情報資産の管理・運用事例

2019年8月30日

早稲田大学　高橋　智広

事例紹介内容

1. 情報資産の取り扱いを定めた経緯
   - ■ 技術的対策
   - ■ 人的・組織的対策
2. 従来の情報資産の取り扱い状況
3. 情報資産管理ルールの制定
   - ■ 従来の情報資産の管理・運用状況の問題点
   - ■ 情報資産管理の対策・方針
4. 情報資産の管理・運用フロー概要
   - ■ 情報資産の機密レベル
   - ■ 情報資産の保管場所
   - ■ その他運用ルール
   - ■ 管理検査

1．情報資産の取り扱いを定めた背景

■ 技術的対策

- 2014年12月のマルウェア感染による情報流出の疑いが発生した事案を受けて、主に職員が利用する事務系システムを対象に以下の技術的対策を講じた。

✓ 事務系システム・ファイルサーバーのファイル暗号化
✓ 事務系システム・PCへのエンドポイントセキュリティソフトの追加導入
✓ 事務系ネットワークでの不審通信検知・遮断ソリューションの導入　等

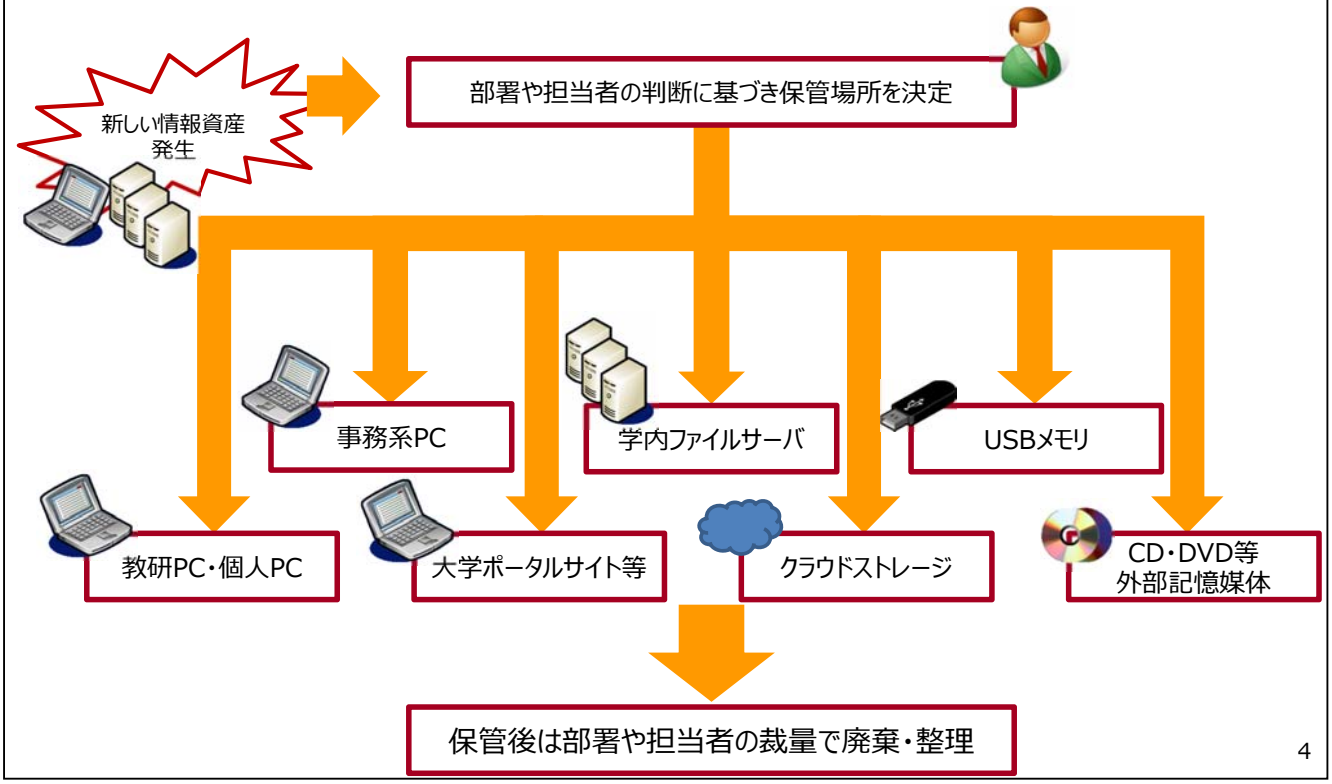
■ 人的・組織的対策

- 攻撃手法は日々高度化・巧妙化しており、技術的対策でマルウェア感染・感染拡大・情報流出等のリスクを「ゼロ」にすることはできない。
- リスクの最小化のために事務系システム利用者を対象に以下の人的・組織的対策も講じた。

✓ 標的型攻撃メール対策訓練・研修を通した利用者教育（毎年実施）
✓ **情報資産の取り扱いを定め、組織的に情報資産を把握・管理**

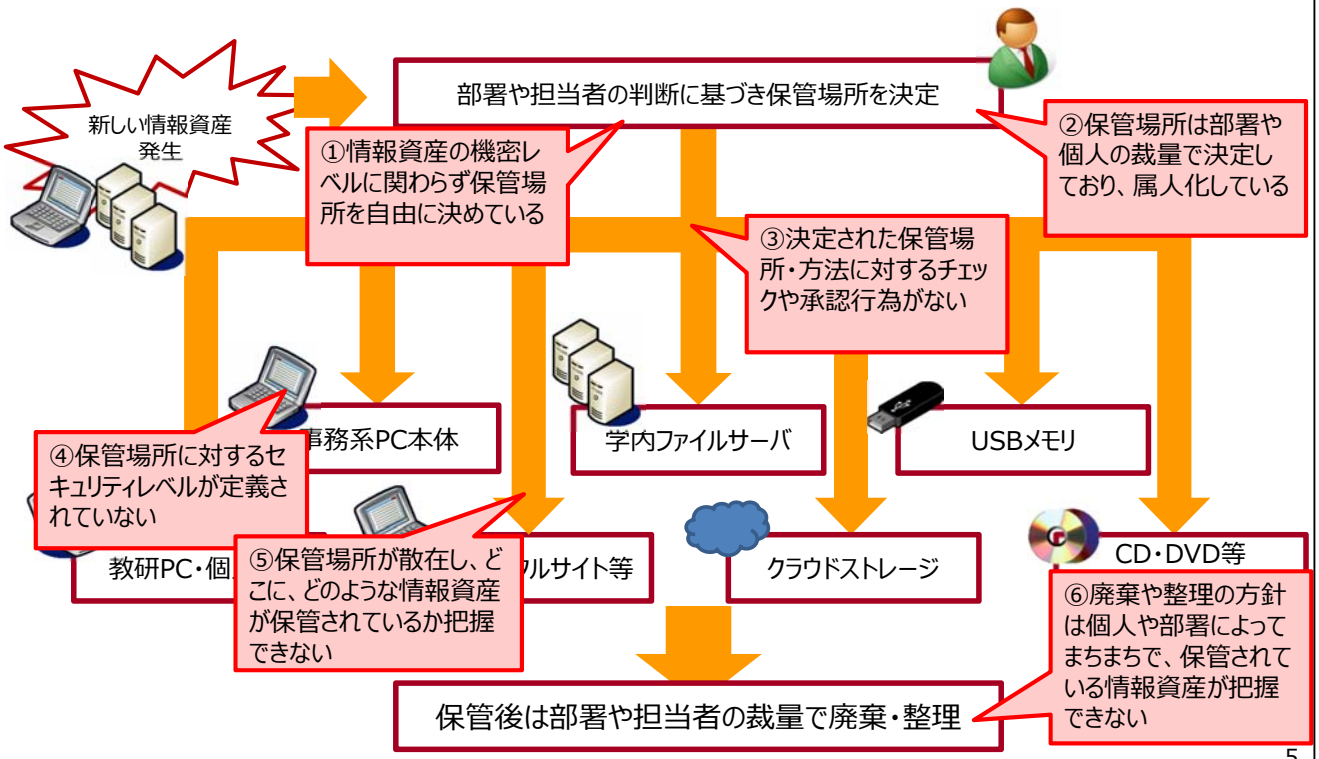
2．従来の情報資産の取り扱い状況

情報資産の管理方法について、明確なルールは存在しなかった。そのため情報資産が発生するたびに部署や担当者の裁量で自由に保管場所・方法を決めて管理していた。



2．従来の情報資産の取り扱い状況

技術的対策だけでは情報流出のリスクが高い。取り扱い状況を網羅的に把握できていないため、情報流出時に影響範囲の特定も出来ない。



3．情報資産管理ルールの制定

■ 従来の情報資産の管理・運用状況の問題点

- 機密レベルに応じて情報資産が保管されていないため、情報流出のリスクが高い。
- 情報資産の破棄・保管状況等、運用状況が網羅的に把握できていないため、情報流出時に影響範囲の特定が困難となっている。

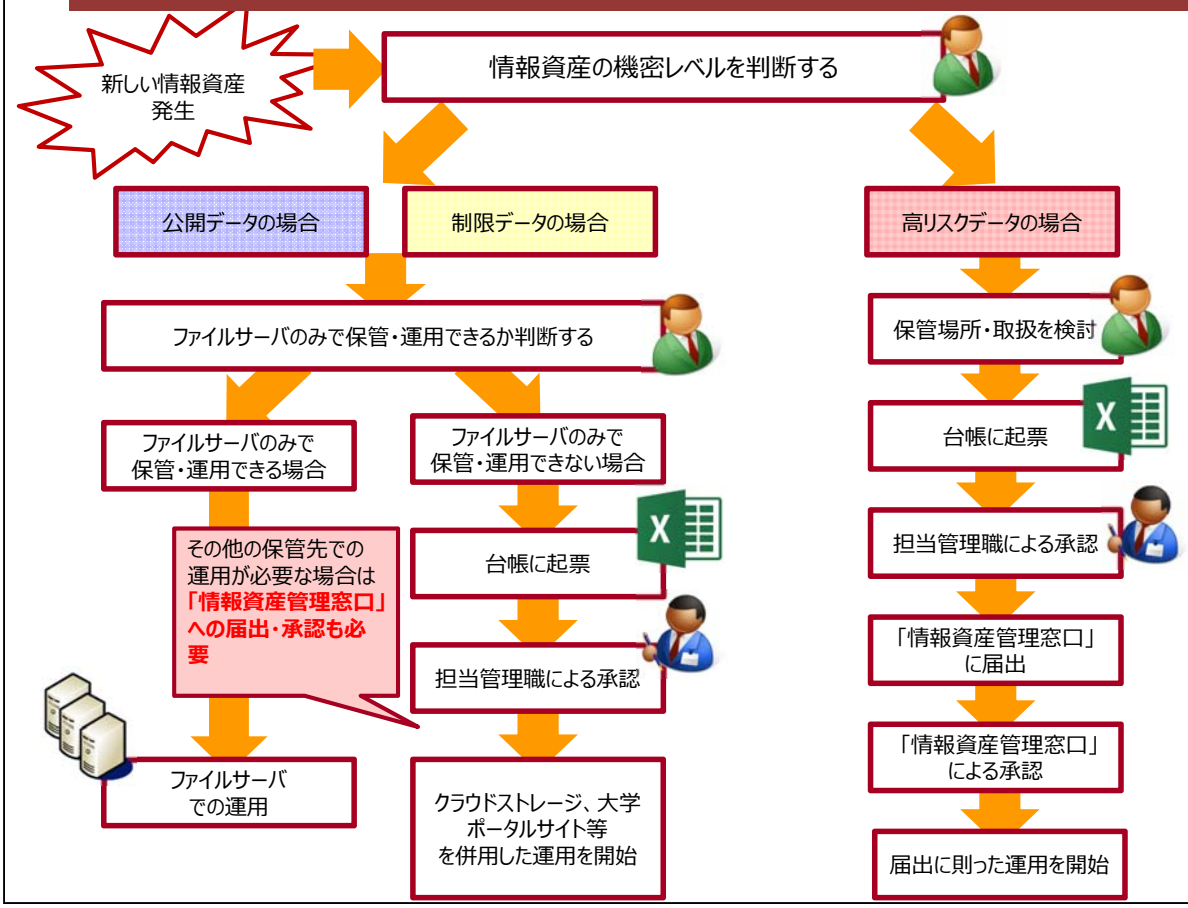
① 情報資産の機密レベルに関わらず保管場所を自由に決めている
② 保管場所は個人や箇所の裁量で決定しており、属人化している
③ 決定された保管場所・方法に対するチェックや承認行為がない
④ 保管場所に対するセキュリティレベルが定義されていない
⑤ 保管場所が散在し、どこに、どのような情報資産が保管されているか把握できない
⑥ 廃棄や整理の方針は個人や箇所によってまちまちで、保管されている情報資産が把握できない

■ 情報資産管理の対策・方針（2016年1月～）

- 情報資産の管理方法について要綱を制定する
- 情報資産の機密レベルを定め、保管場所と運用ルールを定義する
- 担当者、担当管理職、部署、管理検査チームによる管理検査を導入する

学内全体で継続的に情報資産を管理・運用する

4．情報資産の管理・運用フロー概要



4．情報資産の管理・運用フロー概要

■ 情報資産の機密レベル

- 機密レベルは**「高リスクデータ」、「制限データ」、「公開データ」**の3つに分類
- 高リスクデータは個別に保管場所および取扱いを定め、事前に情報資産管理窓口に届出、承認を得る

① 高リスクデータ

✓ データの保護が法律・規則によって要求されているもしくは機密性、完全性、可用性の損失が大学に重大な影響を及ぼす可能性がある。

✓ （例）クレジットカード情報、外為法の規制対象となる情報、出題前の入試問題、相談事項のうち、部署が必要と判断したデータ（ハラスメント防止・法務等の相談記録・報告書等）、公益通報関連データ。。等

② 制限データ

✓ データは一般に公開されておらず、機密性、完全性、可用性の損失は大学に悪影響を及ぼす可能性がある。

✓ （例）各種事務系システム内データ、業務情報（大学の規約、大学内部の業務情報、メール、非公開報告書、予算、計画、財務情報、教職員番号等）、教育情報（出席簿・採点簿・学生からの提出物等）。。等

③ 公開データ

✓ 高リスクデータ、制限データのいずれにも該当せず、すでに公開されているか、機密性、完全性、可用性の損失が大学に悪影響を与えないデータ

✓ （例）一般公開されているコンテンツ、教材、大学規則、方針、公募情報、公式な連絡先。。等

４．情報資産の管理・運用フロー概要

■ 情報資産の保管場所

- 保管場所は**「ファイルサーバ」、「クラウドストレージ」、「事務系PC」、「大学ポータルサイト等」**の４つに分類
- 上記以外の保管場所を利用する場合は**「例外的な保管場所」**として、個別に保管場所、取扱いを定め、事前に情報資産管理窓口に届出、承認を得る

①　ファイルサーバ

✓ 学外へデータ等を持ち出されたとしても暗号化対策により参照することが出来ず、セキュリティレベルが高いため、原則として、全ての高リスクデータ、制限データの保管場所とする。

②　クラウドストレージ

✓ セキュリティ設定や認証機能、利用者制限などセキュリティレベルは高いが、ファイル共有機能や公開機能を有することから、原則として高リスクデータ、制限データの保管場所としない。

✓ ただし、制限データのうち業務上必要がある場合（教員・学外への共有、ペーパーレス会議等）のみ、部署ごとの台帳に保管対象となるファイル群を記録し、担当管理職の承認を得たうえで、部署共有フォルダを保管場所とできる。

✓ 保管の際には、学内との共有なのか、学外との共有なのかによって共有範囲を適切に設定する。

✓ 不特定多数に対して共有する場合には、必ず共有設定有効期限およびパスワードを設定する。

③　事務系PC

✓ 作業のための一時的な保管場所とし、永続的な保管場所としない。

④　大学ポータルサイト等

✓ 教育利用のほか、会議資料や規約、学内向け各種マニュアル等の情報資産を、学生・教職員・校友と共有することを利用目的として保管場所とできる。

４．情報資産の管理・運用フロー概要

■ その他運用ルール

①　ファイル添付メールの送信禁止

✓ 誤送信（送信先の誤り、誤ったファイルの添付等）による情報流出の危険性があることからファイル添付メールの送信・転送は禁止とする。

✓ 事務系PC利用者はファイルサーバを利用し、事務系PC利用者以外はクラウドストレージを利用してファイルを提供する。

✓ ただし、相手方の事情によりクラウドストレージを利用した提供が出来ない場合に限り、台帳に起票し、担当管理職の承認のもとファイル添付メールを送付することができる。

②　学外への持出し

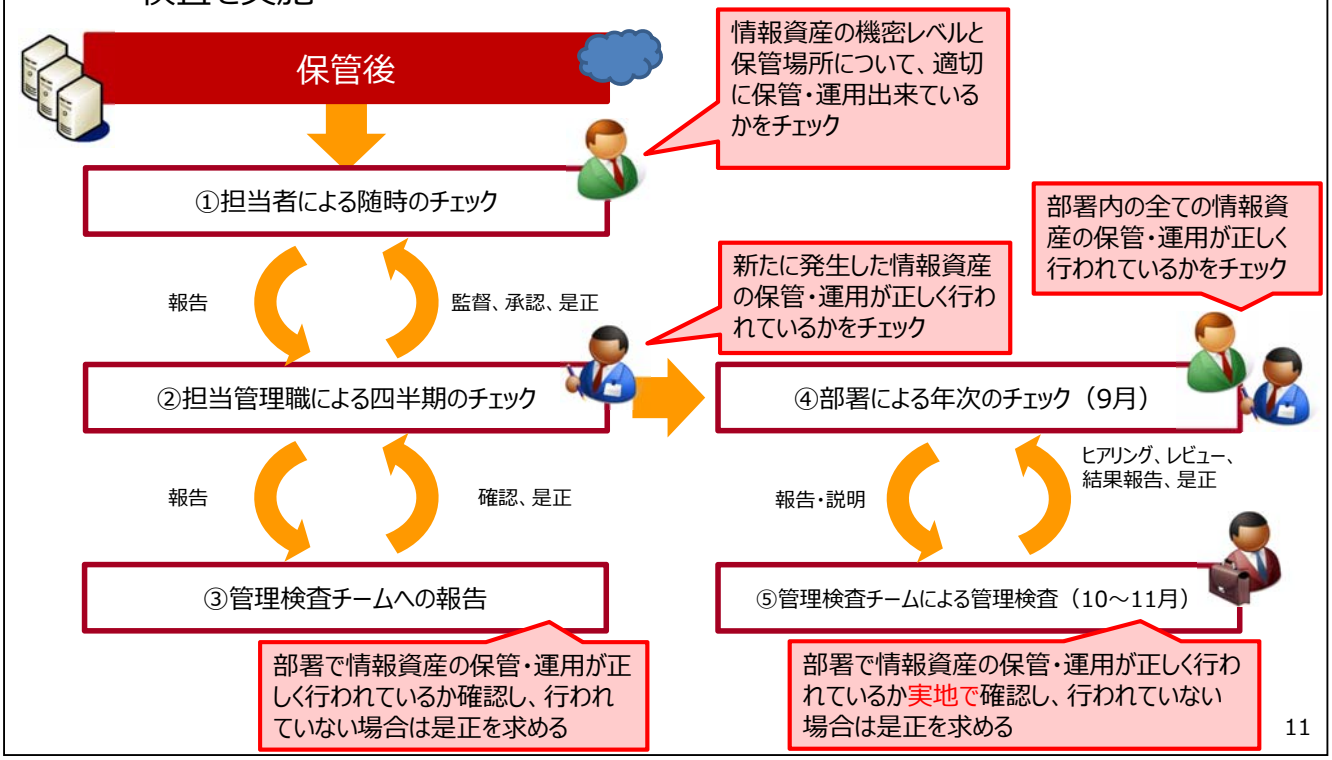
✓ 高リスクデータ、制限データを学外へ持ち出すことは原則禁止する。

✓ ただし、業務上、やむを得ず持ち出す必要がある場合は、事前に情報資産管理窓口へ届出、承認を得て持ち出すことができる。

４．情報資産の管理・運用フロー概要

■ 管理検査

- 情報資産の管理を適切かつ継続的に運用するため、4段階のチェックと管理検査を実施



ご清聴ありがとうございました。

本学の事例が皆様のご参考になれば幸いです。