NECグループにおけるITによる情報漏えい防止の取り組み ～情報漏えい防御システムARGUS～

現在、NECでは、新InfoCageシリーズを核に、ITにより情報漏えいを防御するための仕組み(ARGUS:NEC Information Audit-trail & Guard System)を開発しています。その目的は、これまでは規則やモラルに頼らざるを得なかったオフィスの外での作業や情報を第三者に預託するケースにおいてもITによる管理下に置き、情報漏えい事故を防止する、あるいは発生しても影響を最小化することを実現することにあります。ARGUSは、2006年度下期より一部の部門で先行導入を開始しており、2007年度よりNECグループへの本格導入を開始する予定です。

はじめに

NECは、NECグループ(協力会社など業務委託先を含む)においての情報漏えい事故を防止するため、情報漏えい防御システムARGUSを開発しています。人の意識や行動に頼るだけでは、情報漏えい事故を完全に防ぐことはできません。人が原因で発生する情報漏えい事故を、ITにより最大限に防御する(事故を防ぐ、仮に発生しても被害を最小化する)ことを目的としています。

本稿では、ARGUSを開発するに至った背景、目的、機能の概要、今後の展開について紹介します。

開発の背景

NECは、NECイントラネットと呼ばれるNECグループの企業ネットワークを構築、運用しています。これまでIT面では、NECイントラネットを中心に、下記に示すセキュリティ対策を実施し、その延長で情報漏えい対策を進めてきました。

(1)NECイントラネットのセキュア化
商用インターネットとの接続管理、NECイントラネットの状態監視、セキュリティ基準を満たさないPCのNECイントラネットへの接続の排除など

(2)NECイントラネット接続機器のセキュア化
セキュリティパッチ自動適用、ウイルス対策ソフトの自動更新、PC暗号化ソフトの導入など

(3)NECイントラネット内の情報のセキュア化
ファイルの暗号化、ファイルへのアクセス制限など

(4)NECイントラネット利用者の管理
人事情報に基づく全利用者のIDの一元管理、IDによる権限の管理

しかしながら、お客様情報等をオフィス外で取り扱う業務が多く、NECイントラネットだけではなく、業務委託先を含む情報のライフサイクル(情報の受領・作成から廃棄・返却まで)全体をカバーする情報漏えい対策が必要となってきています。

情報の漏えいリスクの所在

情報の受け渡しのルートと流出のリスクを**図1**にまとめました。また、過去の事例およびお客様対応を実施している複数のプロジェクトのヒアリングにより、次のことが分かりました。

1) 情報漏えい事故の主要因は、PCやモバイルメディア(USBメモリ)の盗難/紛失、Winnyなどによるネットワークを介した流出の2つに集約される。

2) 業務委託先の作業者が情報を入手する方法は、お客様あるいはお客様システムから直接入手、NEC社員から入手、プロジェクトサーバから入手など、様々である。

3) 情報が最終的に協力会社社員に渡るまでに、必要に応じて情報の複製・加工が行われている。

4) 作業環境が保護されていないことが事故の発生（被害の拡大）の原因の1つである。

また、情報の持ち出され方については、次のことが分かりました。

(1)業務上、情報を持ち出す必要があった事例が多い。
①業務委託先での開発のため
②お客様システムの保守のため
③作成した情報を、お客様に納入するため

(2)業務上、情報を持ち出す必要性は認められたが、規則に則らず持ち出した事例が多い。
①正規の持ち出し手続きを経ず持ち出し

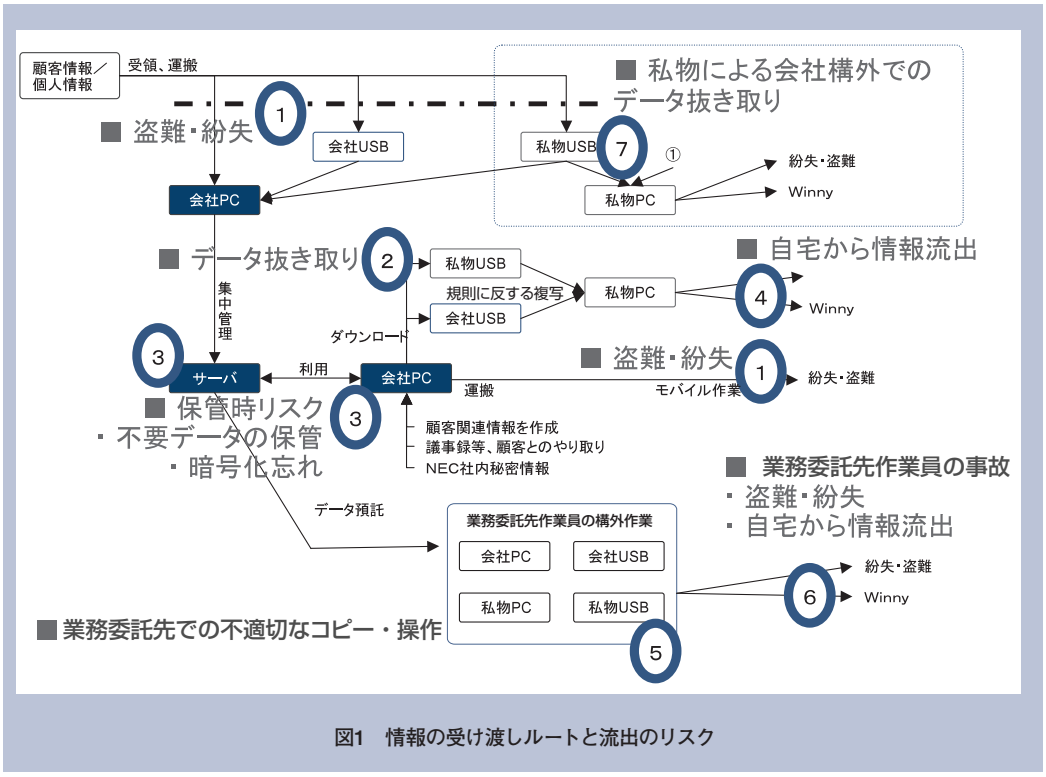

図1　情報の受け渡しルートと流出のリスク

②持ち出した記録を残さず持ち出し
③私物のPCやモバイルメディアの使用

(3)業務上不要な情報も持ち出し、PC上にファイルを保有することで、被害を拡大している。

①要不要を判断せず、情報を一括して持ち出し
②不要になった過去の情報を削除せず保持

システムのめざすもの

以上の分析により、NECグループでの情報漏えい事故を防ぐため、下記の機能を有するシステムを実現することを、目標と定めました。

(1)NECグループの情報を取り扱う会社・組織を網羅

NEC～NEC関係会社～協力会社～再委託先を含む。

特に、これまで有効な対策ができていなかった、協力会社、再委託先への情報の授受についてITによる管理下におく。

(2)情報のライフサイクルを通した管理

情報の受領・作成～活用・保存～返却・廃棄までの情報のライフサイクルを通じて情報を保護し、また、管理・追跡を可能とする。

(3)情報の一元管理とフェイルセーフ化

保護すべき情報はファイルサーバ/ストレージサービスに格納、管理する。作業に必要な情報のみ必要時にPC上にダウンロードし使用する。また、暗号化されていないファイルは、自動的に暗号カプセル化する。

(4)NECグループとしてのITによる統制の強化

情報やモバイルメディアの管理ポリシーを強制適用する。また、PCの使用ログ、ファイルへのアクセスログを

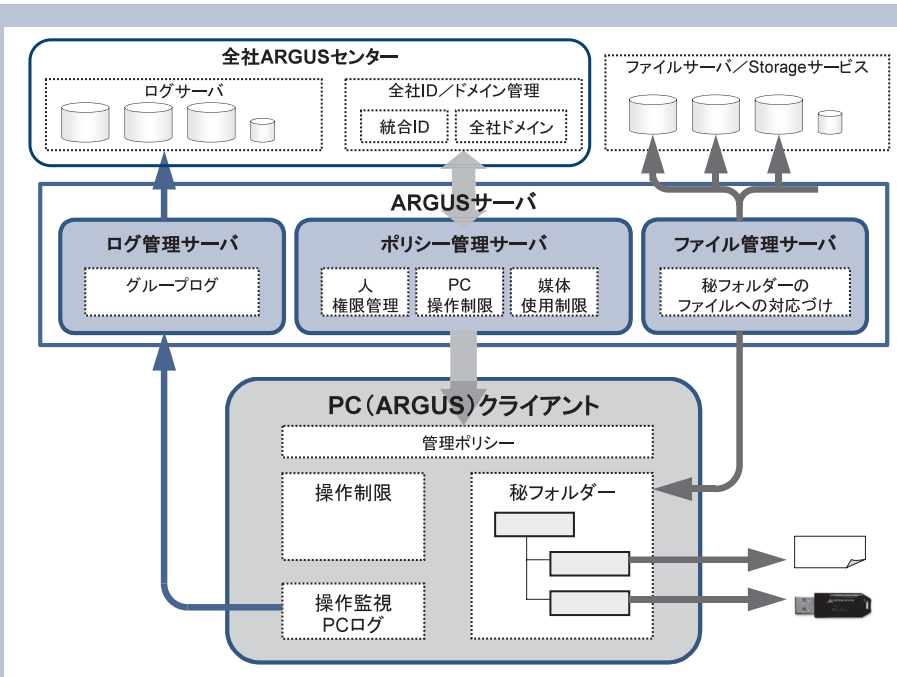

図2　ARGUSの機能構成

集中管理し、必要に応じて検索可能とする。

ARGUSの機能と構成

ARGUSは、(1)ARGUSクライアント、(2)ARGUSサーバ、(3)全社ARGUSセンター、(4)ファイルサーバ/ストレージサービス、から構成されます(図2)。

(1)ARGUSクライアント

ARGUSクライアントは、管理対象とするクライアントPCにインストールされ、ARGUSのポリシー管理サーバから配付されたポリシーに基づき、PCの操作監視、USBデバイスのコントロール、ファイルの暗号カプセル化とファイルサーバ/ストレージサービスへの保存、ファイルの操作ログの記録、を行います。

ARGUSクライアントでファイルを作成すると、作成者以外閲覧不可の閲覧権が付与されます。万が一そのファイルが流出しても、第三者は閲覧できません。

そのファイルをプロジェクトで共有する場合は、秘フォルダに置くことにより指定された要員のみが閲覧できる属性がそのファイルに付与され暗号カプセル化され、ファイルサーバ/ストレージサーバに保存されます。

また、業務委託先に情報を渡すための、特殊な暗号カプセル化の機能(エクスポート機能)を持っています。この機能により、ARGUS環境ではない一般の環境において、利用できる環境を指定してファイルを渡すことを可能とします。それ以外ではそのファイルは開けないため、情報の二次流出を防ぐことができます。

(2)ARGUSサーバ

ARGUSサーバは、ログ管理サーバ、ポリシー管理サーバ、ファイル管理サーバから構成されます。

ログ管理サーバは、定期的にPCからログを吸い上げ、全社ログ管理サーバに蓄積します。

ポリシー管理サーバは、管理下のPCに対して、人(ID)、

PC、モバイルメディアの管理ポリシーを配付し、組織としての統制を可能にします。たとえば、会社指定のUSBメモリ以外は使用不可というようなコントロールを、管理ポリシーを配付し、強制します。

ファイル管理サーバは、ARGUSクライアント上の仮想フォルダと、実際のファイルの保存場所であるファイルサーバ/ストレージサービスとのリンケージを管理します。

(3)全社ARGUSセンター

全社ARGUSセンターは、ログを集中管理しNECグループ全体の統制を行います。また、ARGUSサーバは、全社ID/ドメイン管理と連携し、人(ID)の管理を行います。

(4)ファイルサーバ/ストレージサービス

ARGUSクライアントにより暗号カプセル化されたファイルを保存します。ここに保存されたファイルに対する操作は、操作ログとして記録されます。

導入の効果

情報の受け渡しのルートと流出のリスク(図1)に対する、ARGUSでのリスクコントロール策を**表**に示します。

ARGUSでの管理は、安全なサーバに暗号カプセル化したファイルを保管し、必要な情報を必要な期間だけ持ち出すことが基本となります。

したがって、ARGUSの管理は、情報を入手したら、まず、安全なPCあるいはモバイルメディアに一時的に格納し会社に持ち帰り、ARGUSサーバを介しファイルサーバ/ストレージサーバに保存することから始まります。これにより、ARGUSによる管理追跡が可能になります。

表　ARGUSでのリスク・コントロール策

No.	リスク	リスク・コントロール
①	盗難・紛失	■顧客情報・個人情報・企業秘密情報をすべて暗号カプセル化し、第三者の閲覧不可 ■USBメモリは会社指定製品のみ使用可
②	データ抜き取り	■会社指定のUSBメモリ／USB周辺装置のみ接続可 ■操作ログを監視し不正操作を検知・アラート
③	保管時リスク	■未暗号ファイルは強制暗号化 ■保存期限によりファイル自動削除
④	自宅から情報流出	■顧客情報・個人情報・企業秘密情報をすべて暗号カプセル化し、第三者の閲覧不可
⑤	業務委託先での不適切なコピー・操作	■エクスポート暗号カプセル化 ⇨許可された環境で利用可能
⑥	業務委託先作業員の事故 ・盗難・紛失 ・自宅PCから流出	■顧客情報・個人情報・企業秘密情報をすべて暗号カプセル化し、第三者の閲覧不可 ■エクスポート暗号カプセル化

今後の予定

2006年度下期より、一部の部門でARGUSの先行導入を開始しています。2006年度は、情報漏えい対策のニーズが高いプロジェクトに対し導入を進め、2007年度より、本格的にNECグループへの導入を開始する予定です。

執筆者プロフィール

田村 卓
IT戦略部
マネージャー

神田 昌彦
IT戦略部
シニアマネージャー