



テレワークにおける 情報セキュリティを担保する ファイル管理システムの6要件

日鉄ソリューションズ株式会社
デジタルテクノロジー&ソリューション事業部

目次

1. テレワークにおけるファイル管理システムの要件	3
2. Boxを推奨する理由	10
3. Box導入による効果	11
4. Boxの安全性	12
5. 弊社の優位点	13

テレワークにおけるファイル管理システムの要件

テレワークにおける社内の様々な文書ファイルの利用においては、下記のセキュリティ対策および使い勝手の確保が必須要件になります。

1



ファイルのローカルへの保存や印刷禁止

2



メールのファイル添付を行わない

3



ユーザ権限管理を自動化

4



機密情報は多要素認証にする

5



文書毎のアクセスログ管理

6



ファイルサーバーと同等の
使い勝手を確保

1 ファイルのローカルへの保存や印刷禁止



オフィス外で社外秘以上の秘密文書は、ローカルPC内へのダウンロードや保存を禁止

- PCの置忘れや不正利用による情報漏洩事故につながるため、秘密文書はどのような環境でも、システム機能としてローカルPC内へのダウンロードや保存を禁止する



オフィス外での機密文書の印刷を禁止

- 印刷物は不正な複写や置き忘れなどの情報漏洩の危険性が高く、漏洩してもトラッキングできないため、システム機能として印刷できなくする

**文書ファイルの参照や編集の権限管理だけでは不十分
印刷不可、ダウンロード不可のコントロールができる文書管理システムの利用が必要**

2 メールファイル添付を行わない



関係者へのファイル送信や共有においてメールへのファイル添付は禁止

- 情報拡散や情報の所在が追えなくなるため、情報漏洩リスクが高い
- 外部のメールサーバを経由する場合もあり、情報漏洩リスクが高い
- メールに添付されたファイルによるウィルス感染の危険がある
- 誤送信による情報漏洩リスクが高い

関係者へのファイル送信や共有において、メールへのファイル添付はセキュリティリスクが高い
関係者への文書ファイルの共有や配信では、文書管理システムを利用する運用が必要



ファイルの公開範囲や秘密度により、利用者の所属や役割、役職に応じた操作権限をコントロールする

- 不要なファイルへのアクセスを禁止する
- 参照、編集、複写、削除などの権限をコントロールする

利用者の所属、役職、役割に対して、フォルダやファイルごとに操作できる権限（アクセス権限）を自動コントロールできる文書管理システムの利用が必要

機密情報は多要素認証にする



秘密度の高い文書や個人情報へのアクセス権限管理には、通常
のユーザ認証に加え、端末認証などを組み合わせるなどのより
厳しい対策を講じる

- 秘密度の高い役員会議資料や機微情報へのなりすましログインによる不正アクセスのリスク低減には、端末認証を組み合わせるなどの対策を講じる

秘密度の高い情報への不正アクセスをより高度に制御するには、端末
証明書による端末認証などを組み合わせ可能な文書管理システムの認
証機能を利用するのが有効



不正アクセスへの抑止のため、および漏洩拡大防止のためには、事故原因や不正内容の把握が必要である

- 秘密度の高い役員会議資料や機微情報へのなりすましログインによる不正アクセスのリスク低減には、端末認証を組み合わせるなどの対策を講じる

監査ログ記録は必須機能であり、ログは1年以上の保管が必要

6 ファイルサーバーと同等の使い勝手を確保



**通常使用しているイントラ内のファイル管理システムと同等の
使い勝手を確保する**

- 普段使いしている部門別ファイルサーバは セキュリティ対策上は脆弱である反面、参照、複写、編集などの操作性には優れる
- テレワークでは、ファイルサーバと同等のファイル参照や編集ができ、かつ前述のセキュリティ対策ができる必要がある

テレワーク環境では、ファイルサーバと同等以上の操作性とセキュリティ対策が両立する文書管理システムの利用が適す

Boxを推奨する理由

1. Boxは、前述の要件をすべて満たすクラウドコンテンツ管理サービスである。
2. パブリックなストレージサービスやファイルサーバでは、前述の要件を満たさない。
3. Boxは、米国政府機関でも採用されている高い信頼性や、導入実績が多数である。
4. Boxは、すぐに利用開始でき、スモールスタートが可能である。
5. Boxは、ワークフローシステムや、電子契約などのシステムとの連携可能である。



box



コンプライアンス
セキュリティ



- Officeドキュメント
- その他ドキュメント
- イメージファイル

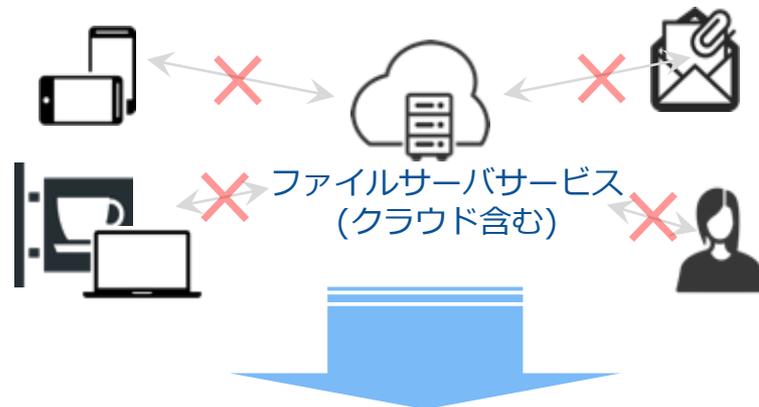
Box導入による効果

デバイスの制限

iPad等モバイルデバイスの活用に制限

場所の制限

ファイルサーバへアクセスできる環境に制限があるため、働く場所に制限がでる



社外からのメール添付制限

社内へのアクセスが制限されるため、ファイル保存先がローカルPCへ保存することが中心となる可能性がある

社内・外部メンバー間の共有制限

ファイルの共有にメール添付やUSB等の許可されていないデバイスなどを使用する可能性がある

Box活用により仕事の仕方が変わる

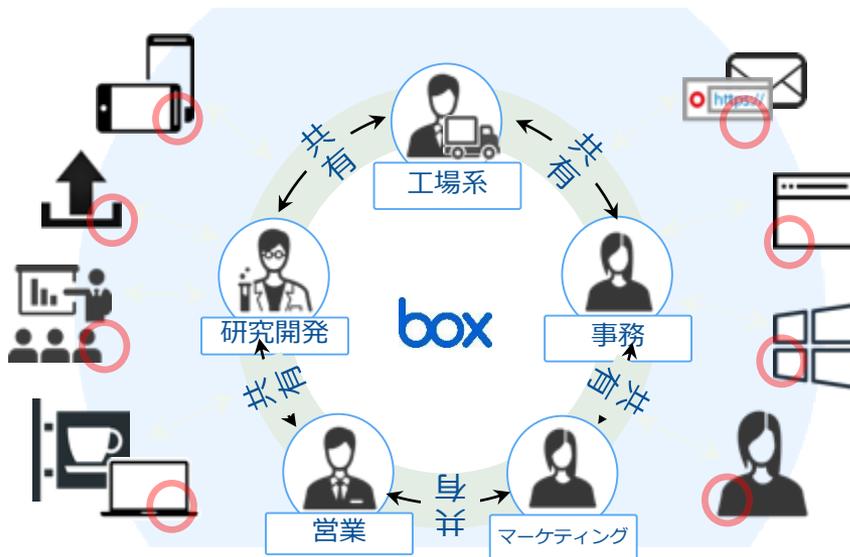
マルチ・デバイス

iPad等モバイルデバイスでのアクセス

FTP等ファイル転送の代替
大容量ファイルの保管・転送

会議資料のペーパーレス化
ビューア・Box Notes等を活用

どこでもオフィス化
カフェや自宅でのアクセス



メール添付ファイルの廃止
共有リンクによるファイル共有

新入社員ポータルとして
新入社員向けコンテンツを配布

Office 365/Salesforceとの連携
3rd PartyとのNative接続

外部協力会社との共有フォルダ
協力会社との共有が容易に

Boxの安全性

Boxは、様々な安全性基準の審査に合格しています。



ISO 27001
情報セキュリティとシステム制御に関する
国際標準に適合



PCI DSS 3.1 Level 1
サービスプロバイダとして最高レベルのコンプライアンス



ISO 27018
クラウド内の個人データ保護に焦点を
合わせた実務規範に適合



FedRAMP
クラウド製品やサービスに対するセキュリティ
評価、
認証、および継続的なモニタリングに関する
標準化規格



HIPAA and HITECH
PHI、PHRs、および医療のための
信頼されたプラットフォーム



SSAE16 Type II, SOC1 and SOC2
第三者機関によるテストと認証の取得



FINRA/SEC 17a-4
米国証券業界最大の自主規制機関



FIPS 140-2
機密情報を保護する暗号モジュールのセキュリティ
要件を規定する米国政府のセキュリティ
基準に適合

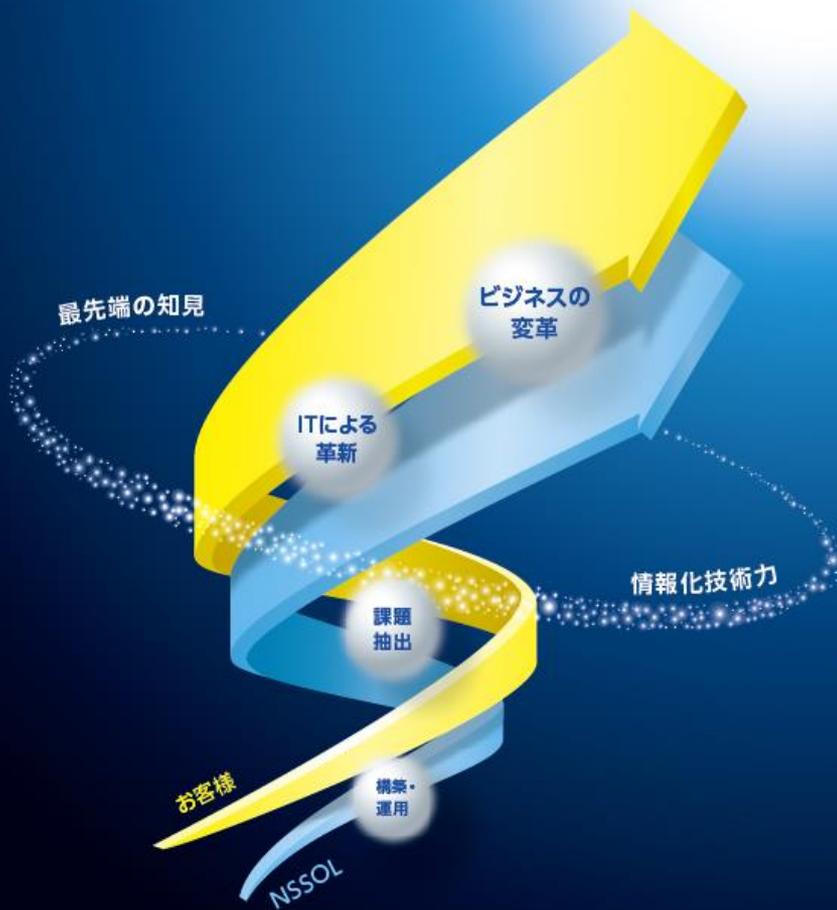
弊社の優位点

弊社は、自社での長年のテレワーク実施経験と 関連するツールやネットワーク環境構築・運用保守を数多くの実施してきた経験があります。

- ・ 国内トップクラスのIaaS,PaaS,SaaSの提供実績
- ・ 国内トップクラスのシンクライアントシステムの構築・運用実績
- ・ 国内トップクラスの数多くの文書管理システムの構築・運用実績
- ・ Boxとの各種連携サービスの提供
- ・ 20年間のクラウドサービス提供や導入経験



ともに、
その先の答えを



お問い合わせ先：

日鉄ソリューションズ株式会社
デジタルテクノロジー&ソリューション事業部

メール：dts-marketing@jp.nssol.nipponsteel.com

・ NS（ロゴ）、NSSOL、NS Solutionsは日鉄ソリューションズ株式会社の登録商標です。
・ その他本文記載の会社名及び製品名は、それぞれ各社の商標又は登録商標です。