2022年度 ISSスクエアシンポジウム

研究分科会成果報告

日本企業におけるＢＹＯＤ標準指針に関するガイドライン作成

2023年3月3日

マネジメント分科会

目次

1．マネジメント分科会の紹介

概要		マネジメント分科会では、技術的対策と組織的対策を統合するセキュリティマネジメントの観点から、様々な課題に対する具体的な対応策を明らかにすることを目指す	
メンバー	リサーチリーダー	情報セキュリティ大学院	稲葉 緑　准教授
	学生	情報セキュリティ大学院	新水 美代子 大村 篤生 岩下 央 孫 岳 中條　正志 及川 耕一 岡本 優 渡辺 雄太 稲田 陽一 西丸 真生

２－１．研究背景・経緯①

参加メンバーにて、以下の通りに検討候補テーマを挙げ、“技術的対策と組織的対策を統合するセキュリティマネジメントの観点から、様々な課題に対する具体的な対応策を明らかにすること”に資する今年度の研究テーマが何かについて、リモートワークの環境が広がる中、BYODを使う人がセキュリティ課題を守れない事例があるのではとの課題提起に対し各自が解決に取り組むべきテーマとして日本企業におけるＢＹＯＤの標準指針をテーマとし、検討を進めることとした

No.	テーマ案
1	日本国企業におけるセキュリティバイデザイン適用事例からみる課題と対応方針について
2	日本国企業におけるクラウドCoE設置事例等からみる導入課題と対応方針について
3	従業員の不注意によるルールや基準からの逸脱行動とそのリスクマネジメントの検討について
4	日本国企業におけるITセキュリティ人材の調達、育成にかかる状況と、現場にて要する人材数と実態の乖離、及びその補完について
5	社内ｸﾗｳﾄﾞｻｰﾋﾞｽ管理のﾍﾞｽﾄﾌﾟﾚｸﾃｨｽ検討及び企業目線からの企業のｸﾗｳﾄﾞｻｰﾋﾞｽにISMAPが導入されているのか
6	高度なばらまきメールの組織的対策について
7	機密情報保護の更なる保護策の検討及び機密文書の取り扱いルールのあるべき国内標準指針
8	データ越境移転の日本国内現状調査及びそれを踏まえた効果手的な対策について
9	企業としてのパスワードのあるべきガイドライン
10	誤った使い方の個人にあるべき正しいパスワードの使い方／啓蒙の在り方
11	BYODの企業利用ルールのあるべき国内標準指針
12	日本国政府からみたISMA制度運営に対しての課題・対応策
13	テレワーク環境におけるネットワーク関連の安全強度管理策
14	日本国企業の情報ｱｸｾｽ権限付与課題（最小権限原則が徹底されていない）、可用性の観点からも、よりよいﾊﾞﾗﾝｽ

２－１．研究背景・経緯②

NIST SP800-114、地方公共団体における情報セキュリティポリシーに関するガイドライン、その他研究事例を参照し、技術的安全措置については整ったガイドラインが整備されていることもあり、組織的安全管理措置・人的安全管理措置の２面に関するカテゴリに関するものを対象とし、ガイドライン案を作成・整備することを通じ、各自の知見を高めることを狙いとした

No.	目次		補足　※以下は執筆担当割時の案で、ガイドライン作成中に一部統廃合等したものあり
1	はじめに		本標準指針の背景や目的、前提、想定読者等を示す
2	BYODの形態		BYODを２種類のデバイスに分類し、各形態のセキュリティ等の留意点について示す（テレワーク形式との関係性も参考に示す）
3	BYOD導入にあたって検討すべきこと		BYOD導入にあたってのメリットデメリット、BYODの適用範囲定義の重要性、特にアンコントロールとなるリスクを明確に示し、経営レベルで判断すべきことを示す
4	BYODにおけるガバナンス	ガバナンス・リスク管理	BYOD実施に当たって生じるせキュリティポリシー（基本方針）の見直しの観点を示す
5			BYOD実施に伴うセキュリティ対策実施に必要となる組織・人材の組成と予算の確保を行う必要性の観点を示す（従来の延長戦では解けないことが何なのかをわかってもらうための章）
6			ガバナンス・リスク対策の継続的な見直しの必要性を示す
7		データ保護	BYODにおける情報取り扱いに関する取扱いの必要性の観点及び、私物情報と会社情報の峻別・分離対策の必要性を示す
8		インシデント対応・ログ管理	BYOD導入の際の企業におけるインシデント対応計画見直し観点を示す
9		ルール	BYOD利用ルールの観点を示す　利用範囲（方針、適用業務、取扱情報）、利用申請手続き、企業NW接続時の禁止点・留意事項、BYOD機器管理　等
10		教育・人事労務	セキュリティ研修におけるBYOD遵守事項の組み込みの必要性、人事労務制度関係（勤務管理、懲罰関係等）の見直しの必要性・観点を示す。従業員プライバシー配慮も示す

２－２－１．指針の適用範囲・前提

１．デバイスの種類および適用範囲

デバイスの形態は以下２種類に限定する。またこれらデバイスの総称をBYODとする。
①個人所有のPC（以下：個人PC）
②個人所有のスマートフォン、個人所有のタブレット
(以下、個人スマートフォン、個人タブレット)

また、適用範囲は原則として、以下のBYODの利用組織、個人としての利用者とする。
・組織：国内の一般企業・組織・団体
※組織では、オフィスおよびリモートのハイブリッドによる業務形態
・利用者：上記組織で業務する従業員（役員・一般社員・派遣社員・パート）

なお、適用範囲の決定においては、各組織の業務形態および、従業員の役職・雇用形態によって利用方法が異なることを想定し、ガイドラインの内容が煩雑とならないように、組織ごとに策定することを重要視し決定できるものとする。

２．各デバイスのセキュリティに対する留意点

１．盗難・紛失による情報漏洩
２．第三者による不正ログイン
３．BYODにおけるウイルス対策
４．私用・業務利用の境界線の明確化

２－２－２．ＢＹＯＤ導入に当たっての検討事項

組織ごとにBYODに導入に向けた検討を行うため、一般的な課題やメリット・デメリットを示し、
それらの解決策・事例を理解しておくことで、検討を促進の支援につなげる。

１．BYODのメリット・デメリット

メリット	説明
企業の端末購入・維持コスト抑制	私物端末を利用により、企業・組織側の端末購入コストや維持費を抑えることができる。
業務効率向上	使い慣れている端末を使用することで、従業員の業務効率が向上し、労働時間短縮や生産性向上、ひいては売上や利益の増加につながる。
従業員満足度（ES）向上	私物端末で仕事ができれば複数の端末を持つ必要がなく、使い慣れたデバイスで操作面でもストレスが少なく、従業員満足度の向上が期待できる。
テレワーク等の多様な働き方スタイルの導入	テレワーク（在宅勤務・リモートワークなど）でBYODが導入されていると、適切な管理、活用が進められ、多様な働き方のスタイルを効率的に取り込める。
「シャドーIT」の抑止	BYODを導入し、整備されたルール下でデバイスを適切に管理することにより、未許可の私物端末を使う必要がなくなる、企業内の「シャドーIT」が抑止につながる。

デメリット	説明
情報漏えい等セキュリティリスク	私物端末は、利用場所、アプリ種別、インターネットのアクセス先等が広範囲に亘るため、結果として情報漏えいのセキュリティリスクが高まる。
労務管理の複雑化	私物端末を利用すると時間や場所を選ばず業務を遂行することが可能となる反面、仕事とプライベートの境界線がつけにくく、労務管理が複雑化する懸念がある。
運用ルールの徹底やセキュリティ教育の負担増加	BYODの導入にあたっては、運用に必要となるルールの設定や、そのルールに関する教育も必要となる。企業規模が大きい場合、適用範囲が広がる可能性もあり、運用ルールの徹底するためのコストも膨大となることも考えられる。

２．BYODの導入にあたって考慮すべき点

BYOD導入におけるメリット・デメリットから、導入に当たって考慮すべき点を示す。
ここではガバナンス、マネジメントの観点から「運用面」「教育面」「労務面」の３つの観点で示す。

①運用面

社内ガイドラインの設定で運用を明確化

利用する端末の範囲や用途、どこまでの情報を保護するかといった企業ポリシーに沿ったガイドラインを設定することが重要である

わかりやすくシンプルな運用ルール

ガイドラインの設定と合わせて、運用ルールはわかりやすくシンプルなものにすることを心掛け、実際の円滑に運用されるものでなければならない。

②教育面

セキュリティ意識の向上

情報漏えいを防ぐためには、リスクを従業員自身が強く意識し、その企業のセキュリティポリシーを十分理解し、日々の運用を徹底できるような教育が必要

③労務面

就業規則への反映

BYODで在宅勤務を行う場合の残業時間管理や申請プロセス、私物端末利用やその費用負担等、BYODに関する就業規則への反映が必要となる場合がある

グローバル展開企業での導入

BYOD導入にあたっては事前に、国ごとの法律を事前に把握し、その国での導入の是非を判断する必要がある。

２－２－３．ガバナンス・リスク管理①

（１）情報セキュリティ関連規程修正観点

情報セキュリティポリシーは、事業内容や扱う個人情報の種類、社内ITインフラ環境などの違いによって、適切なセキュリティ対策も異なるため、企業の状況に見合った内容である必要がある。

1.利用開始前
BYODを新たに導入する場合、情報セキュリティポリシーの業務で利用する情報機器などの項目に「私有ＩＴ機器の利用」についての項目を追加する。

2.利用開始時
利用を開始する前に利用する本人が以下を実行する。
・情報システム管理者が指定するウイルス対策ソフトウェアをインストールし、定義ファイルを更新する。
・業務に支障が出る可能性があるソフトウェアを削除する。

3.利用期間中
利用期間中は、利用するＩＴ機器に以下に該当する機能がある場合には実行する。
・ウイルス対策ソフトウェアの定義ファイルを常に最新版に更新する。
・OSやアプリケーションソフトのアップデートが通知されたら速やかに実施する

4.社内での利用
利用期間中にＩＴ機器を社内に持ち込む場合は、情報システム管理者の許可を得る。

5.利用終了時
利用を終了する際には、情報システム管理者が指定するツールを使用してＩＴ機器業務で利用したデータを完全に消去し、復元できない状態にして情報システム管理者の了解を得る。

(2)BYODにおける利用ルール

BYODを行うにあたり、企業はBYODの利用にかかるルールを適切に定めなければならない。また、定めたルールを須らくBYODを実施するユーザー並びにその責任者に周知し、認識させる必要がある。ルールの内容は継続的な運用管理を見据えたルールである必要がある

1. BYODの利用範囲
✓ 企業はBYODにて業務を行うことのできる範囲を明確に定める。定めた範囲をユーザー等に周知し、認識させるべきである
（適用業務/対象範囲）

2. BYODの利用申請手続き
✓ 企業はBYODの実施状況について把握する必要がある
（利用申請及び同意事項 / 適用業務と取扱情報の内容）

3. 企業NW接続時の禁止点･留意事項
✓ 上記の禁止点や留意事項をまとめ、周知する必要がある

3. BYOD機器管理
✓ 申請情報を集約して管理し、時にチェックする必要性がある
（ユーザー部署による管理台帳の作成と管理 / BYOD管理部署による集約管理）

２－２－３．ガバナンス・リスク管理③

(３)BYODにおけるセキュリティ対策のための資源（予算、教育等）確保

BYODについて安全安心に導入・利用するにあたっては、従来のセキュリティ対策に加え、BYOD自体への固有セキュリティ対策追加が望ましく、その為の資源確保が必要。予算確保に当たっての実施事項例は以下の通り

対象層	実施事項
経営層	・BYODに関する必要なセキュリティの事前対策を明確化、それに要する費用やその他リソースを明らかにするよう、セキュリティ担当へ指示 ・セキュリティ運用や、教育を実施するにあたり、要員の増加が必要な場合は、企業内の人事部門に対する人員調達の調整・企業内異動に関する手続き実施 ・自社内でBYOD研修の計画化・資料策定・研修完結実施が困難な場合は、専門ベンダーの活用を検討、外部委託費用確保 ・企業内の意思決定会議・決裁プロセスにて、セキュリティ対策・教育対策の内容に見合った適切な費用かどうかを評価した上で、予算として承認
セキュリティ担当	・BYOD導入範囲・利用者・取扱情報・企業システム接続箇所等を明確化の上、端末・接続対象システムのリスク特性を洗い出し ・リスクに対する安全対策の目標を定め、必要となる安全対策基準・対策の選択を実施 ・安全対策の目標に対し、安全対策の費用対効果、対策に関する費用対効果、それぞれが最大となる経営資源配分を考慮し、最終的に安全対策を決定 ・最終決定された安全対策措置を行うにあたり必要となる予算見積 ・想定するリスクを踏まえ、必要に応じてコンティンジェンシープランを策定する ・上記内容について経営層へ協議・報告の上、合意を取り付け

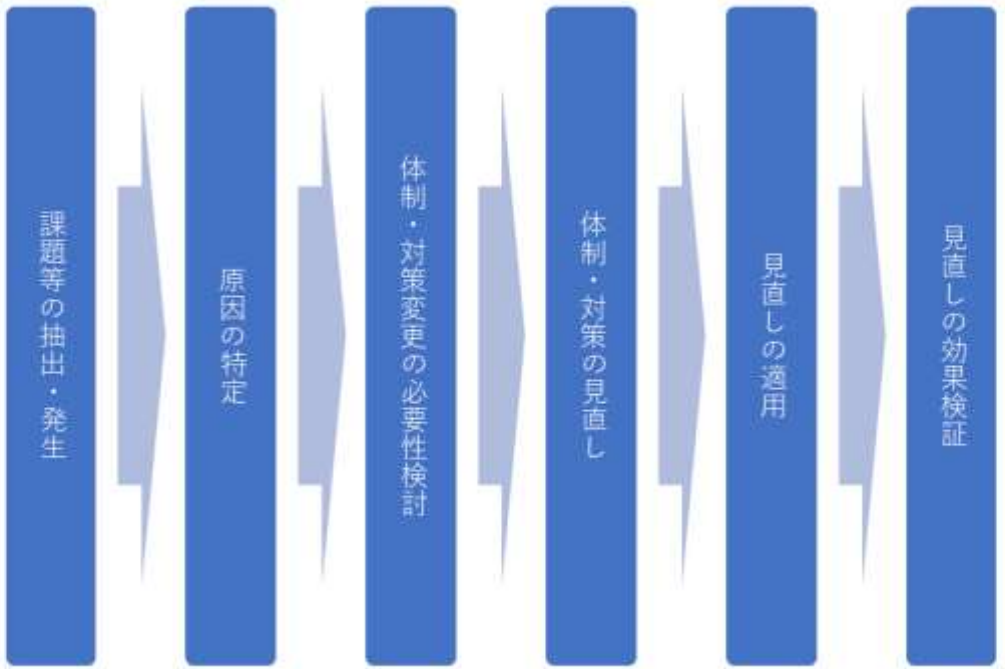
2－2－4．ガバナンス･リスク対策の継続的な見直し

- ガバナンス/リスク対策は，制定後も更新が必要
  →見直しの要因）自社が置かれた状況の変化，技術の進歩，etc.

- 定期的および随時の見直しが可能
  →定期：緩やかな状況変化に対応．ガバナンス体制&リスク対策の見直しにも
  →随時：インシデントや急激な状況変化に対応．顕在化した問題の見直し

- 実際に見直しが行われることが重要
  →更新のプロセスを規程しておくことで見直しを担保

- 見直しプロセス



２－２－４．ガバナンス・リスク対策の継続的な見直し

- 成熟度モデル
  - きちんと見直しができる体制であるか否かを検討するために，CIIMに類したプロセス成熟度の概念を導入した
  - 必ずしもレベル5を目指すことが目的ではなく，自組織の目的とする成熟度とのFit-Gap分析に有効

レベル1	継続的見直しが明文化されておらず，実行されていない
レベル2	継続的見直しが明文化されていないが，実行されている
レベル3	継続的見直しは明文化されている
レベル4	継続的見直しが明文化されており，実行されている
レベル5	継続的見直しが明文化され，明文化された見直し期間・方法がレビューされており，見直しプロセスの継続的な改善が可能になっている

２－２－５．データ保護

BYOD導入により企業統制環境外で重要データを取り扱うことがあり得る場合、本来は統制外であるが、統制外領域（従業員のプライベート領域）でデータを保護するために、そのデータ保護を図るための措置が必要。検討観点・対策例は以下の通り

	検討観点	対策例
従業員プライベート領域におけるデータ取扱範囲の極小化	データ取扱範囲・要領	・端末にデータを持たせない ・BYOD端末での取扱データの絞り込み ・機密性の高いシステムは利用不可とする ・機密性の高い機能は利用不可とする
従業員プライベートデータと企業管理データの隔離	従業員プライベートデータと企業管理データの分離要領	・MAM（Mobile Application Management）の導入・運用 ・分離ルールの統制
紛失・盗難対策	紛失・盗難に対する情報漏えいリスク考慮、盗難・紛失時におけるデータ保護策	・暗号化・パスワードの設定 ・MDM（Mobile Device Management）の導入・運用
ルール遵守	ー	・①データ取扱範囲②データ分離③盗難・紛失等に関するルールの策定・徹底 ・誓約書を徴求、誓約書の徴求前に研修受講を義務化、誓約の形骸化防止のため継続的に教育研修

2－2－6．インシデント･ログ管理

（1）インシデント対応

従来のインシデント対応フローにおいて，再検討すべき事項

① リスクの洗い出し

（例：盗難・紛失による情報漏洩，第三者による不正ログイン，ウイルス感染など）

② インシデントの検知手法，対応手法，復旧方法について検討

③ インシデント対応計画の策定

④ インシデント発生時の連絡手段や窓口の確認または整備

リスク分析シート

リスク	検知	対応	復旧
端末の紛失・盗難			
端末のウイルス感染			
社内システムへの不正アクセス			
：			

（2）ログ管理

ログ管理において，検討及び留意すべき事項

- 必要となるストレージの試算及び古いストレージを初期化するタイミングの検討
- BYOD端末がそのほかの社内システムと同一のタイムラインでログに記録するよう設定する
- ログにおける管理者権限の使用等，定期的にログの確認を実施する.
- 不審なログに対する自動アラート通知機能の導入

２－２－７．人事労務・教育

１．人事労務

従業員が業務で私用端末（BYOD）を利用するにあたって、業務を脅かす使用、過剰な利用、業務システムへの接続とデータの取得について制限がなされなければならない。

①従業員はBYODポリシーに従うことについて書面で同意する

②ポリシーはその対象者が容易に閲覧できる場所に保管する

２．教育

BYOD利用者は正しい利用を遂行するために必ず適切な時期に適切な教育を受けなければならない。

①トレーニングの種類

・初回トレーニングの実施（アクセス権限毎のトレーニング）

・定期的なトレーニングの実施（ユーザー用研修、マネージャ用研修）

②トレーニング

・トレーニングは必ず記録を残さなければならない

・BYOD研修内容には以下を含めること

利用のルール・手続き, 情報セキュリティ, 利用範囲, 私的利用の制限, 登録・設定,リスク管理, 費用負担及び補償・保険, 手順 (問題発生時の報告, 業務または業務外における外出時の取扱い, 紛失時, 緊急事態時, 離職・退職時, 懲罰)

３．まとめ

日本企業におけるＢＹＯＤ標準指針

目次

御清聴、有難うございました