imagio Neo 350/450 シリーズのセキュリティ ～ ISO/IEC 15408 認証取得 ～

Security of imagio Neo 350/450 Series - ISO/IEC 15408 Certification

太田　雄介[*]　　金井　洋一[*]
OHTA Yusuke　　KANAI Yoichi

要　　旨

2002年6月，リコーのデジタル複合機 imagio Neo 350/450 シリーズは，デジタル複合機として世界で初めて ISO/IEC 15408 の認証を取得した．ISO/IEC 15408 は，IT製品のセキュリティ機能が矛盾のない設計に基づいて正しく実装されていると，第三者機関が公的に評価・保証するための国際標準である．認証取得にあたっては，imagio Neo 350/450 を単なるコピー機ではなく様々な脅威にさらされているネットワーク機器ととらえた上で，セキュリティの観点から分析を行った．具体的には，製品が使用される環境を想定，保護資産とそれに対するセキュリティ脅威を定義し，必要なセキュリティ機能を明確にして「セキュリティターゲット」と呼ばれる文書にまとめた．さらに実際の評価作業では，仕様書や設計書およびマニュアル等の文書の検査のほか，実機テストや開発現場の監査等，様々な観点からの評価が行われ，ユーザが安心して使用できる製品として世に送り出した．

ABSTRACT

In June 2002, Ricoh's digital multi-functional printer "imagio Neo 350/450 Series" was certified in accordance with ISO/IEC 15408, which is the international standard for official evaluation bodies to determine if the seuciry functionalities are consistently designed and correctly implemented. For the certification, Ricoh analyzed imagio Neo 350/450 as the network equipment from the view point of verious security threats not as a copier. Some assumptions concerning the environment of imagio Neo 350/450, some assets to be protected, some threats against those assets, and security functions to counter those threats are defined and described in document called "Security Target". The evaluation body inspected many documents such as specification, design document, guidance document, etc., performed tests against the actual product, visited the development site, and so on. This certification means that imagio Neo 350/450 is examined as the secure product by the objective third party.

[*] 研究開発本部 オフィスシステム研究所
Office System R&D Center, Research and Development Group

1. 背景と目的

近年，ITセキュリティに対する関心が高まってきている．ICカードやファイアウォールといったセキュリティに直接関わる製品はもちろんのこと，それ以外の一般的な IT製品のセキュリティの重要度も着実に増しており，リコーの主力製品であるデジタル複合機（MFP = Multi-Functional Printer）やレーザープリンタ等のオフィス機器のセキュリティもその例外ではない．

特に MFP はコピー・プリンタ・スキャナ・ファクスといった複数の機能を持ち，それが取り扱う対象はオフィスにおける重要な資産である紙文書から電子データまで幅広い．また，ネットワークや電話回線に接続されることがほとんどであり，このような環境においては資産に対する外部からのセキュリティ脅威が存在することは明白である．

また，ITセキュリティ業界では第三者機関による製品の評価が重要視されている．セキュリティ機能は，それが正しく働いていることを目で確認することが難しい場合が多く，「製品が仕様どおりに正しく実装されていることを第三者に保証してもらう」ことが大切なのである．欧米では 10年以上前から独自の評価基準を用いてそのようなセキュリティ評価を実施していたが，1999年に各国の評価基準が統一され，国際標準 ISO/IEC 15408 が発行された．日本国内ではようやくその重要性が認められつつある段階である．

このような状況を踏まえ，リコーは主力製品である MFP のなかから imagio Neo 350/450 シリーズ（Fig.1）を選択，ISO/IEC 15408 に基づく客観的な評価を受け，その認証を取得することで，リコーの MFP は安全なものであることを主張していくこととした．

以下，2章では MFP のセキュリティ設計について，3章では ISO/IEC 15408 の概要と imagio Neo 350/450 シリーズが実際に認証を受けた際の評価内容について説明していく．

Fig.1　imagio Neo 350/450.

2. MFPのセキュリティ設計

2-1　前提条件，保護資産とセキュリティ脅威

製品が持つセキュリティ機能の目的を明確にするためには，その製品がどのような環境で使用されることを前提としているのかをまず明確にしなければならない．今回，次のような条件を MFP の使用環境として想定した．

- 内部ネットワーク（LAN = Local Area Network）および電話回線に接続されているものとする．
- LAN はファイアウォール等により安全に管理され，盗聴等のLAN に対する直接攻撃はないものとする．
- 本体に対する物理的攻撃はないものとする．
- 管理者およびサービスマンは信頼できるものとする．

上記の条件の下，MFP に関する次の保護資産を定義し，使用環境下で考えられるセキュリティ脅威からそれら資産を守ることを目的とした．

- 重要な蓄積文書

  ユーザが自分の意思で MFP に保存する文書のうち，所有者が第三者の使用を防ぎたいと思う文書を指す．具体的には「ドキュメントボックス（imagio Neo が持つ電子文書蓄積場所）」にパスワード付で蓄積された文書，PCから「機密印刷」の指定でプリントされた文書，パスワード付の「Fコードボックス」に送信されたファクス文書の3種類を指す．

  【脅威】正当なユーザ（パスワードを知っているユーザ）以外の人物がこれらの重要な蓄積文書に不正にアクセスするかもしれない．(Fig.2 A)
- 残存データ

  コピーやプリント時に，MFP 内のストレージ（RAM や HDD）に一時的に展開される原稿のイメージデータを指す．蓄積文書と異なり，ユーザの意思で保存されるものではない．

  【脅威】前のユーザによって使用された残存データが，次のユーザに不正に使用されてしまうかもしれない．(Fig.2 B)
- MFP を含む内部ネットワークリソース

  MFPのリソースおよび，MFP が接続されている LAN 上のサーバやクライアント等のリソースを指す．

【脅威】外部にいる攻撃者が，電話回線経由でこれらのオフィス内リソースに不正にアクセスするかもしれない．(Fig.2 C)

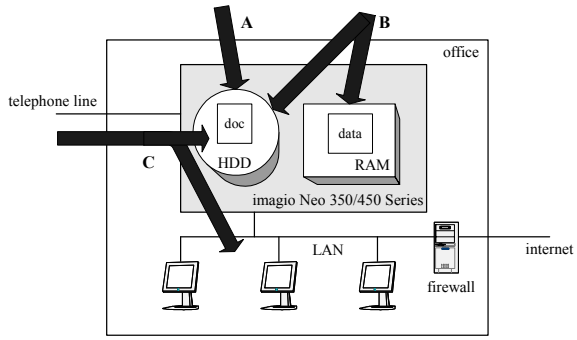

Fig.2　Treats around imagio Neo.

2-2　セキュリティ機能

2-1節で述べた保護資産に対するセキュリティ脅威に対抗するために，imagio Neo 350/450 シリーズには次に述べるセキュリティ機能が実装されている．

(1)　重要な蓄積文書の保護機能
正しいパスワードを入力することによって重要な蓄積文書にアクセスすることができる．パスワードの照合が3回連続失敗するとその文書はロックされ，以降は主電源を再投入しない限り，正しいパスワードを入力してもアクセスすることができない．

(2)　残存データ保護機能
コピーやプリント等の処理の終了後，およびリセット操作を実施すると，以降はその処理時に保存された残存データを出力する手段はなくなる．

(3)　電話回線からの不正侵入防止機能
あらかじめ規定されたプロトコル，すなわちファクスの送受信およびリコーが提供するリモートメンテナンスシステムである CSS（Customer Support System）のコマンド以外の通信はすべて拒絶する．

(4)　管理者の認証
正しい管理者パスワードを入力することによって，管理機能を使用することができる．

imagio Neo 350/450 シリーズは，今回新しく「セキュリティ強化モード」を新設している．ユーザの使いやすさとセキュリティとは互いに相反する性質を持つことがあるため，モードの切り替えを可能にすることによって様々な使用形態に対応できるようになっている．上記のセキュリティ機能のうち (1) の文書ロックに関する部分はセキュリティ強化モードで有効となる．(1) のパスワード照合に関する部分および (2)，(3) についてはセキュリティモードか否かに関係なく有効な機能であり，従来の機種でも同じように実装されていたものである．

3. ISO/IEC 15408 認証取得

3-1　国際標準に基づくセキュリティ評価

ISO/IEC 15408 に基づくセキュリティ評価とは，ある特定の製品のセキュリティについて，公的に認められた第三者評価機関が検査を行うことである．製品が持つセキュリティ強度の評価と誤解されやすいが，強度分析は評価全体の中のごく一部であり，「製品がリーズナブルで矛盾のない設計に基づいて安全な環境で正しく実装され，かつユーザが正しく使用できる方法を提供している」ことを保証するためのものであることに留意する必要がある．このため評価の対象は，製品のセキュリティ仕様書・設計書・マニュアル・開発現場のセキュリティ・製品の製造および配送方法に至るまで多岐にわたる．

ISO/IEC 15408 には検査の深さに応じて「評価保証レベル（EAL = Evaluation Assurance Level）」が規定されている．簡単な検査だけで済む EAL1 から，非常に厳密な検査まで行われる EAL7 まで，7段階のレベルが存在する．軍事・金融などのクリティカルな分野では EAL5 以上の高いレベルが適用されることが多いが，一方で検査内容が厳密かつ複雑になるため評価コストも高くなる．このため，一般のユーザが広く使用するような民生品については EAL1～EAL4 までのレベルが適用されることがほとんどである．

3-2　imagio Neo 350/450 のセキュリティ評価

2002年6月，imagio Neo 350/450 シリーズは，2章で述べたセキュリティ機能について ISO/IEC 15408 EAL3 の認証を取得した．評価はドイツ連邦共和国の評価機関である TUViT 社に依頼，評価ドキュメントの作成および連絡等は英語で行った．

今回のセキュリティ評価のためにリコーが用意，評価機関へ提出したドキュメントは Table 1に示すとおりである．

Table 1　Evaluated Documents.

仕様・設計	
	Security Target（セキュリティターゲット） 製品のセキュリティ設計の基本的な方針と，それに基づくセキュリティ機能を説明するもので，セキュリティ評価における最重要文書.
	Functional Specification セキュリティ機能仕様書．セキュリティ機能を外部インタフェースの観点から説明する文書.
	High-level Design 上位レベル設計書．製品がどのような構造でセキュリティ機能を実現しているかの概要を説明する文書.
分析	
	Correspondence Analysis 上記3つの文書が矛盾なく記述されていることを分析する文書.
	Strength of Function Analysis 製品が持つ機能強度を分析する文書.
	Vulnerability Analysis 製品に内在する脆弱性が問題とならないレベルであることを分析する文書.
テスト	
	Security Test Documentation 製品のセキュリティ機能が正しく動作していることを確認するためのテスト仕様とその結果のレポート.
ガイダンス	
	Guidance Documentation ユーザマニュアル．ユーザに対して必要十分な情報が含まれ，かつ誤った使い方を誘発する記述がないことが求められる.
開発・製造・配送	
	Development Security 製品の開発現場が安全である（機密情報の漏洩がない）ことを説明する文書.
	Configuration Management 開発現場において，正しいバージョンの製品が開発されるような開発方式を採用していることを説明する文書.
	Production Procedure 製造現場において，正しいバージョンの製品が安全に製造されていることを説明する文書.
	Delivery Procedure 正しいバージョンの製品がユーザまで安全に配送されるような方法を採用していることを説明する文書.

評価機関は上記の 12文書が ISO/IEC 15408 に規定されている保証要件を満たしているかどうかの検査を行ったほか，実際に来日した上で開発現場のセキュリティを始めとするいくつかの点について現場を確認したり実機によるセキュリティテストを実施したりした．

4．成果

リコーはオフィス機器業界に先がけて，MFP全体のセキュリティに関する取り組みを実施．網羅的なセキュリティ設計を行った上で，デジタルモノクロ複合機 imagio Neo 350/450 シリーズについてISO/IEC 15408 に基づく評価を受審，その認証を取得した．これは MFP本体としては世界初の認証取得であり， imagio Neo 350/450 シリーズがセキュリティに関して正しい設計のもとで確実に実装されていることを第三者評価機関によって認められたことを意味している．特に，ユーザからの実際の要望が多い「電話回線経由の不正侵入防止機能」について，第三者機関からのお墨付きが得られたことの意義は大きい．

5．今後の展開

リコーはMFPを始めとするあらゆるオフィス機器のセキュリティを重視し，今回の認証取得で得たノウハウをもとに，十分な検討，それに基づく設計，確実な実装を実践して，ユーザが安心して使用できるオフィス機器を提供していく．

謝辞

MFP に搭載されているセキュリティ機能の詳細な内容や開発・製造・配送現場のセキュリティについての調査，セキュリティテストの実施，セキュリティマニュアルの作成等，様々な分野にわたって多数の方々にご尽力・ご協力いただきました．この場を借りて厚く御礼申し上げます．

参考文献

1) ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security
ISO/IEC 15408-1:1999(E), Part 1: Introduction and general model
ISO/IEC 15408-2:1999(E), Part 2: Security functional requirements
ISO/IEC 15408-3:1999(E), Part 3: Security assurance requirements

略語

MFP　Multi-functional Printer
LAN　Local Area Network
EAL　Evaluation Assurance Level