに，高いセキュリティを確保するソフトウェア「セキュア通信基盤」を適用し，ユーザー認証，アクセス管理，および暗号化通信の機能を提供する。

このソリューションでは，従来の複数のネットワーク製品の組み合わせなどによって実現していたPKI(Public Key Infrastructure:公開鍵暗号)の電子認証技術や暗号化通信の機能を一つに結合しているため，セキュリティ情報の一元管理が可能となる。

(4) 業務アプリケーション改修支援

各クライアントにインストールされているクライアントアプリケーションを，ターミナルサーバで正常に動作させるための検証および改修を支援する。

(5) 段階的セキュリティ対策導入支援

庁内のすべてのパソコンをセキュア化していくうえでの導入方法として，既存のパソコンに対するローカル ハード ディスクや持ち出しメディアの暗号化，アクセス制御機能を備えたソフトウェア「秘文(ひぶん)」を適用し，順次，「セキュリティPC」を導入するなど，段階的なセキュリティ強化を支援する。

4　適 用 例

4.1　「窓口業務型モデル」の適用イメージ

「窓口業務型モデル」の事例として，自治体窓口での「複数業務を1台の端末で共有」，および「業務ごとに端末を専用化」している場合のそれぞれへの適用について以下に述べる(**図6**参照)。

4.1.1　複数業務を1台の端末で共有

窓口業務では，戸籍謄抄本の発行や住民票の発行など，複数の業務システムを1台で共有して使用する場合がある。このとき，複数の担当者で業務システムを並行して処理し，担当者以外が本来閲覧できない他の業務情報をのぞき見できたり，ローカル ハード ディスクへ無意識にログ情報が残留することなどにより，情報の入手が可能となる危険性が発生する。

このような危険性への対応策として，「セキュリティPC」を活用した「窓口業務型モデル」が有効である。

これまでの端末を「セキュリティPC」に代えることで可能になるのは，以下の2点である。

(1) パソコン使用時のアクセス権限認証により，接続可能な対象業務システムを限定して担当者以外からの業

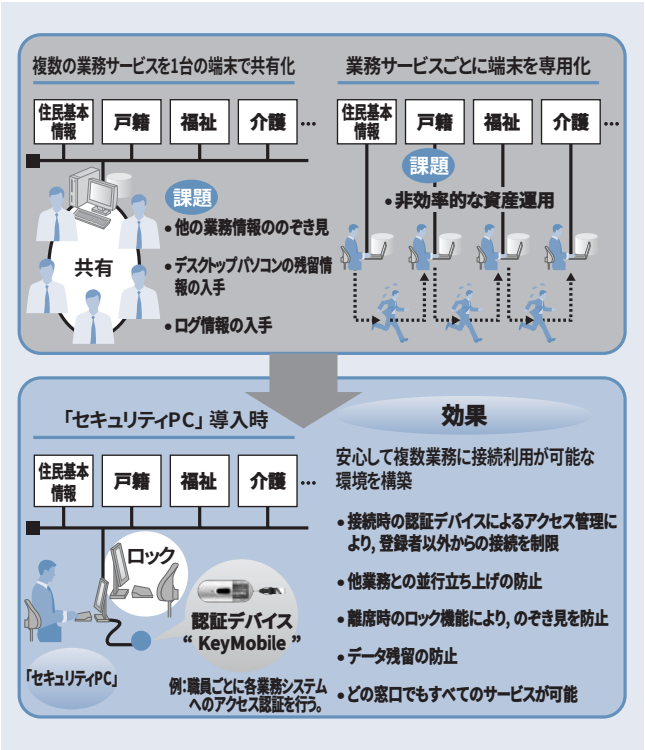


図6 「窓口業務型モデル」の適用効果
「セキュリティPC」を導入することにより，自治体窓口での課題に対応することができる。

務システムへの接続を防ぐ。

(2) 離席時には画面をロックする機能を備え，他者からのデータののぞき見・盗難を防ぐ。

このような接続方法や「セキュリティPC」の特徴を活用し，担当者以外からのデータののぞき見やデータの入手を防ぐことにより，個々の業務情報のセキュリティを確保し，複数業務を1台で安心して使用する環境ができる。

4.1.2 業務ごとで端末を専用化

業務システムごとに1台ずつ専用化する場合でも，「セキュリティPC」を活用した「窓口業務型モデル」は有効である。

しかし，業務システムごとに端末を区分するため，セキュリティ上の安全性はある程度確保されているものの，資産運用面では非効率的となってしまう。

そのため，業務システムごとに専用化している端末を1台の「セキュリティPC」へ集約することにより，窓口を固定しないで，どの窓口からでもすべての業務が行えるようにした。したがって，繁忙期などの業務量の変動に合わせた窓口対応もでき，住民サービスの向上につながる。

このように，複数の業務システムを共有しても，接続時のアクセス権限によって担当者以外の接続を防止することができ，専用端末の環境と同等のセキュリティで，運用面のコスト削減や資源の有効活用を図ることができる。

4.2 「外回り業務型モデル」の適用イメージ

自治体での税金・年金・福祉などの各種相談や，水道料・税金・統計・介護訪問などの調査，消防の予防業務などの外回り業務には，専用のハンディターミナルやPDA(Personal Digital Assistant:携帯情報端末)を利用しているものがある。しかし，現在の携帯端末には，ハードディスク容量の問題や，スタンドアロン機器として持つために検索機能に限界があること，個人情報などの機密情報を保持するにもかかわらず情報漏えいなどのセキュリティ対策が万全でないことなどの課題がある。また，業務アプリケーションとのリアルタイムの連動がなく，再度入力が必要となるなど，作業効率上の課題もある。

これらの課題に対応する，外回り業務での「セキュリティPC」利用の利点は以下のとおりである。

(1) 個人情報漏えいの防御

パソコン自体に情報を持たせないので，紛失・盗難の際も住民の個人情報は漏えいしない。

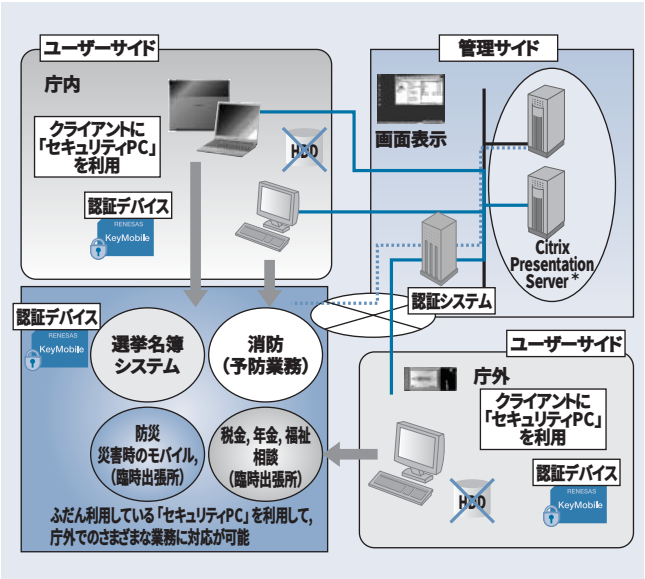
(2) 端末の兼用

“ KeyMobile ”により，同じパソコンで各作業者の環境がそれぞれ独立・安全に利用できるため，外出用のパソコンは利用人数分を必要としない。

(3) 作業内容の拡大

ブレードPCまたは普通のパソコンに接続するため，大容量のデータを扱うことができる。

このように，「セキュリティPC」の利用により，モバイル環境下で安心して重要な業務データを扱えるようになることから，作業の幅を広げることが可能となる。現在はモバイルPCの適用が困難な分野である自宅や支所での作業，出張や訪問先などの外回り業務で「セキュリティPC」の利用が可能になれば，作業効率やサービスの面で大きな効果が見込まれると考える。



注:*Citrix Presentation Serverは，米国Citrix Systems, Inc.の製品名称である。

図7 ふだんのパソコンの兼用利用例
ふだん利用している「セキュリティPC」を別業務に利用することが可能となる。

また，クライアントとなる端末を個人利用に特定する必要がなくなるため，ふだん利用している「セキュリティPC」を利用して，庁外でのさまざまな業務に対応することができるようになると考えられる（**図7**参照）。

5 今後の展開

5.1 セキュリティシステム開発環境マネジメント

システム開発プロジェクトでは，設計書やテストデータが開発者のパソコンから情報漏えいするリスクが想定される。これは，複数の開発会社でプロジェクトを組み，繁忙期には一時的に増員が必要となるシステム開発で情報漏えいのリスクが高いことを示している。

日立製作所は，自社の業務インフラ環境の整備はもとより，開発プロジェクトで使用するパソコンについても「セキュリティPC」を導入し，個々のパソコンへの情報保持を不可能として，データの盗難・紛失を防止するとともに，認証デバイスを用いたなりすましの防止，外部媒体へのコピー防止によって重要情報の漏えいに対してのリスク管理を実施していく。

開発プロジェクトでは，情報管理基準を明確にして個々の開発者に徹底させることは必須である。しかし，短期間での開発を要求される案件が多い現在，開発者への教育が行き届かない可能性がある。「セキュリティPC」を導入した開発プロジェクトでは，情報漏えいリスクをシステム的に管理できるため，顧客のシステムにかかわる重要情報や，データを確実に保護することができる。これにより，開発者や管理者への情報漏えいリスク管理にかかわる負荷を削減することができる。

日立製作所は，ここで述べた取り組みを含め，公共分野の顧客へ提供する各種製品やサービスにおいて，セキュリティの品質向上に努めたシステム開発によってセキュリティ上の欠陥（ぜい弱性）を発生させることなく品質を確保するとともに，規則やガイドライン，教育などの整備を進め，高いセキュリティレベルを実現する製品・サービスを提案していく考えである。

5.2 「公共向けセキュアソリューション」の方向性

「公共向けセキュアソリューション」では，セキュリティレベルの向上に加え，データのセンター集中化による運用面でのTCO（Total Cost of Ownership）の削減や，利用者へのサービスレベルの向上を実現する。今後は，「業務別セキュリティ対策モデル」のいっそうの拡充や，「セキュアプラットフォーム構築支援サービス」の詳細化を図るとともに，災害時のデータ資産のバックアップ，サービスの担保など，問題発生時の被害の極小化への対応なども含めた，安全・安心な環境，高効率な業務環境を実現するソリューションを提案していく。

6 おわりに

ここでは，情報漏えい対策を強固にする日立製作所の「公共向けセキュアソリューション」について述べた。

セキュリティについての関心は高まる一方である。しかし，対策には費用がかかり，導入することによって操作性や利便性を損なうこともあらかじめ考慮しなければならない。

日立製作所は，これからも，予算や利便性などを考慮し，バランスのよい適切なセキュリティ対策をソリューションとして提案していく考えである。

執筆者紹介

太田 慶一
1992年日立製作所入社，情報・通信グループ 公共システム事業部 公共セキュアソリューションビジネス推進センタ 所属
現在，公共セキュアビジネスの推進に従事
E-mail:keiichi.ohta.sw@hitachi.com

菊地 輝治
1993年日立製作所入社，情報・通信グループ 公共システム事業部 公共セキュアソリューションビジネス推進センタ 所属
現在，公共セキュアビジネスの推進に従事
E-mail:koji.kikuchi.kw@hitachi.com

梅木 市朗
1998年日立製作所入社，情報・通信グループ 公共システム事業部 公共セキュアソリューションビジネス推進センタ 所属
現在，公共セキュアビジネスの推進に従事
E-mail:ichiro.umeki.pk@hitachi.com

佐藤 衣子
2001年日立製作所入社，情報・通信グループ 公共システム事業部 電子自治体ソリューション統括部 所属
現在，公共セキュアビジネスの推進に従事
E-mail:maiko.sato.tw@hitachi.com

田中 雅子
2000年日立製作所入社，情報・通信グループ 公共システム事業部 官公システム企画統括部 所属
現在，公共セキュアビジネスの推進に従事
E-mail:masako.tanaka.zd@hitachi.com

田島 主成
1995年株式会社日立情報システムズ入社，公共システム本部 システムサービス部 所属
現在，公共セキュアビジネスの推進に従事
E-mail:k-tajima@hitachijoho.com