特集

# 富士通ソリューションスクエアにおけるセキュリティの取組み

## Security at FUJITSU SOLUTION SQUARE


**あらまし**

インターネットの普及に伴い，企業における情報セキュリティの重要性はますます高まっている。企業にとって重要な資産とも言える情報を外部から守るためには，しかるべきセキュリティ基盤の構築が必須である。富士通においても，セキュリティは重要なテーマであり，近年はこれがビジネスチャンスに結びつくことも多い。セキュリティビジネスにおいて，お客様から信頼されるためには，自社で情報セキュリティを実践し，実績を持つことが重要と言える。富士通では，新しい拠点である「富士通ソリューションスクエア」を，最新セキュリティの実践の場として位置付け，様々なセキュリティの取組みを行っている。

本稿では，この富士通ソリューションスクエアでの具体的な取組みについて紹介する。

まず，セキュリティポリシー，電子透かし技術の適用について述べた後，パソコンデータの暗号化，操作ログの収集，最後に個人およびネットワークの認証について述べる。

Abstract

Information security in companies has been growing in importance as Internet penetration continues to increase. To protect their information against outside attacks, companies must build a strong security foundation. Security is also a key theme at Fujitsu, and it has led us to various business opportunities over the years. We have gained customer confidence in our security business by building our own security foundation, maintaining the security of our information, and providing our customers with the results they require. We have established “FUJITSU SOLUTION SQUARE,” which is a new environment in which the most up-to-date security technology and various security approaches are practiced. This paper introduces the practical approaches we take at FUJITSU SOLUTION SQUARE. First, we describe the implementation of our Security Policy and digital-watermarking technology. Then, we present one of our customer’s observations about using our security services. Lastly, we describe the collection of an operation log and then conclude the paper.



**山本岩男（やまもと　いわお）**

fujitsu.com室SolutionNET推進部所属
現在，富士通ソリューションスクエアにおけるインフラの開発，整備に従事。

**門木久夫（かどき　ひさお）**

fujitsu.com室SolutionNET推進部所属
現在，富士通ソリューションスクエアにおけるインフラの開発，整備に従事。

**戸枝健司（とえだ　けんじ）**

fujitsu.com室SolutionNET推進部所属
現在，富士通ソリューションスクエアにおけるインフラの開発，整備に従事。

# 富士通ソリューションスクエアにおけるセキュリティの取組み

## ま え が き

インターネットの普及に伴い，企業における情報セキュリティの重要性はますます高まっている。インターネットを通じて，世界中の企業がネットワークで接続されている今日，企業にとって重要な資産と言える自社の情報を外部から守るためには，しかるべきセキュリティ基盤の構築が必須である。富士通がソフト・サービスでビジネスを展開する上でも，セキュリティは重要なテーマであり，近年はこれがビジネスチャンスに結びつくことも多い。セキュリティにおいて，お客様から信頼されるためには，自社で情報セキュリティを実践し，実績を持つことが重要と言える。富士通の新しい拠点である「富士通ソリューションスクエア」（東京都大田区蒲田，2003年11月開設）を，富士通の最新セキュリティの実践の場として位置付け，様々なセキュリティの取組みを行っている。

本稿では，この富士通ソリューションスクエアでの具体的なセキュリティの取組みについて紹介する。

## セキュリティポリシー

セキュリティレベルを高める上で，一番重要なのは個人のモラルであり，セキュリティマインドである。これが欠如していては，いかに優れたセキュリティ技術を取り入れようとも，意味をなさなくなる。そこで，最初の取組みとして，富士通内における情報管理規定をもとに，セキュリティポリシー[(1),(2)]を二段階に大別することにより運用ベースで簡略化した。また，施策においては，最新技術を取り入れることで，その時点で最適なセキュリティを実現した。

本章では，以下の二つについて説明する。

（1） セキュリティポリシーの簡略化

（2） 最新技術適用

### ● セキュリティポリシーの簡略化

セキュリティポリシーは文書化された規約であり，作成しただけでは「絵に描いた餅」でしかない。これが正しく運用されることにより，セキュリティとして初めて意味を持つ。しかし，その内容が複雑なものになれば，各人の意識から外れることが多くなり，結果として守られないものとなってしまう。そのため，全員に確実に認識してもらい，規約を守ってもらうため，必要以上に施策を増やさず，できる限りシンプルにまとめることを心掛けた。例えば，企業内を流通する秘密情報に関して，富士通の情報管理規定では「他社秘密情報」「関係者外秘情報」「社外秘情報」などのように情報を細かく分類しているが，ここでは情報をその重要度に応じて二段階に分類し，それぞれにおいて守るべき規約を策定した（**図**-1）。

### ● 最新技術適用

前節で述べたとおり，セキュリティポリシーにおいて，セキュリティを確実なものにするためには，正しい運用を行うことが必然であり，それに加えて，最新セキュリティ技術の適用も重要な要因である。コンピュータやネットワーク技術の進化に伴い，我々のワークスタイルは大きく変化してきており，それに応じて，採るべきセキュリティ対策も変えていく必要がある。近年のネットワーク環境の進化に伴う，不正手口の複雑化や，不正アクセス手法の多様化に対応して，不正アクセス対策も総合的に高度化すべきであり，セキュリティポリシーにおける規定を作成する中で，最新セキュリティ技術を積極的に取り入れた。

## 電子透かし技術の適用

社内で取り扱う秘密情報において，最も重要性（機密性）の高い情報はお客様から預かった情報（以下，顧客情報）であり，細心の注意を払って取り扱う必要がある。従来，顧客情報などの重要情報の取り扱いに関しては，鍵付きロッカへの保管，情報管理責任者の許可による閲覧，記録簿による参照記録管理などの運用を行ってきたが，情報管理責任者の負担増大や，情報管理責任者が不在時の対応において課題を残していた。そこで，重要情報のセ

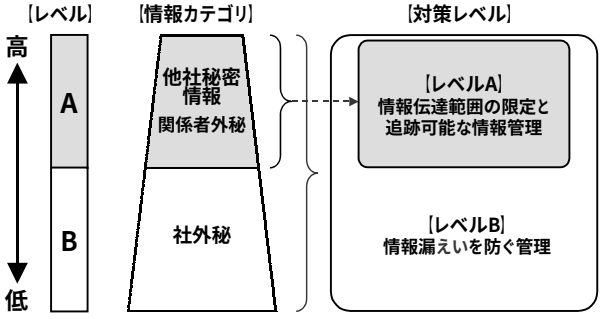


図-1 情報分類概念
Fig.1-Concept of information classification.

キュリティレベルを維持した上で，関係者内でタイムリに情報を共有するために，以下の施策を適用するものとした。

(1) 文書管理システムによる利用者制限および原情報の施錠管理
(2) 電子透かしの埋込み
(3) 利用者認証プリンタによる印刷

これらについて以下に説明する。

● **文書管理システムによる利用者制限および原情報の施錠管理**

文書管理システムへ情報登録することにより，関係者内でその情報を共有する。この情報登録時に情報へのアクセス権限設定が可能であり，アクセスを関係者のみに限定することができる。また，関係者以外からは，その情報の存在自体も知ることができない。これにより，重要情報のセキュリティレベルを維持し，かつ，タイムリな情報共有が可能となる。また，原情報は従来どおり，鍵付きロッカで保管する。鍵管理は情報管理責任者が行い，関係者以外が不正に閲覧するのを防止する。この情報が不要になった場合は，顧客へ返却するか，顧客承諾のもと，情報管理責任者が媒体破壊などにより，復元不可能状態にし，確実に破棄する。

● **電子透かしの埋込み**

デジタルデータは紙を媒体にした情報と異なり，複製や加工が容易であり，便利である反面，セキュリティ面や著作権保護といった面で不正が行われやすい。これを解決する技術として，電子透かしが挙げられる。一般的には，著作権保護目的でマルチメディアコンテンツ（音楽データや画像データなど）に用いられることが多い。保護したいデジタルデータに見えない形で著作権管理情報を埋め込み，それを必要時に検出可能とすることにより，不正を防止する技術である。

富士通ソリューションスクエアでは，電子透かしの対象をビジネス文書（重要情報）とし，電子透かしを「見える形」で埋め込む（**図**-2）。電子透かしを見える形で埋め込むことは，すなわち，原情報を見た目上，改変することを意味する。しかし，ビジネス文書においては，マルチメディアコンテンツと異なり，見た目上の違いは重要視されないことから，見える形で埋め込むことは問題にならない。実例を挙げると，文書の背景に“CONFIDENTIAL MATERIAL”など秘密情報である旨の表示に加え，その文書の登録日時，および登録者情報（登録者の所属，氏名），取得日時，取得者情報を埋め込む。これにより，利用者へ重要情報であることの意識付けを行い，安易にその情報をほかで再利用，配布することを防ぐ。

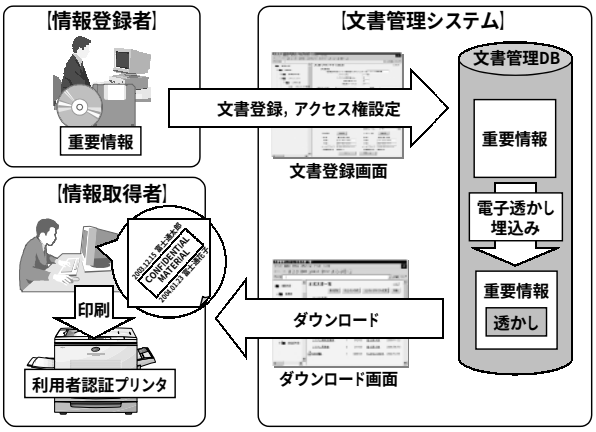


図-2 電子透かし利用イメージ
Fig.2-Example of digital-watermarking use.

● **利用者認証プリンタによる印刷**

情報の印刷において，印刷物がそのまま放置される場合がある。これは他者による不正持去りの危険にさらされることになり，とくに重要情報を印刷した場合は，この危険性を考慮する必要がある。従来は「印刷したらすぐに取りに行く」という運用を行ってきたが，この運用では徹底が難しく，完全なセキュリティは望めない。この対処として，重要情報の印刷は，利用者認証プリンタで行う（図-2）。利用者認証プリンタでは，印刷者がプリンタで認証することにより，印刷される。これにより，他者による不正な持去りを防ぐことできる。

## パソコンデータ暗号化と操作ログの収集

多くの企業でビジネスやコミュニケーションに不可欠なものとして使用されるモバイルパソコンには，企業の生命にかかわる極めて重要な情報までも格納される機会が増えている。ネットワークのセキュリティ対策のめまぐるしい進歩とは対照的に，パソコンの盗難・紛失により重要な情報が漏えいする事件や事故は急増し，社会的な問題となっている。これらの問題を解決する手段として，つぎのソフトウェアを適用した。

(1) 暗号化ソフトウェア適用
(2) パソコン操作ログ収集ソフトウェア適用

**● 暗号化ソフトウェア適用**

外部へ持ち出すモバイルパソコンに対し，データ暗号化ソフトウェアを導入した（**図**-3）。このソフトウェアを導入することにより，つぎの対処が可能となる。

(1) ブートプロテクション（起動防止）

モバイルパソコンの電源投入後，OS起動前にユーザ認証を行うことにより，他者によるパソコン起動を防止する。

(2) ハードディスクの完全暗号化

ハードディスク全体を完全に暗号化することにより，ハードディスクを取り出し，解析ツールなどを使用しても，ハードディスク内のデータへアクセスすることは不可能となる。

この二つの対処により，モバイルパソコンの紛失・盗難による情報漏えいを防ぐことができる。

**● パソコン操作ログ収集ソフトウェア適用**

重要な情報を扱うパソコンには操作ログ収集ソフトウェアを適用する（**図**-4）。これにより，そのパソコンにおける操作をログとして記録し，その操作ログをサーバで一括監視することが可能となる。ログでは情報の「印刷」「ファイルコピー」「ネットワーク送信」などの操作が記録されるため，外部への重要情報の流出を監視することが可能となる。また，このソフトウェアを導入することにより，不正への抑止力となることが期待できる。

## 個人認証およびネットワーク認証

本章では，個人認証およびネットワーク認証について，富士通ソリューションスクエアでの取組みを述べる。

**● PKI（Public Key Infrastructure：公開鍵基盤）による個人認証および電子署名，暗号化**

富士通では個人を認証する技術としてPKIを導入している。このPKIを利用することにより，ネットワークアクセスにおける「不正アクセス」「なりすまし」「改ざん」といった脅威を排除でき，セキュアなネットワークインフラを構築することが可能となる。また，e-JAPAN構想においても個人認証は重要な位置を占め，PKIはその中核技術として採用されており，今後の商談活動をサポートするためにも，社内実践を進めている。富士通におけるPKIでは個人の秘密鍵および公開鍵証明書をIDカードに埋め込まれているICチップ内に格納している。このIDカードをパソコンに接続したカードリーダに差し込んで，PIN（Personal Identification Number）を入力することにより，PKIを利用できる。以下に，このPKIの利用例を二つ取り上げて説明する。

(1) Web認証（シングルサインオン）

Webシステムにおける認証としては，従来，IDとパスワードの組を入力することにより認証する方式（基本認証）が一般的であり，その簡易性から現在も多くのWebシステムで用いられている。しかし，ID，パスワードのハッキング，盗聴による情報漏えいの危険性が高く，とくに重要な情報を扱う企業内の基幹システムなどでは，個人認証の強化が求められていた。そこで，PKIが持つ強力な個人認証を，Webシステムの認証へ適用することにより，高い信頼性を確保することができる。また，従来，Webシステムごとに個別のID，パスワードを管理する必

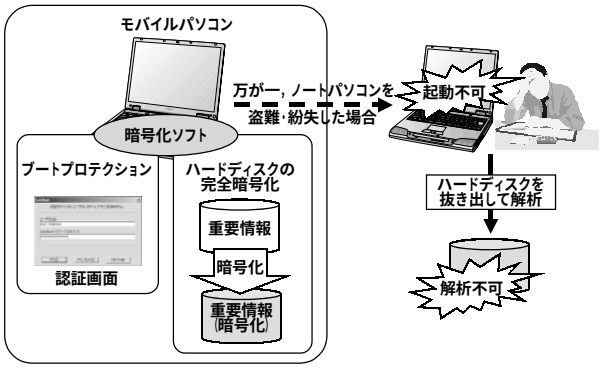


図-3 暗号化ソフトウェア利用イメージ
Fig.3-Example of encryption software use.

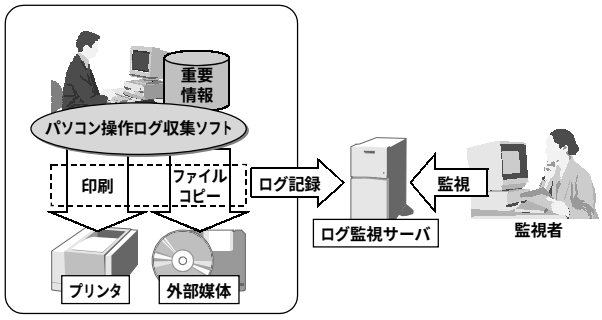


図-4 パソコン操作ログ収集イメージ
Fig.4-Example of personal computer operation logging.

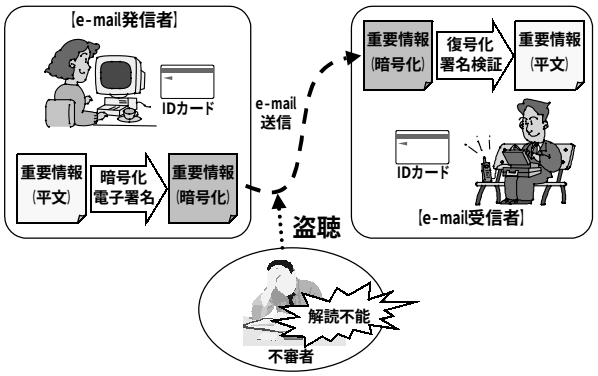


図-5　電子署名・暗号化メール利用イメージ
Fig.5-Example of electronic signature and encrypted e-mail use.

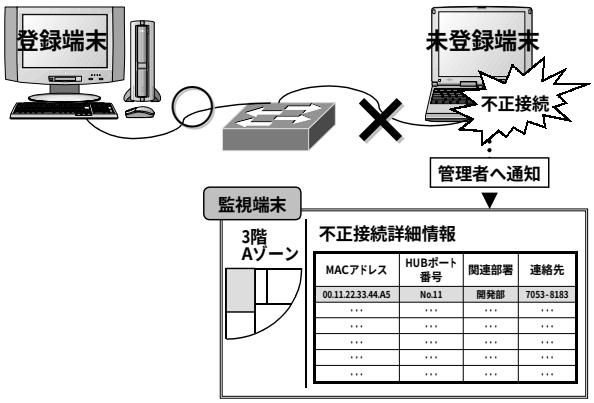


図-6　未登録端末の接続監視
Fig.6-Connection surveillance of unauthorized terminal.

要があったが，PKIで認証することにより，シングルサインオンが可能となる。これにより，一般利用者においては安全性と利便性が両立でき，システム管理者においては運用コストの削減につながる。

(2)　電子文書への署名，暗号化

企業の業務改善を図る上で，ネットワークを利用した情報（電子文書）の円滑な流通が重要であるが，前述したように，デジタルデータは改ざんが容易であり，受信データの正当性を証明する手段が求められていた。その解決として，紙文書で用いられている署名や押印を，電子的手段として持ち込んだのが，電子署名である（**図**-5）。この電子署名を行うことにより，その情報の責任所在が明らかになり，また，情報が改ざんされていないことを証明できる。また，このほかに電子メールの標準暗号化技術であるS/MIMEが利用でき，電子メールを暗号化して送信することにより，正当な受信者のみが，それを復号化できる（図-5）。これによって，従来，電子メールで不安視されていたネットワーク盗聴や，送信ミスによる関係者以外への情報漏えいが排除できる。

富士通では，PKIを次のような場合に適用している。

・重要情報をe-mail送信する場合の暗号化
・職制レポートなどをe-mail送信する場合の電子署名
・システムにログインする場合の個人認証

## ●　ネットワーク認証

インターネットの普及や企業内ネットワークの整備が，企業の生産性を大きく向上させてきたが，それと同時にネットワークを通じた不正アクセスや悪質なコンピュータウイルス，ワームの侵入が新たな脅威として問題となってきている。これらに対する取組みについて説明する。

(1)　PKIによる無線LAN認証

ここ数年，無線LANの急激な普及が進んでおり，今後も爆発的な普及が予想される。ノートパソコンのLAN接続方法としては，今後，無線LANが主流になっていくと考えられるが，その認証や通信の暗号化に関しては現状，高いセキュリティ環境を準備できているとは言い難い。今後，IEEE 802.11iの策定やWPA（Wi-Fi Protected Access）の普及が進むにつれ，無線LANのセキュリティも向上していくと予想される。

富士通ソシューリョンスクエアでは，PKIを無線LAN接続時の認証方式として適用しており，ネットワーク接続時のセキュリティを向上させた。

(2)　未登録端末の接続禁止および監視

ネットワークに接続するパソコンはあらかじめMACアドレスをDHCPサーバに登録し，ネットワーク接続時に自動的にIPアドレスが配布される。MACアドレスが登録されていない不正なパソコンがネットワークに接続された場合は，DHCPサーバからIPアドレスが配布されないため，正常にはアクセスできない（**図**-6）。また，仮に，ネットワーク構成情報を知ることで，直接ネットワーク設定（IPアドレス，ネットマスクなど）を行って接続した場合でも，不正利用者監視システムがネットワークを常に監視しており，MACアドレス未登録端末を即座に検知し，ネットワーク管理者へそれを通知する。

以上の技術により，不審者によるネットワーク接続および侵入を防ぐことを可能とした。

## むすび

本稿では，富士通ソリューションスクエアで取り入れているセキュリティについて紹介するとともに，富士通におけるセキュリティの取組みの一部を説明した。

将来にわたり，富士通がセキュリティにおいて信頼されるためには，セキュリティ技術を向上させるだけではなく，それを確実に運用し，実績を積み重ねていくことが重要と考えている。

**参 考 文 献**

(1) 綱井理恵：実践！情報セキュリティポリシー運用.
http://www.atmarkit.co.jp/fsecurity/rensai/policy11/policy01.html
(2) 野坂克征：情報セキュリティ運用の基礎知識.
http://www.atmarkit.co.jp/fsecurity/rensai/info01/info01a.html