

情報セキュリティ報告書 2007

2007年12月

富士ゼロックス株式会社

目次

1. 基本情報	1
1.1 本報告書の目的	1
1.2 本報告書の対象期間	1
1.3 本報告書の責任部署（連絡先）	1
2. 経営者の情報セキュリティに関する考え方	2
2.1 富士ゼロックスの考える情報セキュリティ	2
2.2 対象範囲	2
3. 情報セキュリティガバナンス	3
3.1 全社の情報セキュリティマネジメント体制	3
3.2 情報セキュリティに関わる会議体	4
3.3 情報セキュリティに関わる重要なリスク	4
3.4 情報セキュリティ戦略	5
3.5 情報セキュリティに係る主要注力テーマ	6
4. 全社の情報セキュリティ	8
4.1 2006 年度に実施したこと	8
4.2 今後、実施すること	9
5. 部門の情報セキュリティ	11
5.1 新本社の取り組み事例	11
5.2 SE 部門の取り組み事例	12
6. 提供商品の情報セキュリティ	13
6.1 2006 年度に実施したこと	13
7. 情報セキュリティ機能・商品の提供	14
7.1 当社が提供するもの	14
7.2 「ドキュメントセキュリティ」とは	14
8. 情報セキュリティ事故の管理	15
8.1 事故の報告	15
8.2 事故からの学習	15

9.	第三者評価・認証	17
9.1	ISMS 認証取得状況	17
9.2	プライバシーマーク認証取得状況	18
9.3	ISO/IEC 15408 認証取得状況	18

1. 基本情報

1.1 本報告書の目的

本報告書は、富士ゼロックス株式会社（以下、「富士ゼロックス」といいます）の情報セキュリティへの取組みをステークホルダー¹⁾の皆様に説明し、事業への信頼性を高めていただくことを目的として公表します。本報告書における内容は、公表にあたり、情報セキュリティの効果を阻害しない範囲で、ステークホルダーの皆様に開示することが適当であると判断した情報を記載しています。

1.2 本報告書の対象期間

本報告書が対象とする期間は、2006年4月1日～2007年3月31日とします。

1.3 本報告書の責任部署（連絡先）

〒107-0052 東京都港区赤坂9丁目7番3号
富士ゼロックス株式会社
情報セキュリティ部 部長 関 昭男
電話：03-6271-5190（部直通）

1) 本報告書で使用する「ステークホルダー」は、お客様、社員、取引先、株主、地域住民その他の利害関係者とします。

2. 経営者の情報セキュリティに関する考え方

2.1 富士ゼロックスの考える情報セキュリティ

富士ゼロックスは、ブロードバンド環境を積極的に活用するユビキタス時代の新たな働き方と、オフィス、企業、国や地域といった枠組みを越えて知と知のコラボレーションを実現し、よりフレキシブルに働ける場をお客様に提供したいと考え、「オープン オフィス フロントティア」を事業ビジョンとして掲げました。

お客様がオープンなオフィスで情報の利活用や流通を促進するためには、セキュアな環境が保証されなければなりません。情報セキュリティが確保された環境の下でこそ、企業や組織は、その枠を越えて自由にコラボレーションでき、そこで働く個人は創造性にあふれる仕事を行うことが可能になるのです。このように富士ゼロックスは、情報セキュリティを事業ビジョン「オープン オフィス フロントティア」実現のための必須要件だと考えております。

富士ゼロックスの情報セキュリティへの取組みにおいては、利便性と安全性の適正なバランスや個人情報保護などのコンプライアンスを実現するために、マネジメント体制の整備や適切な IT 技術を導入する一方で、日々の業務遂行において従業員一人ひとりの情報セキュリティに対する感性を高め、自律的な行動が取れるようにすることが重要だと考えています。

2.2 対象範囲

本報告書が対象とする組織は、富士ゼロックスおよび関連会社²⁾（以下、「全社」といいます）とし、対象者は、全社の役員ならびに社員、社員外従業員、派遣社員等の会社の情報資産を取り扱うすべての従業者とします。

2) 関連会社とは、富士ゼロックス株式会社が議決権の過半数を直接または間接に保有する会社とします。個々の関連会社については、<http://www.fujixerox.co.jp/company/locations/>をご参照ください。

3. 情報セキュリティガバナンス

3.1 全社の情報セキュリティマネジメント体制

(1) 情報セキュリティマネジメント体制

個人情報保護法への取組みをきっかけに、2005年7月1日付で情報の保護と利活用の促進を目的とした専任組織として「情報セキュリティ部」を本社に新設しました。情報セキュリティ対策が実効性をあげるためには、ファイアウォールや認証などのITによる対策に加え、コンプライアンスや倫理などの人的対策も重要であり、両者を適切に組み合わせて実施する必要があります。この考えに基づき情報セキュリティ部が、ITによる情報セキュリティを担当する情報通信システム部や企業倫理やファシリティマネジメントの側面から情報セキュリティを担当する総務部と一体となって、全社の情報セキュリティガバナンスを推進しています。(図1)

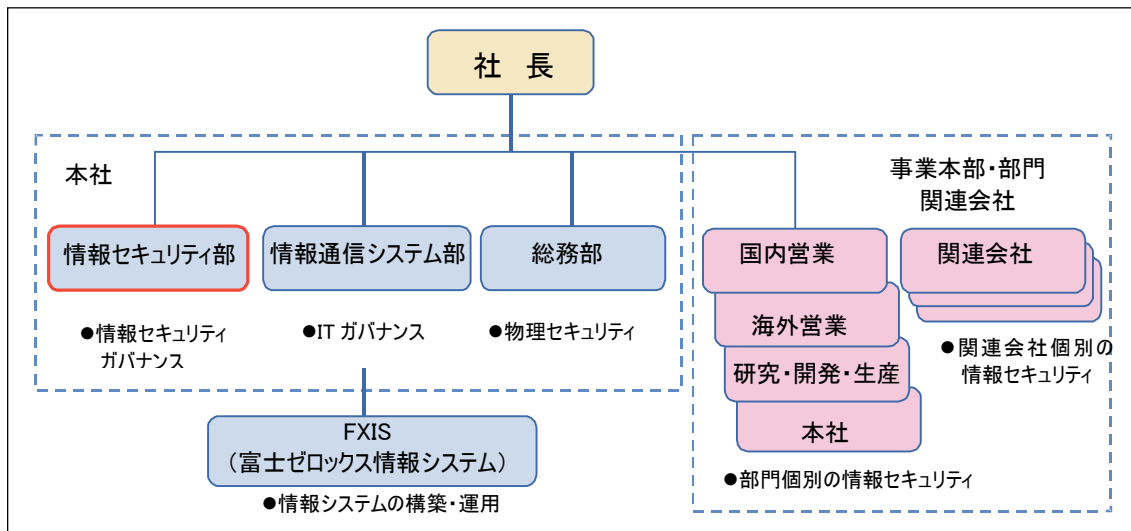


図1 全社情報セキュリティマネジメント体制

(2) 本社組織の役割

① 情報セキュリティ部

情報セキュリティ部は、第一に本社組織として全社の情報セキュリティ方針・規程・ルールを作り、第二にこれらに基づく全社統制、監視活動、統制環境の整備等を行い、第三に社内実践事例の構築・ノウハウの蓄積による成果を全社およびお客様へ展開しています。

② 情報通信システム部

情報通信システム部は、インターネット接続環境におけるファイアウォール、リモートアクセスや各種業務システムの利用における個人認証、コンピュータウイルス対策など、コンピュータシステムに対するセキュリティを担当しています。

③ 総務部

総務部は、企業倫理の観点から情報セキュリティ意識の醸成・定着、およびファシリティマネジメントの観点から情報資産・文書資産に対する物理的セキュリティ対策の役割を担っています。また、文書管理の観点からバイタル・レコード・マネジメントを実践しています。

(3) 事業本部・部門および関連会社の役割

本社が全社共通の情報セキュリティ対策（以下、「全社の情報セキュリティ」といいます）を担うのに対し、現場における従業員一人ひとりのレベルで情報セキュリティを徹底するために、共通課題を抱える複数の組織の集合体や関連会社ごとに、現場主体で情報セキュリティに取り組んでいます（以下、「部門の情報セキュリティ」といいます）。

(4) 富士ゼロックス情報システム株式会社の役割

富士ゼロックス情報システム株式会社は、1984年9月、富士ゼロックスの100%出資により設立されました。その後、富士ゼロックスから情報システム部門の機能の一部とホストコンピュータ・ネットワーク回線等のインフラ資産の移管を受け、外販の一方で全社の社内システムの開発・運用やネットワークインフラの運用管理を担当しています。

3.2 情報セキュリティに関わる会議体

情報セキュリティに関わる意思決定機関は、社長が議長を務めるリスク&エシックス会議としています。ここでは、情報セキュリティに関する重要な戦略・方針・規程等の審議・決定や、大規模な情報漏洩時の対応方針の審議・決定等を行います。

さらに、リスク&エシックス会議の下部機関として全社情報セキュリティ連絡会を設置し、リスク&エシックス会議への上程についての審議・決定やリスク&エシックス会議の決定事項の推進を行っています。この、全社情報セキュリティ連絡会は、関連会社を含めた各組織の代表で構成されています。

3.3 情報セキュリティに関わる重要なリスク

情報セキュリティに関わるリスクとしては、お客様へ製品を提供する上でのリスク、社内でお客様情報・個人情報・機密情報を扱う上でのリスクを重要なリスクとして捉えています。

(1) セキュアでない製品やサービスをお客様に提供してしまうリスク

富士ゼロックスは、全社を通じてお客様が情報を取り扱うための製品やサービス（以下、「商品」という）を提供しています。お客様に提供するこれらの商品がお客様の情報資産の保護を妨げる事態が発生した場合、お客様に多大なご迷惑をおかけしてしまいます。また、それに伴い市場の信頼を失い、ひいてはブランド価値の低下を招き、全社の事業継続に多大な影響を与えるものと認識しています。（6章参照）

(2) 内部の従業員の悪意によるリスク

富士ゼロックスでは、「個人情報保護法」の施行に伴い、従来にも増して情報セキュリティの強化を図ってきました。しかしながら、サービスビジネスを展開する上で、「お客様の情報資産へのアクセス権限を有する業務」、「お客様・情報主体からの情報資産をお預かりする業務」などでは、事故が発生した場合の影響度が高くなってきています。また、このような業務では、お客様の情報資産に触れる機会が多くなっており、内部の悪意を持った従業員による情報の持ち出し等のリスクも無視できないものになってきています。

以上のことから、事故の発生頻度は低いものの、内部の犯行や悪意による情報セキュリティ上のリスクを新たな課題として認識しています。（3.5（1）、8.2参照）

(3) 大規模災害のリスク

地震等の大規模災害は、情報セキュリティの観点から次の2つの側面において、会社の事業継続に甚大な影響を与えると考えています。（3.5（3）参照）

- (A) 会社の事業を支える情報通信機能やお客様からお預かりしている情報資産に対する脅威となる。
- (B) 提供商品が、お客様の情報資産の保護を、特に完全性および可用性の面で妨げる脅威となる。

3.4 情報セキュリティ戦略

(1) 情報セキュリティ戦略の概要

富士ゼロックスでは、情報セキュリティ部が中心となり、約3年後のあるべき姿を目標として設定した全社の情報セキュリティ戦略を立案し、毎年、予算に反映した上で実行しています。今年度は、安全性と利便性の両立を中心施策に据えています。

これと並行して、情報セキュリティの視点で重要な業務・情報資産に対する徹底的な安全性追求策も計画しています。

(2) 全社の情報セキュリティ

情報セキュリティ部が中心となって実施する全社の情報セキュリティは、情報セキュリティマネジメントの成熟度を向上させるとともに、情報セキュリティパフォーマンスの維持向上（情報セキュリティ事故の低減）を目的としています。それを達成するために、すべての従業員に対して次のような全社共通の情報セキュリティ対策（ベースライン対策）を実施しています。

- 高リスク業務に対するリスク評価と、脆弱性に対する徹底対応
- 従業員の意識向上のための企業倫理・情報セキュリティ教育の再徹底
- シンクライアントの導入による利便性と安全性の両立

AFSC（All Fuji Xerox Security Card：全社で運用する全従業員を対象とした個人認証用の IC カード）活用の本格化

- 使用禁止ソフトの検知/削除指示、例外使用許可等の運用開始
- 情報セキュリティ対策の遵守状況の監視・監査
- 脆弱性検査の強化（Web アプリ、重要情報取扱い業務等）

(3) 部門の情報セキュリティ

全社を 17 の管理単位に分け、その責任者は、配下の固有リスクを把握し、上記ベースライン対策に加え個別対策を策定・実施しています。個別対策の例としては、次のようなものが挙げられます。

- サービスビジネスにおける情報セキュリティ品質の強化
- 高リスク業務の抽出と脆弱性改善計画の立案・遂行
- 委託先管理ガイドに基づく委託先の管理・監督強化

3.5 情報セキュリティに係る主要注力テーマ

(1) 「内部の悪意」に対抗しうる情報セキュリティマネジメントの強化

最近、いくつかの内部の関係者による情報漏洩事件がマスコミで報道されております。これらの事件では、漏洩の事実自体が企業にとって大きなダメージとなったり、極めて重要な営業秘密が流出したにもかかわらず、事件の立件自体が困難とされるなど、流失した情報資産の保護については疑問が残る結果となっています。これらの事件を通じて、情報セキュリティは「内部の悪意」には極めて脆弱であることが露呈しました。

富士ゼロックスにおいても、昨年 9 月に発生した情報資産にまつわる内部の関係者による脅迫事件をきっかけに、社長特命による専門チームを結成し、情報漏洩により、社会やお客様に深刻な影響をおよぼす可能性がある重要情報を取り扱う業務を洗い出し、その業務プロセス上に想定される「内部の悪意」にも対抗しうる対策を実施しています。

(2) 海外子会社における情報セキュリティマネジメントの強化

2007 年度からサービスビジネスのグローバル化が本格的にスタートするのにあたり、提供するサービスにおける情報セキュリティを確保することは、この事業を成功させるための最重要課題の一つであると認識しています。

そのための施策の一環として、海外（富士ゼロックスはアジア・パシフィック地域を販売テリトリーとしています）の子会社における情報セキュリティレベルの底上げをねらいとして、富士ゼロックス共通のルールを適用し、情報セキュリティ事故の報告を義務付けました。

また、今後とも、ルールの展開や教育の実施を通じて、富士ゼロックスブランドの下で業務に従事するすべての従業員に、富士ゼロックスが目指す情報セキュリティ意識を醸成し、日常業務における具体的な行動に応用できるようにしていきます。

(3) 基幹情報システムとデータセンターの対災害能力の強化

富士ゼロックスの事業を遂行するために、eHUB³⁾ を中心とした基幹情報システムは大きな役割を担っています。現段階ではデータセンターに被災対策を施しているとはいえ、大地震等の大規模災害時に、一定期間のシステム停止状態が発生し、事業遂行に影響を及ぼす可能性があることを認識しています。

そのための施策として、地震等の天災およびライフラインの停止に対応することを目的に対災害能力が、さらに優れたデータセンターを確保し、基幹情報システムを移設・収容することを計画しています。

3) eHUB とは「Enterprise Hub (エンタープライズ・ハブ)」をあらわし、「富士ゼロックスにおける業務の機軸となるシステム」という意味が込められています。

4. 全社の情報セキュリティ

4.1 2006 年度に実施したこと

ここでは、2006 年度に実施した全社に対する取組みについて説明します。

(1) 情報セキュリティマネジメント成熟度の向上に関する対策

2006 年度は、「全社セクター管理体制の整備・定着」、「コンプライアンス対応力の強化」、「事業継続性の担保」および「積極的情報公開」を重点テーマとして実施してきました。これら施策の実施状況は次のとおりです。

- 全社情報セキュリティ連絡会を設置し、関連会社も含めた 2 ヶ月に一度の定期的な開催を開始しました。
- 各組織の固有課題を明確にするために、各組織ごとの実施計画書を作成し、進捗管理・レビューを行いました。これにより国内営業部門を中心に、高リスク業務の洗出しや海外営業部門における規程の整備が進みました。
- 個人情報管理台帳の整備の一環として、システムの利便性向上を図り、個人情報により確実に管理できる仕組みとして充実させました。
- 教育の一環として、情報セキュリティ基礎教育のほか、個人情報に関する委託先管理ガイド、顧客接点業務におけるガイドの展開を行いました。

(2) 情報セキュリティパフォーマンスの維持向上に関する対策

2006 年度は、「重要な情報資産（PC、USB メモリ）の事故低減」、「高リスク業務に対する内部の悪意対策の円滑な導入」および「サービス業務における情報セキュリティ品質の向上」を重点テーマとして実施してきました。これら施策の実施状況は次のとおりです。

- PC のハードディスク全体暗号化ツールの展開による持出し PC の情報漏洩対策を導入しました。また、持出し PC、およびオフィス内業務用 PC の運用ガイドを展開し、事故低減を図りました。そして、事故報告全体件数に占める PC、USB メモリの事故比率は、目標である対前年 30% 減に対して 47% 減となりました。このことから、施策の効果が現れてきていると考えられます。
- 高リスク業務に対する内部の悪意対策のために、リスクレベルを設定し、国内営業部門を中心にそれに基づく高リスク業務を特定し、特にレベルの高い業務については脆弱性検査を実施した上で施策案を整理しました。そして、その結果を該当部門へ展開、該当部門では具体的な実施計画を立て、高リスク業務への施策実施に着手しました。
- 事業継続性担保の一環として、重大事故の教訓を生かすためのビデオ教材を制作し、教育展開しました。

- AFSC の全社展開に基づき、次のシステムを一部の事業所へ導入し、セキュリティレベルの向上を図りました。
 - ・ AFSC 認証による入退出管理システム
 - ・ AFSC 認証によるセキュアプリント出力システム 等
- モバイル環境で安全に電子メールを利用するために、PC 用 Web メール、携帯電話用 Web メールを導入し、運用を開始しました。

4.2 今後、実施すること

(1) 情報セキュリティマネジメント成熟度の向上に関する対策

今後、実施予定の主な対策は次のとおりです。

- 高リスク業務(情報資産)を継続的に把握し、リスクに応じた施策を計画的に実施していきます。
- 現場点検の定期実施(日常的な現場点検の実施、Web 脆弱性検査の定期実施等)により、リスクの評価と現場への是正の指摘を行います。
- ベンチマークレベルの実践事例を構築し、「言行一致」⁴⁾の対策を推進します。
- 情報セキュリティ人材像を明確にした上で、情報セキュリティ人材育成・教育体系の整備を図り、それに基づく教育を計画し推進します。
また、情報セキュリティガイドラインを整備・展開し、全従業員のさらなる基本の再徹底、意識向上を図ります。
- 海外関連会社を含めたグローバル情報セキュリティガバナンスの仕組みの強化を図ります。

(2) 情報セキュリティパフォーマンスの維持向上に関する対策

今後、実施予定の主な対策は次のとおりです。

- サービスビジネス推進のために、経常的に情報セキュリティの品質保証を行うための機能を立ち上げます。
- ルールの再徹底を図るために、情報セキュリティ規程の見直しを行います。
- 業務リスクの抽出と脆弱性検査手法の確立・展開により、サービスビジネスにおける個別案件業務のリスク低減を図ります。
- 紙文書の抜本的セキュリティ強化に取り組みます。(複合機・プリンタを通じての情報漏洩、ファックスの誤送信等の防止)

4) 富士ゼロックスにおける「言行一致」とは、まず社内に対するサービスの提供・効果の検証を行い、その経験から得られた「知」をお客様に提供するという文化のことをいいます。

- シンクライアント、端末認証、文書管理サーバ、漏洩検知、禁止ソフト対策、電子署名等により、安全性と利便性の両立を図っていきます。
また、社外とのドキュメント交換において PKI の利用を促進し、お客様との間のドキュメント交換時のセキュリティを充実させます。
- 環境に配慮したシュレッダーやメディアクラッシャーなどの配備をさらに拡大し、廃棄機器からの情報漏洩防止の徹底を図ります。

5. 部門の情報セキュリティ

5.1 新本社の取り組み事例

当社は、約2年にわたる社内プロジェクト活動を経て、2007年1月に本社を東京ミッドタウンへ移転しました。新本社で目指す姿の1つとして、「物理セキュリティ・情報セキュリティの強化」を掲げ、これらを実現するための施策として、個人認証用のAFSCを導入しました。

AFSCを利用した施策の中で、主なものは次の2点です。

(1) 物理セキュリティの確保

新本社への入館および各階ごとの入場制限機能により、物理的セキュリティを確保しています。(図2)

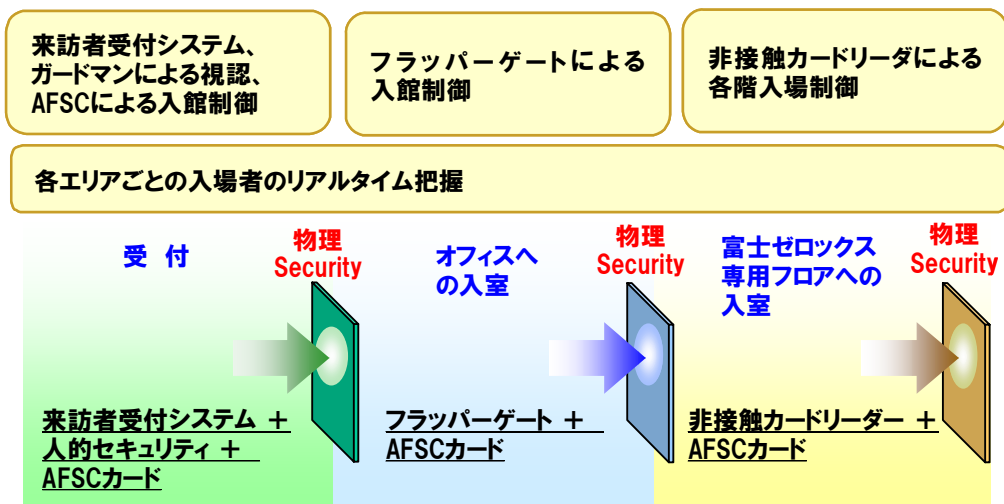


図2 新本社の物理セキュリティ

(2) ドキュメントセキュリティの確保

富士ゼロックスの複合機 ApeosPort との連携により、出力認証を中心とした情報セキュリティの確保とプリントの無駄排除を推進しています。

具体的には、「複合機のユーザ管理」、「複合機側でのプリントジョブ選択」、「ペーパーレス FAX」を実現し、いつでも、どこでも、どの複合機からも、必要に応じて出力できる環境を構築しました。また、事前にデータベースに登録されている従業員のみがプリントが許可されることで、よりセキュアな環境となりました。そして、放置プリントの撲滅、出力枚数の削減、効率的な配置による複合機全体の台数削減も達成しています。

5.2 SE 部門の取り組み事例

(1) 背景と経緯

システムエンジニアリング部(以下、「SE 部」といいます)が提供するソリューションサービスでは、設計は SE 部が行ない、実装は外部に委託するケースが多く、ソリューションサービスのセキュリティを確保するには委託先の管理・監督を適切に行っていくことが非常に重要です。

そこで、SE 部では、委託先のセキュリティマネジメントをより強固なものにするため、2006 年 11 月に主要委託先に対して、富士ゼロックスの「個人情報に関する委託先管理ガイド」に則り、「パートナー様向け情報セキュリティ説明会」を開催し、各社における「個人情報・機密情報取扱い状況」についての調査協力依頼を行いました。

(2) 委託先の調査結果

パートナー各社からの調査結果を分析し(図 3)、一定水準に満たない委託先(調査票の質問項目の整備状況を点数化しボーダラインを設定)に対して個別に訪問し改善計画の提出を依頼しました。

SE 部では、この調査を毎年継続し、改善計画の進捗を監査することで、委託先の情報セキュリティマネジメントを確実に行っていきます。

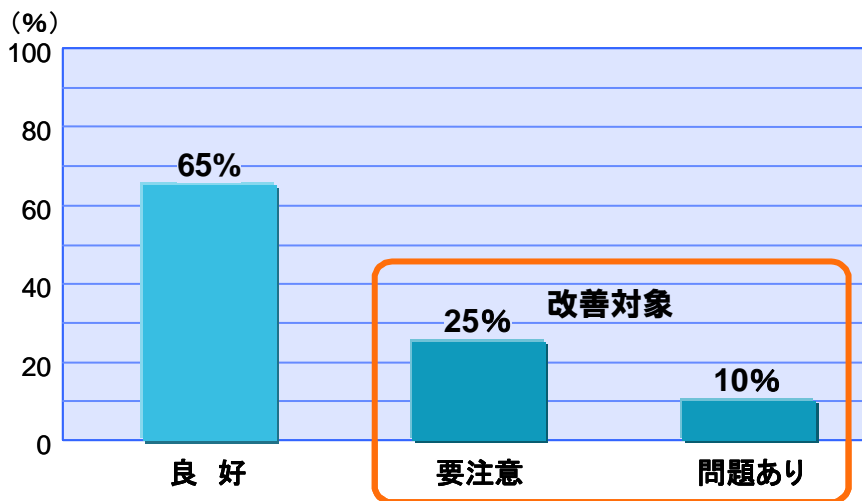


図 3 調査票分析結果

6. 提供商品の情報セキュリティ

「提供商品の情報セキュリティ」とは、商品に対するサイバー攻撃や不正アクセス、ウイルス感染などの意図的脅威からお客様の情報資産を守り、その機密性・完全性・可用性を確保し、維持することを意味します。

この意図的脅威に起因するリスクを最小限に抑えるため、富士ゼロックスでは、企画から設計／開発、生産準備に至る一連の商品開発プロセスの一部として、「セキュア開発プロセス」を組み込むとともに、お客様へセキュリティ上安全な商品を提供できるような商品開発体制を構築しています。

一方、富士ゼロックス商品の不具合や使用者の操作ミスなどによる偶発的脅威に起因する情報セキュリティ問題については、「セキュア開発プロセス」を包含する商品開発プロセス全体の中で、対応・改善することとしています。

6.1 2006 年度に実施したこと

2006 年度は、セキュリティに関わる市場・顧客要求へタイムリーに対応していく中で、セキュアな設計・開発手法をより強固なものとするため、過去の問題事例の再発防止に立ち返り、機能のロジックやデータ整合性のチェックを通して、手法やツール類を拡充してきました。

また、セキュリティ技術教育の一環として、「セキュアプログラミングガイド」を再整備するとともに、実習的な教育教材も開発し、社内展開を行ってきました。

7. 情報セキュリティ機能・商品の提供

7.1 当社が提供するもの

近年の情報セキュリティ関連の設備投資動向を見ると、ネットワークセキュリティへの投資は一段落し、投資の主体は、センターサーバ監視から、さらにはコンテンツ監視に移行しつつあります。また、コンピュータやインターネット関連機器のコモディティ化に伴い、コンテンツとしては、従来の構造化データに加え、非構造化データである電子文書や紙文書の流通量が飛躍的に増えてきています。一方、個人情報漏洩事故を見ると、電子文書に加え、紙文書もかなりの件数を占めています。

富士ゼロックスでは、これらの状況を踏まえ、電子文書と紙文書を統合的に取り扱うことができ、機密性と利便性を両立させた、セキュアなドキュメント利用環境を提供していきます。その利用環境を実現するための技術の総称が、現在、研究開発中の「ドキュメントセキュリティ」です。

7.2 「ドキュメントセキュリティ」とは

「ドキュメントセキュリティ」は、(1) ドキュメントの利用制御技術、(2) ドキュメントの利用履歴管理技術 から構成されます。

ドキュメントの利用制御とは、利用する権利を持つユーザだけに、電子文書や紙文書の利用を許し、権利を持たないユーザには不正利用させないことです。その制御範囲は、サーバ（ハードウェア）、PC、複合機、プリンタ等の、機器レベルでの制御から、Webアプリケーションサーバやデータベース、コンテンツ・マネジメント・システム等のサーバレベルでの制御、文書アプリケーション、プリントアウトされた物理的実体（紙）等の、コンテンツレベルでの制御にまで及びます。不正利用の禁止だけではなく、抑止効果の付与も重要です。

一方、ドキュメントの利用履歴管理とは、ユーザが電子文書や紙文書を利用した際の履歴を捕捉することです。利用する権利の有無や、利用の成功・失敗にかかわらず、ユーザが利用した、もしくは利用しようとした事実がログとして捕捉されます。機器レベルでの利用、サーバレベルでの利用およびコンテンツレベルでの利用を履歴対象とします。

ドキュメントの利用制御と利用履歴管理とは、対をなす関係にあります。利用制御が能動的な機密性の確保だとすると、利用履歴管理は受動的なものと言えます。どちらも重要で、対をなすことで、初めて機密性を確保できます。

富士ゼロックスではすでに、「ドキュメントセキュリティ」の研究開発成果の一端を、複合機やプリンタ、コンテンツ・マネジメント・システム、文書アプリケーション等の自社製品の中で実現し、提供しています。今後とも、これらのセキュアなドキュメント利用環境の提供に向け、邁進していきます。

8. 情報セキュリティ事故の管理

富士ゼロックスでは、情報セキュリティ事故防止のための最も有効な手段として情報セキュリティ事故の管理を重視し、事故からの学習を通じて改善策の立案・展開につなげています。

8.1 事故の報告

事故が多いのか少ないのか、増えているのか減っているのか、深刻な状況なのか否かなどのシグナルを察知するためには、まず事故がどのくらい発生しているのか、その分母を把握することが重要です。分母を捉えるためには、事故が発生したら必ず報告するということを全社に徹底しなければなりません。

そのために、2 時間以内に緊急報告をし、その後は所定の報告フォームに内容を記述し、事態の進展の都度報告することを全社員に義務づけています。毎年、事故報告件数は増加傾向にありますが、報告内容は、軽微な事故報告も含めて着実に報告されるようになってきており、事故報告の仕組みが定着してきたと考えています。

現在、これらの仕組みは国内において実施されており、海外子会社については同一の仕組みではありませんが、各会社毎に結果を取りまとめ報告されるようになっています。

また、事故報告管理の面では、セキュリティ施策の効果を評価する指標として、重大なリスクに発展する可能性があるという観点から、ノート PC、USB メモリの事故報告件数を捉えていますが、2006 年度は、これらの事故報告件数は減少傾向にあり、各種施策の効果が現れてきたものと判断しています。

8.2 事故からの学習

2006 年 9 月 7 日、当社は公式ホームページなどを通じて国内子会社の協力会社社員が脅迫の容疑で警視庁に逮捕された事件（内部の者により意図的に引き起こされた戸籍情報総合システムに関わる事件）について公表しました。この事件では、多くのお客様にご心配やご迷惑をおかけすることになりました。二度とこのような事件・事故を繰り返さないために、内部からの情報漏洩に対しても十分な対応が可能な情報セキュリティ対策への取り組みを始めました。

そのために緊急タスクを発足し、全社にわたり業務プロセスに着目したリスクの調査を急ピッチで進め、重大リスクへの対応に着手し始めています。このタスクでは、お客様の情報資産や個人情報に関わる情報を大量に扱う業務に着目し、①その業務の中から高リスク業務を絞り込み、②その業務に対して脆弱性検査を実施し、③脆弱（悪意に弱い）部分

について緊急対策を行うというステップで活動を進めています。さらに全社に対する情報セキュリティ意識向上策を実施しています。

9. 第三者評価・認証

富士ゼロックスでは、内部監査に加え、第三者認証機関による認証を取得しています。ここでは、外部の第三者機関による認証取得の実績をまとめます。

9.1 ISMS 認証取得状況

2007年3月現在、次の組織がISMS認証を取得しています(表2)。

表2 ISMS 認証取得状況

取得年月	取得会社名称	取得認証規準	取得部門名称
2002年1月	富士ゼロックス(株)	BS7799-2:2002 ISO/IEC 27001:2005 (2005年12月取得)	Xnet(電子証明書発行サービス) 情報通信システム部他
2003年11月	富士ゼロックス(株)	ISMS-Ver2.0 BS7799-2:2002	販売本部官公庁支社
2004年1月	富士ゼロックス(株)	ISMS-Ver2.0 BS7799-2:2002	オフィスサービス事業本部 ドキュメントアウトソーシングサービス 事業部
2004年3月	富士ゼロックス システムサービス(株)	ISMS-Ver2.0 BS7799-2:2002 ISO/IEC 27001:2005 (2007年3月取得)	板橋事業所(2004年3月) 大阪事業所(2005年3月) 板橋事業所(移行審査) 大阪事業所(移行審査) 電響社ビル事業所(拡大審査)
2004年3月	富士ゼロックス千葉(株)	ISMS-Ver2.0 BS7799-2:2002 ISO/IEC 27001:2005 (2007年3月取得)	全部門
2005年3月	富士ゼロックス(株)	ISMS-Ver2.0 BS7799-2:2002	オフィスサービス事業本部 ブロードバンド事業開発部
2005年9月	富士ゼロックス(株)	ISMS-Ver2.0 BS7799-2:2002 ISO/IEC 27001:2005 (2006年9月取得)	富士ゼロックス株式会社(販売会社 含む)の国内における営業活動、お 客様提供サービスに関わる全業務 関連部門
2005年11月	富士ゼロックス 情報システム(株)	ISMS-Ver2.0 BS7799-2:2002 (2005年11月取得) ISO/IEC 27001:2005 (2006年5月取得)	ソリューションサービス事業部(外 販)、およびシステム運用部(海老名 DC)
2006年1月	(株)クロスワークス	ISMS-Ver2.0 BS7799-2:2002 ISO/IEC 27001:2005 (2006年12月取得)	本社、武蔵事業所 全社全部門に拡大
2006年3月	富士ゼロックス(株)	ISMS-Ver2.0 BS7799-2:2002 ISO/IEC 27001:2005 (2007年3月取得)	ビジネス&サプライチェーン改革部
2007年3月	富士ゼロックス上海	ISO/IEC 27001:2005	

9.2 プライバシーマーク認証取得状況

2007年3月現在、子会社4社がプライバシーマークを取得しています（表3）。

表3 プライバシーマーク取得状況

取得年月	取得会社名称
2001年4月	富士ゼロックスシステムサービス(株)
2002年1月	富士ゼロックス情報システム(株)
2004年6月	富士ゼロックスキャリアネット(株)
2005年7月	(株)富士ゼロックス総合教育研究所

9.3 ISO/IEC 15408 認証取得状況

2007年3月現在、表4のとおり、複合機のオプションであるデータセキュリティキットにて、ISO/IEC15408の認証を取得しています。（適合する保証要件：EAL2）

今後も、認証取得の機種数を増やしていく計画です。

表4 ISO/IEC15408 取得状況

取得年月	商品名
2004年9月	モノクロ複合機 DocuCentre 719/659/559 シリーズ データセキュリティキット
2005年7月	カラー複合機 ApeosPort C4535 I/C3626 I/C2521 I シリーズ DocuCentre C4535 I/C3626 I/C2521 I シリーズ データセキュリティキット
2006年2月	モノクロ複合機 ApeosPort 750 I/650 I/550 I シリーズ DocuCentre 750 I/650 I/550 I シリーズ カラー複合機 ApeosPort C7550 I/C6550 I/C5540 I シリーズ DocuCentre C7550 I/C6550 I/C5540 I シリーズ データセキュリティキット
2006年9月	モノクロ複合機 ApeosPort 750 I/650 I Series DocuCentre 750 I/650 I Series ApeosPort 550 I/450 I/350 I Series DocuCentre 550 I/450 I Series カラー複合機 ApeosPort C7550 I/C6550 I/C5540 I Series DocuCentre C7550 I/C6550 I/C5540 I Series Security Kit for Asia Pacific

2006 年 12 月	<p>カラー複合機 ApeosPort- II C4300/C3300/C2200 シリーズ DocuCentre- II C4300/C3300/C2200 シリーズ</p> <p>データセキュリティキット ApeosPort- II C4300/C3300/C2200 Series DocuCentre- II C4300/C3300/C2200 Series</p> <p>Security Kit for Asia Pacific</p>
2007 年 2 月	<p>モノクロ複合機 ApeosPort- II 4000/3000 シリーズ DocuCentre- II 4000/3000 シリーズ</p> <p>カラー複合機 ApeosPort- II C7500/C6500/C5400 シリーズ DocuCentre- II C7500/C6500/C5400 シリーズ</p> <p>データセキュリティキット WorkCentre 7228/7235/7245 Series</p> <p>Security Kit</p>

以上

<訂正履歴>

日付	訂正箇所	訂正内容
2007.12.25	(公式 Web サイトにて 2007 年度版 公表)	