2.3. エンドポイントのためのセキュリティ対策

1 人 1 台以上のパソコンの普及やネットワーク環境の充実、USB メモリ等可搬媒体の大容量化により、短時間に多くの人に情報が伝達できるようになりました。このように便利になる一方、コンピュータウィルス／スパイウェアの感染や、盗難、紛失、誤操作、P2P ファイル共有ソフトウェアによる情報漏洩の危険性も高まっています。

学内のイントラネットでは、ファイアウォールの設置やサーバのセキュリティ対策、ネットワーク／サーバの監視等、システム管理者によりセキュリティ対策がなされています。しかし、利用者側のパソコンについては、利用者依存になっている部分が多く、対策が充分できているとは言いがたい状況です。そのため、利用者パソコンが原因で、サーバ側のサービスに影響を及ぼすこともあり、システム管理者の負担を増やす要因となっています。このことから、エンドポイント（利用者側）のセキュリティ対策が重要と考え、対策を検討しました。

エンドポイントのセキュリティ対策は、対象者（教員、職員、学生、技術専門職員、その他（研究員、名誉教授、特任教授、客員教授）毎に、ソリューションを松竹梅で検討しました。以下に概要を示します。

対策レベル１：梅

エンドポイントでセキュリティ対策を実施します。具体的には、ウィルス・スパイウェア対策ソフトウェアやパーソナルファイアウォールの導入、ファイルの暗号化、重要データのファイルサーバへの集約等の対策です。

この対策の利点としては、簡単に始められる、今の利用形態と差が少ない、端末毎の多様性（OS、アプリケーション）が許容される等が挙げられます。

一方問題点としては、利用者任せのセキュリティとなる、機器の紛失、データの漏洩が防げない、事前に被害の可能性が把握できない等が挙げられます。

コストは、短期的には投資額は低く抑えられますが、インシデント発生時にコストが高くなる可能性があり、中長期的には保守コストとの兼ね合いで評価する必要があります。

また、対策レベル１.５として、梅に加え、エンドポイントをフィイアウォールや NAT で隔離することが考えられ、更にセキュリティレベルを上げることができます。

対策レベル２：竹

エンドポイントでセキュリティ対策を実施し、ネットワーク側で実施状況を確認します。具体的には、パソコン等機器をネットワーク接続時に認証や検疫、アクセスコントロールを行います。

この対策の利点としては、利用者管理が可能となり梅よりセキュリティが高い、簡単に始められる、今の利用形態と差が少ない、エージェントレスの場合、端末毎の多様性（OS、アプリケーション）が許容される等が挙げられます。

一方問題点としては、認証に時間がかかる、エージェントの場合、端末の多様性(OS)に対応できない、機器やデータが持ち出し可能であり、機器の紛失、データの漏洩が防げない、事前に被害の可能性が把握できない等が挙げられます。

コストは、短期的にはある程度投資が必要ですが、中長期的には保守コストとの兼ね合いで評価する必要があります。

また、対策レベル２.５として、ブレード PC が考えられます。ブレード PC は、PC を構成する CPU、メモリ、ハードディスクなどの主要な部品を、１枚のブレード（基盤）に集積し、マシンルームにまとめて設置します。クライアント側には画面を転送し操作します。このようにディスクレスにすることで、データの漏洩を防ぐことが可能です。一方、問題点としては、竹と同様セキュリティ対策が利用者任せになってしまう点が挙げられます。

対策レベル３：松

エンドポイントにはデータを保持せず、センター側でソフトウェアやデータを一元管理します。具体的には、端末はシンクライアントとし、アプリケーションは業務で必要なものに限定し、データはセンター側で一括管理する等、管理を徹底します。

この対策の利点としては、セキュリティ対策が一元化できる等管理が容易、利用者による情報漏洩等のリスクが低い、予防／対策が迅速にでき徹底することが可能、被害規模の想定が可能等が挙げられます。

一方問題点としては、集中管理していることから、インシデント発生時に影響が大きいことが挙げられます。

コストは、短期的には投資額が大きくなりますが、保守コストが低減できることが考えられるため、中長期的には保守コストとの兼ね合いで評価する必要があります。

上記の通り、セキュリティ対策を松竹梅のレベルに分けて提示させていただきましたが、センターのポリシーや予算に合わせて選択いただければと考えます。

その他、エンドポイントの課題として以下が考えられ、今後検討していく必要があると考えます。

USB メモリ等の可搬媒体が普及し、容易にデータ交換が可能になりました。一方可搬媒体からウィルス／スパイウェアに感染するケースが増えており、可搬媒体を PC 等の機器にさす前に、ウィルスチェックできる仕組みが必要です。

また、利用者側のセキュリティ対策が進まない原因として、ウィルススキャンのやり方が分からない、時間がかかる等利用者の負担になっていることが考えられます。これらの解決策として、USB にさせば自動的にチェックする等、容易にウィルススキャンできる仕組みが必要と考えます。

更に、P2P ファイル共有ソフトウェアによる情報漏洩も後を絶たないことから、業務に必要ないアプリケーションの使用を禁止、利用できるアプリケーションを限定できるような仕組みが必要と考えます。