Internal

ビジネスパートナー向け
情報セキュリティガイドライン

Version 3.2
メルセデス・ベンツ日本株式会社
IT部
Aug 10, 2022

Mercedes-Benz

更新履歴

Update date	Update Contents	Ver.	Editor
2015.01.05	• 新規作成	1.0	MBJ IT
2017.12.25	• 最新のセキュリティ事件・事故対応ふまえ5章、6章、7章を追記	2.0	MBJ IT
2021.01.15	• 全体をレビューし、必要箇所を更新 • 管理者向けのセキュリティ対策強化のため、3章「情報セキュリティのための組織・体制」を8章内へ移動 • P39, P46, P47, P51, P53を追加 • 付録にダイムラーのWebMailツールについて追記 • 本ガイドラインに関するお問い合わせ先変更	3.0	MBJ IT
2021.03.31	• 6.4) 社外から社内ネットワークへのアクセスの追記 • 6.5) 在宅勤務要件の追記 • 7.11)システムへのアクセスと認証の文言修正	3.1	MBJ IT
2022.08.10	• 社名変更に伴いダイムラー社からメルセデス・ベンツ社に記載変更 • 販売店基準の必須項目に関する記載を追加 • サービスデスクの連絡先の変更 • ウイルス対策のソフトウェア（例）を更新	3.2	MBJ IT

目次

1. 本ガイドラインについて

1. 本ガイドラインについて

1）目的

本ガイドラインは、メルセデス・ベンツ日本株式会社のグループ企業（以下、MBJグループという）と取引を行うビジネスパートナー（販売店、認定サービス工場など含む）が 、**情報資産を適切に取り扱うための規準・行動指針を定めたもの**です。MBJグループにおける情報セキュリティのポリシーおよびスタンダードに準拠しており、特に物理的安全管理措置と技術的安全管理措置について定めています。

販売店契約上、本ガイドラインはビジネスパートナーに遵守いただくべき文書の一つとして位置づけられており、「必須項目」と記載された項目については、販売店基準の必須項目となります。なお、ガイドラインに修正・更新が発生した場合は、ビジネスパートナーより案内された時点から更新版が有効となります。

2）適用対象者

本ガイドラインは、**ビジネスパートナーとしてメルセデス・ベンツビジネスに関わる全ての企業、及び全ての個人に適用**されます。ビジネスパートナーの皆さまには、自社の情報セキュリティ活動の推進にあたり、このガイドラインを活用ください。

3）免責事項

本ガイドラインに起因してビジネスパートナーに生じるいかなる費用・損害からも、MBJグループとその親会社であるメルセデス・ベンツ社は免責されます。

2. 情報セキュリティ基礎

2. 情報セキュリティ基礎

1）基礎知識（1/2）

情報セキュリティ対策とは

「情報」は「ヒト」、「モノ」、「カネ」と同様に企業活動を継続する上で重要な経営資産の1つです。
「情報セキュリティ対策」とはこの「情報」を漏えい、改ざん、破壊などの脅威から保護することです。

情報セキュリティ対策の必要性

情報システムは業務効率を高める反面、大きなリスクも持ち合わせています。
適切な情報セキュリティ対策を怠った場合には、不正アクセス被害、機密情報/個人情報の漏えいといったセキュリティ事故が発生する可能性があります。

その結果、顧客情報の漏えいによるMBJブランドのイメージダウン、情報システム停止による損失などが発生し、お客様、MBJグループ、ビジネスパートナーに大きな被害や影響をもたらします。

このようなリスクを軽減するためには、本ガイドライン記載の情報セキュリティ対策の実施が必要です。

2. 情報セキュリティ基礎

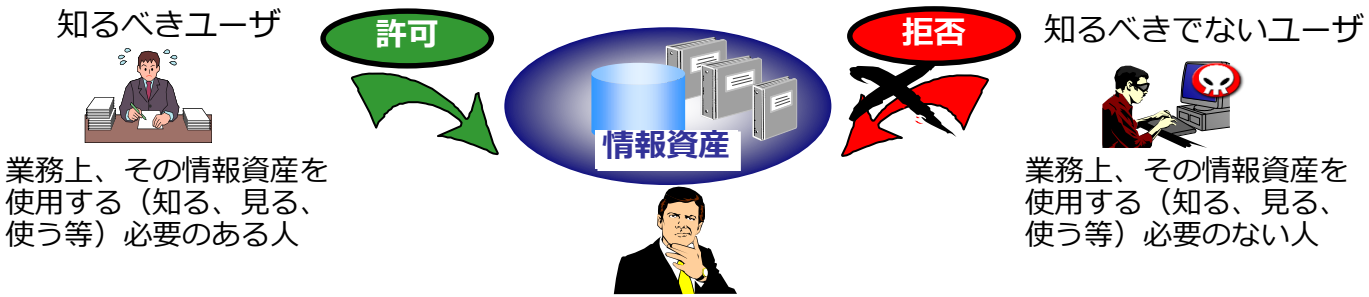
1）基礎知識（2/2）

情報資産とは

本ガイドライン適用対象者が守るべき「情報資産」とは、メルセデス・ベンツ ビジネスで発生、および取り扱われる全ての情報を指します。情報の記録方式や媒体は問いません。

情報セキュリティの基本原則

情報を開示する範囲はその情報を知る必要のある人に限定してください。
これを「Need to Know」（知る必要）の原則と呼びます。



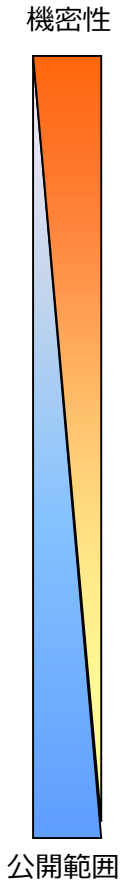
情報資産の責任者（情報オーナー）が決定

2. 情報セキュリティ基礎

2）情報資産区分

情報資産は機密性の観点から4種類に分類されます。この区分は情報オーナーが決定します。
それぞれP10以降に示す区分に応じた管理を実施してください。

※ Internalより上位区分の取り扱いには、下位区分の取り扱い注意点も含まれます。



区分	漏えい インパクト	例	ラベリング	暗号化
Secret （極秘）	重大	•マーケティングあるいは財務戦略に関する情報 •重要な組織改変情報	必須	必須
Confidential （機密）	大	•発表前の価格情報 •従業員・顧客の個人情報 •他社との業務提携にかかわる情報	必須	必須
Internal （社外秘）	限定的	•トレーニング資料 •一般的な電子メール文書	推奨	不要
Public （公開）	なし	•インターネットウェブサイトに公開する情報 •リリース済み製品情報	不要	不要

※ ラベリング、暗号化の方法は、付録を参照してください。

2. 情報セキュリティ基礎

3）情報資産区分に応じた情報の取り扱い（1/2）

Internal （社外秘）の取り扱い

以下を考慮してください。

- ✓ 情報は本来目的とする業務にのみ利用する。
- ✓ 情報は、業務遂行上その情報を必要とする人にのみ提供する。
- ✓ 無許可で情報の社外持ち出しをしない。
  - – 情報を私用メールアドレスに送信しない。
  - – 情報を私用のインターネット上のサイト（クラウドサービス など）で保管しない。
  - – 情報をソーシャルメディア（Facebook, Twitter, LINE など）上に掲載しない。
- ✓ 口頭での取り扱い：電話、会話などで内容が周囲に漏れないよう配慮する。

Confidential （機密）の取り扱い

Internalに区分される情報の取り扱い要件に加え、以下を考慮してください。

- ✓ 個人に関するデータは原則として機密扱いとする。
- ✓ 情報区分が明確になるようラベリングを施す。（最初のページおよびスクリーンに明示）
- ✓ 情報をプリンタ出力、コピーする際は、出力機器の前で立ち会う。
- ✓ 使用中の情報の印刷物は机上、ファックスなどに放置しない。
- ✓ 電子的に保管・受け渡しする際には必ず暗号化する。
- ✓ 使用しなくなった（有効期間を過ぎた）情報はシュレッダーなどで安全に廃棄する。
- ✓ 雑居ビルのエレベーターホール、鉄道車内、レストランなどの公共の場では、機密情報に関する会話をしない。
- ✓ 外部記憶媒体に情報を保存する場合はセキュアUSBを使用する

2. 情報セキュリティ基礎

3）情報資産区分に応じた情報の取り扱い（2/2）

Secret （極秘）の取り扱い

Confidentialに区分される情報の取り扱い要件に加え、以下を考慮してください。

- ✓ ラベリングを施す。（全てのページおよびスクリーン上に明示する）
- ✓ コピー機等によってハードコピー（書類）を複写しない。
- ✓ 電子データの複製はバックアップの目的に限定する。
- ✓ セキュリティが厳重に確保されている場所にて保管する。
- ✓ 外部記憶媒体に情報を保存する場合はセキュアUSBを使用する

3. PC、モバイル端末等の取り扱い

必須項目

3. PC、モバイル端末等の取り扱い

1）ID・パスワードの管理（1/2）

IDの管理

■ IDの改廃

異動・退職等によりID改廃が必要になった場合は、速やかにID変更・削除申請をしてください。

ID変更・削除申請は遅くとも、異動・退職後7日以内に実施してください。

■ 共用IDの禁止

複数人で同一のIDを利用しないでください。1人1 IDを申請してください。

パスワードの管理

■ パスワードの取り扱い

パスワードの窃取などによるシステム不正アクセスなどを防止するために、パスワードの取り扱いにおいて下記の点に留意ください。

- ✓ パスワードは他人に教えないこと。
- ✓ パスワードを記載したメモをディスプレイなど他人の目にふれる場所に置かないこと。
- ✓ パスワードをメール共有する場合は、テキストファイルにパスワードを記載し、本ガイドライン付録の「暗号化の方法」で紹介している方法で暗号化して受け渡しをすること。

■ パスワードのリセット

- ✓ パスワード漏洩の可能性がある場合には、速やかにパスワードのリセットをしてください。

3. PC、モバイル端末等の取り扱い

1）ID・パスワードの管理（2/2）

■ 安全なパスワードの設定

原則、以下のルールに則して、他人に推測されにくいパスワードの設定をしてください。
簡単なパスワードを設定した場合、容易に予想されてしまう為、第三者による不正利用のリスクが高まります。

- ✓ パスワードの長さは**10文字**以上。**大文字・小文字・数字・特殊文字**の中から少なくとも3種類、できれば4種類全て用いて作成してください。
- ✓ 簡単に予想できるものは避けてください。（名前+生年月日、等）
- ✓ パスワードは少なくとも**90日に1回**は変更してください。
- ✓ 過去12回のパスワード変更の中で使用されたものは利用を避けてください。

パスワードの作成方法について、下記の通り一例を示します。

step	手順例	結果
1	最低10文字以上のフレーズを選択する	wagahaiwa nekodearu
2	ひらがな1文字分の文字列毎に1番目のアルファベットを抜き出す	wghiwnkdar
3	普通文字を数字と特殊文字に変換する 例として、“a”の文字を”@”に変換する その他の例： i→1→!，z→2，e→3， s→5→$， o→0， a→@	wgh1wnkd@r
4	大文字を含める 例として、小文字”w”を大文字に変換する	wgh1Wnkd@r

3．PC、モバイル端末等の取り扱い

2）画面ロック

わずかな時間であっても、PCから離れるときは画面の情報を関係ない人に見られないように、
画面ロックをしてください。
これにより、他人が盗み見たり操作することを防ぐことができます。

～画面ロックとは～

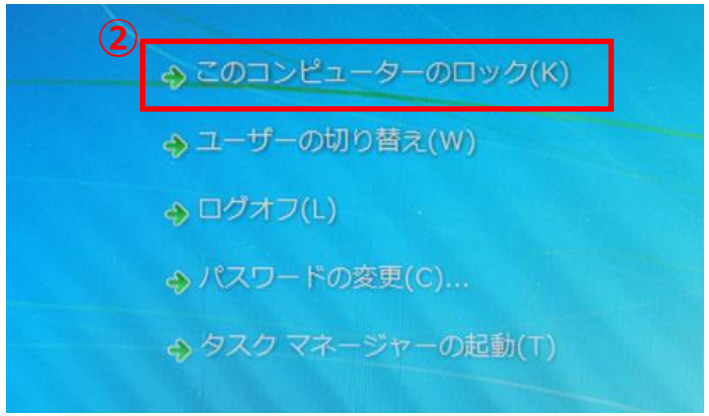
IDとパスワードを入力しないとPCを使えないようにする機能

①キーボードの”**Ctrl**”、“**Alt**”、“**Delete**”ボタンを同時に押します。

②**”このコンピュータのロック”**のボタンを押します。

③コンピュータがロックされます。

④コンピュータを使用する時に、再度“**Ctrl**”、“**Alt**”、“**Delete**”ボタンを同時に押し、ユーザ名とパスワードを入力します。



3．PC、モバイル端末等の取り扱い

3）PC、 外部記録媒体の持ち出し

■無断持ち出しの禁止

- ✓ 会社のPCや外部記憶媒体（USBメモリ、CD, DVD等）を無断で社外に持ち出してはいけません。
- ✓ PCや外部記憶媒体を持ち歩いた場合、盗難や紛失により会社の情報が流出する可能性がありますので、下記を徹底してください。
  - 持ち帰る必要がある場合には、上司の許可を得てください。
  - 外出時はPCをシャットダウンしてください。

■外出時のモバイル機器の管理

- ✓ モバイル機器は、目の届くところに置いてください。飛行機に乗るときは、荷物として預けずに、手荷物として機内に持ち込んでください。
- ✓ モバイル機器が盗難にあった場合には、ただちに上長/オペレーションセンターに連絡をしてください。

4）PCの安全な取扱い

■PCの管理

- ✓ PCは退社時、離席時には施錠された場所（引き出しやキャビネット等）もしくはセキュリティワイヤで固定して使用するなどして盗難に注意してください。

3．PC、モバイル端末等の取り扱い

必須項目

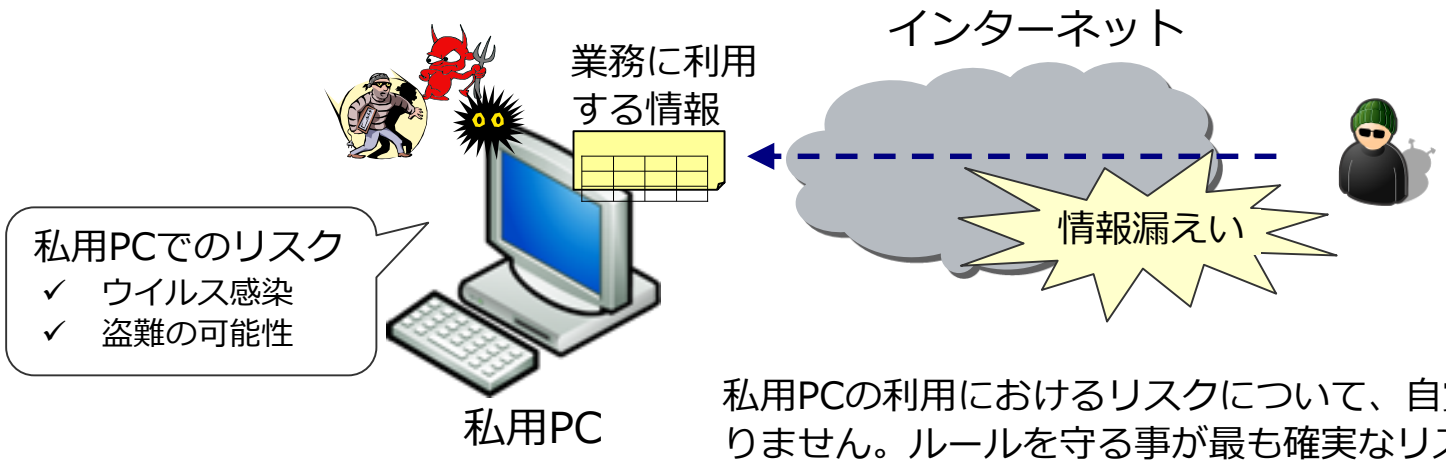
5）私用のITデバイスの取り扱い（１/2）

■会社から貸与されていない、もしくは使用許可を得ていないPCや外部記憶媒体（USBメモリ、CD、DVD等）は社内外問わずいかなる場所でも業務で使用してはいけません。

■私用PCを業務で使用した時の危険性

✓ セキュリティ上の脅威があり、情報漏えいを引き起こす可能性があります。

＜情報漏えい事件例＞



私用PCの利用におけるリスクについて、自覚している人は多くありません。ルールを守る事が最も確実なリスク回避策です。

3．PC、モバイル端末等の取り扱い

5）私用のITデバイスの取り扱い（2/2）

■私用のITデバイスの利用

- ✓ 個人で所有しているITデバイス（スマートフォンやタブレット等）で、機密情報の撮影や録音はしないでください。
- ✓ 私用のITデバイスを業務用PC等の機器へ接続しないでください。
- ✓ 事前に使用許可を得ている個人のITデバイスは、許可の範囲に従って利用をしてください。

3．PC、モバイル端末等の取り扱い

6）暗号ソフトウェアの導入

■機密情報の暗号化

✓ PCには暗号化ソフトウェア（7-ZIPなど）を導入し、機密情報は必ず暗号化してください。

3. PC、モバイル端末等の取り扱い

必須項目

7）安全なインターネットの利用

■私的なインターネット利用の禁止

✓ 業務中は、私用のインターネット利用はしないでください。

8）安全な電子メールの利用

電子メールは、機密性を保持するため以下を遵守してください。

■業務では会社のメールアドレスを利用すること。

■１人１メールアドレスを利用し、共有のメールアカウントは利用しないこと。

■フリーメール (gmail, Yahooメールなど）を業務で利用しないこと。

■メール送信時の宛先は必ず確認すること。

✓ 多数の人に同一内容のメールを送る際には、CC と BCCを適切に使い分けてください。

4.業務情報の取り扱い

4. 業務情報の取り扱い

1）情報漏えいをしないための注意点

■社外でPCを使用する場合の注意点

- ✓ 社外で業務用のノートPCを使用する場合は、のぞき見をされないように注意してください。

■業務で使用するファイルの保存場所

- ✓ 業務で使用するファイルは、原則共有フォルダに保存し、PCのローカルディスクには保存しないようにしてください。

4. 業務情報の取り扱い

2）紙文書の管理

■機密情報

✓ 機密情報が書かれた紙文書は、鍵をかけることが出来るキャビネットで保管してください。

■極秘情報

機密情報の取り扱い要件に加え、以下を考慮してください。

✓ 紙文書を取り出して使う場合は、貸出し台帳にいつ誰が紙文書を取り出したかを記載してください。

✓ 紙文書をキャビネットに返却する場合は、貸出台帳にいつ誰が返却したかを記載してください。

✓ 紙文書を破棄する場合は、貸出台帳にいつ誰がどのような方法で破棄したかを記載してください。

✓ 最低でも1週間に1度の棚卸を実施し、紙文書がすべてそろっているかどうかを確認してください。

4. 業務情報の取り扱い

3）印刷文書の管理

■機密情報の印刷

✓ 機密情報は、ユーザ認証もしくは暗証番号入力機能のついたプリンタを使用して印刷してください。

4）資料の廃棄

■紙・印刷文書の廃棄について

✓ 機密性のある文書を廃棄する際はシュレッダーにかけるなど、会社指定の廃棄手順に従ってください。

5.マルウェア対策

5. マルウェア対策

1）マルウェアとは何か

■ 不正かつ有害な動作を行うことを目的として作成された悪意のあるソフトウェアや悪質なコードの総称です。
下記はマルウェアの一例です。

- ✓ ウィルス

  コンピュータの正常な動作を妨げるコンピュータプログラムの一種。他のプログラムに寄生し、自身のコピーを作成して増殖する。

- ✓ ワーム

  自身を複製して他のシステムに拡散する性質をもったマルウェア。

- ✓ トロイの木馬

  問題のないソフトウェアに見えるよう偽装し、インストールされるとしばらくすると外のある行動を始めるようになるマルウェア。

- ✓ ランサムウェア

  インストールされた端末の使用者に対して、金銭を要求するプログラムです。ファイルやOSを使えなくした後、金銭を払えばまた使えるようにするといったメッセージを使用者に送ってきます。

5. マルウェア対策

2）マルウェアの注意点

■ マルウェアに感染するとどうなるか

✓ 企業にとって、最大のダメージを受ける可能性があるのは個人情報や機密情報の漏洩です。マルウェアの不正な動作により重要な情報が抜き取られ、ネット上に流されると企業としての信用失墜や多額の賠償金負担を招くこともあります。また、データを破壊、消失させるマルウェアもあります。情報が消失するとビジネスにも大きな支障をきたします。

■ ランサムウェアの注意点

✓ 近年、ランサムウェアという種類の不正なプログラムが流行しています。このプログラムは、PCに感染すると例えばPC内部データを暗号化してしまい、「もとに戻してほしい場合にはお金を払うように」と脅迫をするものです。

✓ ランサムウェアに感染した場合には、お金を払って自己解決しようとはせず、必ず会社に報告し、解決策を相談してください。

5. マルウェア対策

3）マルウェアに感染した場合の対応

■マルウェアに感染したことが判明してからの対応手順

- ✓ 端末がマルウェアに感染した場合、すぐに有線及び無線どちらのネットワークからも端末を切断するとともに、セキュリティ担当者に感染の報告をしてください。なお、無線の切り方の例は図１を参照ください。
- ✓ セキュリティ担当者は、同じマルウェアに他の端末も感染する恐れがあると判断した場合には、社員に対してメール等を使って注意喚起を行ってください。
- ✓ マルウェアに感染したPCは、完全にウイルスを除去したと確認できた場合のみ、ネットワークに再接続してください。

無線LANの切断方法(例)

5. マルウェア対策

4）マルウェアに感染しないための注意事項（1/3）

■アンチウイルス製品を効果的に使用するために以下の対策を行ってください。

- ✓ ウイルスは絶えず新しいものが生まれています。アンチウイルス製品の定義ファイルは自動更新される設定にしてください。
- ✓ 他社または外部委託業者から受け取った外部記録媒体の中に入っているファイルを使う必要がある場合は、必ず最新の定義ファイルを使ったアンチウイルス製品でスキャンしてください。

■ PCの設定不備によるウイルス感染を防ぐために以下の項目に注意をしてください。

- ✓ 使用するパソコンの設定を変更してセキュリティコントロールを停止させたり、無視したりできるようにしないでください。

5. マルウェア対策

4）マルウェアに感染しないための注意事項 （2/3）

■メール経由でのマルウェア感染を防ぐために以下の事項を行ってください。

- ✓ プレビュー表示をしただけで感染するマルウェアがあります。従ってプレビュー表示は行わないようにしてください。（プレビュー表示とは、受信したメールをダブルクリックせずに内容を確認する機能です）
- ✓ 不審な電子メールの添付ファイルは、開く前に必ずアンチウイルス製品と最新の定義ファイルを使ってスキャンをしてください。
- ✓ もし最新の定義ファイルを使ったウイルススキャンが出来ない端末で添付ファイルを受け取った場合、最新の定義ファイルでチェック可能な端末で一旦添付ファイルを確認し、問題が無いことを確かめてから該当の端末で開いてください。
- ✓ 昨今、標的型攻撃メールという、特定の個人や組織を狙ったメールによる攻撃が増加しています。主な手法として、業務関連のメールを装ってマルウェアに感染させる手口が知られています。これらの攻撃を防ぐため、以下の点を注意してください。
  - 不審なメールは開かない。
  - 不審なメールの添付ファイル開いたりやメール文面記載のURLをクリックしない。
  - 不審かどうか判別がつかない場合には発信元に問い合わせる(メール返信以外の手段で）などして受信したメールの信頼性を確保する。

5. マルウェア対策

4）マルウェアに感染しないための注意事項 （3/3）

■ファイル共有サービスの利用は以下項目に注意してください。

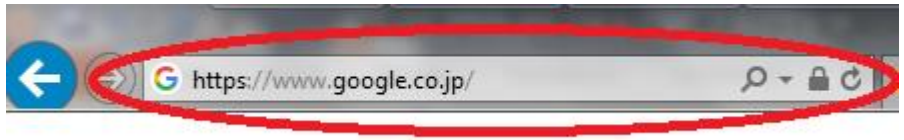
- ✓ Drop BoxやGoogle Driveなどのファイル共有サービス経由でのデータ授受は禁止です。
- ✓ ただし、MBJ IT部が許可したものに限り、許可した使用方法での利用は可能です。

（Daimler Data Exchange, Share Fileなど）

■ インターネット利用時は以下の項目に注意してください。

- ✓ パスワードの入力が必要なWebページ等にアクセスした場合には、ブラウザのアドレスバー（URLが表示されるところ）を確認して、本当に自分がアクセスしているWebページなのかを確認することを推奨します。

※マルウェアに感染した場合、ブラウザから有名なWebページ（検索エンジンや、大手銀行のオンラインバンキングページ等）を表示しようとするとマルウェアが偽のWebページを表示させてしまう場合があります。



6.日々の業務でのその他の注意点

6. 日々の業務でのその他の注意点

1）ソーシャルエンジニアリング

■ソーシャルエンジニアリングとは

- ✓ PCのモニタ画面の盗み見や会話の盗み聞きなど、人間の心理的な隙や、行動のミスに漬け込んで、個人情報や機密情報を入手する手法です。

■社内情報の開示に関する注意点

- ✓ 面識のない人はもちろん、友人知人にも、非公開の社内情報を話さないでください。
- ✓ プライベートな場面において、会話や電話はもちろんですが、ソーシャルネットワークやチャットなどの電子的なコミュニケーションでも非公開の社内情報を取り上げないように気を付けてください。
- ✓ 社内情報は、身元が確実にわかるメルセデス・ベンツ社の社員か認定取引先の社員にのみ提供してください。
- ✓ 個人情報や機密情報は、文書による要請を受けた場合にのみ、開示することを検討してください。
- ✓ 電話やオンラインでのアンケートで社内情報提供依頼を受けた場合は、社内で正式に通達があったときにのみ回答してください。

6. 日々の業務でのその他の注意点

2）安全な会話

■会話による情報漏えいの注意

- ✓ 電話、プレゼンテーション、会議などの場で機密情報について話をする場合には、不必要な人にも聞かれないように注意をしてください。
- ✓ 同窓会や社外サークル活動等、仕事に関係の無い場では機密性のある社内情報の話はしないでください。
- ✓ エレベータホール、コーヒーショップ内や地下鉄内など、公共の場では機密性のある社内情報の話はしないでください。

6. 日々の業務でのその他の注意点

3）施設へのアクセス

■施設への入退館に関する注意点

- ✓ 施設への入退館管理を行う必要があります。
- ✓ 施設内では来訪者には必ず社員の誰かが付き添ってください。
- ✓ 来訪者が施設内において非公開の社内情報に不正にアクセスしないように注意をしてください。
- ✓ 勤務中は常に社員証、もしくは入館証を身に着けてください。そうすることで社員証・入館証を持たずに入館した人物を識別しやすくなります。
- ✓ 社員証・入館証を身に付けていない人物を見かけたら、施設内に立ち入りが許可されている人物かを確認してください。
- ✓ 鍵の掛かったドアを開錠して通る際には、後ろから誰かが一緒に通り抜けをしないように注意してください。
- ✓ 他人に社員証や入館証を貸さないでください。
- ✓ 不審な人物、行為、物体を目にした場合には、上長に連絡してください。

■ 他社、外部委託者のITデバイスの施設内での使用

- ✓ 業務で使用するネットワークには、個人のITデバイスだけではなく、業務上契約のある他社や外部委託業者のITデバイスも接続はさせないでください。

6. 日々の業務でのその他の注意点

4）社外からの社内ネットワークへのアクセス

■無線LANの注意点

- ✓ 無線 LAN 利用には盗聴やなりすましのリスクがありますので、以下の対策を実施してください。
  - ✓ 利用機器のセキュリティアップデートを行い、無線LANに関する既知の脆弱性が存在しないようにする。
  - ✓ 自宅でアクセスポイントを設置する場合は、適切な暗号化方式とパスワードを設定する。
    - ✓ 暗号化はWPAまたはWPA2を選択
    - ✓ パスワードは他人が類推しにくいものを登録
  - ✓ 外出先などでは公共無線LANのアクセスポイントを利用せずに、個人のアクセスポイント（会社支給のWiFiルーターやスマートフォンのテザリング機能）を使う。万が一、不特定利用者を対象とする無線LANのアクセスポイントを利用する場合には以下の二つの条件を満たすこと。
    - ✓ URLが“https:”で接続されるようなウエブサービスに限定した利用もしくは、VPNを経由した利用（MBJのPC利用者の場合にはAlwaysOnもしくはEmergencyVPNの利用）
    - ✓ 接続しているアクセスポイントの名称（SSID）を確認し、暗号化に対応していることを確認する。

■社外から社内ネットワークへの接続方法

- ✓ 社外から社内ネットワークに接続する場合、必ず自社内の接続方法を使ってください。

6. 日々の業務でのその他の注意点

5）在宅勤務

■在宅勤務時の注意点

- ✓ 在宅勤務は、利用する情報資産の管理責任を自らが負うことを自覚し、より一層情報セキュリティに注意を払って社内の規定に沿った業務を実施してください。また定期的に実施状況を自己点検してください。
- ✓ 在宅勤務中であってもマルウェアの感染、メール誤送信などの情報セキュリティ事故があった場合、速やかに関連部署へ報告してください。報告漏れ、報告の遅れが被害拡大につながる恐れがあります。(参考：ビジネスパートナー向け情報セキュリティガイドライン6章 8. セキュリティ事故発生時)
    1. 会社から支給された機材のみを使用し、私用機器を接続しないで業務を行ってください。また、会社から支給された機材であっても、業務上必要がない場合は接続しないでください。
    2. 会社から支給された機材を業務以外で利用しないでください。
    3. 社内データは、絶対に私用の電子メールアドレスや、私用のPCに転送しないでください。
    4. 作業場所は、物理的な安全を確保してください。（自宅、もしくは個室。PCの画面や資料が他人の目に触れないこと、電話・オンライン会議の内容が他人に聞こえないこと。カフェ、レストランなどの不特定多数の人がいる場所は禁止）
    5. 資料の印刷が必要の場合は、公共のプリンターは利用してはいけません。（プリントショップなど）また、印刷物は機密性に応じた適切な管理と廃棄処理を実施してください。機密文書は会社にて適切に廃棄してください。

6. 日々の業務でのその他の注意点

6）業務で使用可能なソフトウェア

原則、IT部・情報システム責任者発注のソフトウェアのみ、使用してください。

（注）特にスマートフォンやタブレットなどのモバイル端末については、簡単にアプリケーションが導入できます。
しかし、業務効率化のために自分で判断してアプリケーションを追加することは避けてください。

7）著作権

✓ 印刷文書、電子文書、その他あらゆる形態の媒体（写真、動画、音楽ファイルなど）に関わる著作権法は、責任を持って遵守してください。

6. 日々の業務でのその他の注意点

8）セキュリティ事故発生時

■セキュリティ事故発生時の対応

- ✓ 万が一、下記のようなセキュリティ事故が発生してしまった場合は、上長・情報システム責任者へ報告してください。
- ✓ 報告内容：発生事象の詳細（いつ・だれが・なにを（情報内容・種類）・どうしたか）、被害状況、実施対応。

PCやモバイル機器などのITデバイスや入室カード、機密情報が含まれた書類や記憶媒体の紛失、盗難時

機密情報を含んだメールを誤送信した時

怪しいメールを受信し、そのメールの添付ファイルや記載のURLをクリックしてしまったとき

7.責任者向け情報セキュリティ対策

7.責任者向け情報セキュリティ対策

必須項目

1）管理体制づくり

■情報システム責任者の任命
各ビジネスパートナーにおいて、情報システム責任者の任命を行ってください。
情報システム責任者が、組織の情報セキュリティの管理と推進を担います。

■情報セキュリティ社内規定の策定
情報システム責任者は、本ガイドラインを参考にして情報セキュリティに関する社内規定を策定してください。

■情報セキュリティの啓蒙活動
情報システム責任者は、情報セキュリティに関する社内規定を従業員に周知徹底し、継続的に啓蒙活動を実施してください。

■情報セキュリティ事故発生時の対応
情報システム責任者は、セキュリティ事故の発生を把握、関係組織と連携して事故の対応、再発防止策の策定の一連の活動を推進します。

■定期レビュー
情報システム責任者は、従業員の情報セキュリティ対策の状況を定期的に確認し、情報セキュリティ活動の評価と見直しをしてください。

7.責任者向け情報セキュリティ対策

2）セキュリティ事故対処方法

セキュリティ事故対応とは、セキュリティ事故の発生を把握、関係組織と連絡をとり事故対応行い、再発防止策を策定する一連の活動のことです。
代表的なセキュリティ事故の対処方法は以下のとおりです。
解決まで責任をもって対応してください。

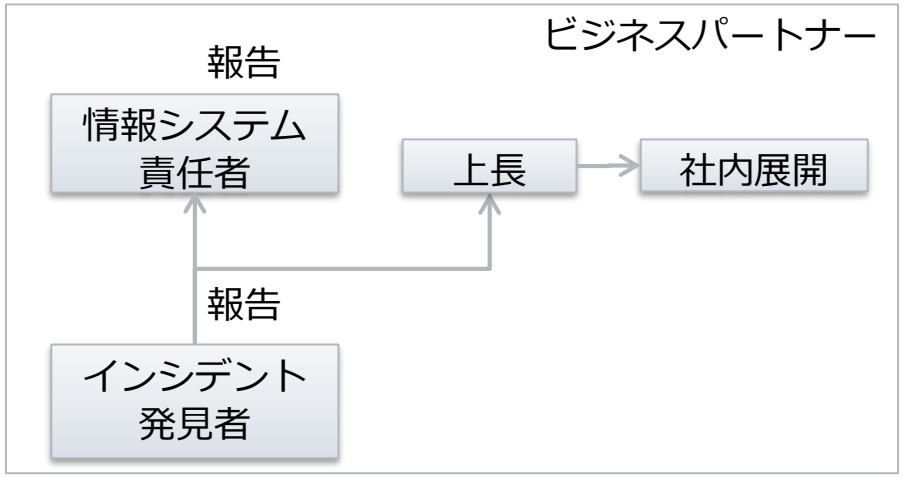
事象	対応
ITデバイスの盗難・紛失	報告、盗難・紛失の日時/場所と記録されているデータ内容の特定、詳細報告
情報漏えい/改ざん、不正な持ち出し	報告、被害情報の特定、手口の調査、再発防止策検討、詳細報告
機密文書の盗難・紛失	報告、盗難・紛失の日時/場所と記載内容の特定、再発防止策の検討、詳細報告
メール誤送信	機密情報の社外メール誤送信の場合に報告、文面/添付ファイルに機密情報が含まれていたか確認、誤送信先へメールの廃棄依頼を実施後、詳細報告
ウイルス感染の疑い	ネットワークから切り離し隔離（LANケーブル抜線、無線LANスイッチOFF）、報告、最新のウイルス対策ソフトでの検査

7.責任者向け情報セキュリティ対策

3）セキュリティ事故発生時の連絡体制

■連絡体制の構築

セキュリティ事故が発生した際、円滑に情報連携、報告ができるよう左図のような連絡体制を構築し、社内周知してください。



■事故発生時の連絡について

□連絡体制の共有
構築した連絡体制を社内で展開し、全従業員がセキュリティ事故発生時に報告すべき連絡先を把握できるようにしてください。

□機密情報の漏洩時
セキュリティ事故の内、機密情報の漏洩の可能性がある場合は、直ちに組織内で報告の上、記録(※1)してください。

※1 記録内容
発生事象の詳細（いつ・だれが・なにを（情報内容・種類）・どうしたか）、被害状況、実施対応内容。

必須項目

7.責任者向け情報セキュリティ対策

4）IT機器の保護：ウイルス対策（1/2）

■アンチウィルス製品の利用

業務で利用するIT機器（PC、モバイル端末、サーバーなど）に対して、アンチウィルス製品を導入してください。導入後は最新の定義ファイルを用いた定期的なウイルススキャンが実施される様に運用してください。また、適宜ライセンスは更新してください。

アンチウィルス製品を正しく運用することで、IT機器のウイルス感染を検知/防止することができます。IT機器がウイルス感染した場合、情報資産が危険にさらされるだけでなく、自分自身が加害者となり、被害を拡大させる可能性があります。

必須項目

7.責任者向け情報セキュリティ対策

4）IT機器の保護：ウイルス対策（2/2）

■アンチウィルス製品の選定

✓ 以下の項目を満たすウィルス対策製品を使用してください。

- 有償の製品でサポートが受けられるもの。
- 自動的に定期スキャンができる機能を備えていること。
- ウイルス定義ファイルやスキャンエンジンが更新されるもの。
- ウィルスの隔離/駆除機能を備えていること
- 製品検査・評価ベンダーによる評価が高いもの。

※製品例は本ガイドラインP62をご参照ください。

■ ウイルス対策ソフトの設定

✓ ウイルスのリアルタイムスキャンだけでなく、週に1度は定時スキャンでハードウエア全体のスキャンを行うとより安全です。

7.責任者向け情報セキュリティ対策

必須項目

5） IT機器の保護：脆弱性対応 (1/2)

■脆弱性とは

PCやサーバー、モバイル機器等のIT機器のOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことです。脆弱性が残された状態でIT機器を利用すると、不正アクセスに利用されたり、ウイルスに感染したりする危険性があります。

■定期的な脆弱性対応運用の確立

脆弱性対応はIT機器の所有者に対応責任があります。業務で利用する全てのPCやサーバーなどのOS（オペレーティングシステム）、ルーターやスイッチなどのファームウェア、各種ソフトウェアに脆弱性が見つかった場合はセキュリティパッチの適用やアップグレードが必要です。また、IT機器の設定に関する脆弱性も存在するので、見つかった場合は適切な変更を行います。
各組織にて自主的に脆弱性対応を推進できるよう、社内における定期的な脆弱性対応の運用を定義し、プロセスドキュメントとして文書化してください。そして、文書化した運用に則り、脆弱性対応を実施してください。なお、プロセスドキュメントはMBJが監査時等に確認させていただきます。

ただし、セキュリティパッチ、ソフトウエアアップデートにより、業務アプリケーションやIT機器そのものの動作に影響を与えることがあります。最悪の場合、業務アプリケーションが利用できなくなったりIT機器の動作が停止する可能性もある為、パッチを適用する前には全管理PCに対し動作検証を行うなど細心の注意を払ってください。

必須項目

7.責任者向け情報セキュリティ対策

5） IT機器の保護：脆弱性対応 (2/2)

■MBJで脆弱性を発見した場合

MBJでは不正通信や脆弱性の検知を目的としたネットワーク監視や脆弱性スキャンを実施しています。

監視やスキャンの結果により、メルセデス・ベンツ社ネットワークに接続されている販売店に設置されたPCやサーバーなどのIT機器において脆弱性やサイバー攻撃の兆候・痕跡を見つけた場合は関係者へご対応依頼の連絡をする場合があります。連絡を受けた場合はすみやかにご対応ください。

■脆弱性対応期日

メルセデス・ベンツ社では、脆弱性の深刻度に応じて対応期限が定められています。
MBJから対応依頼の連絡を受けた場合は下記の対応期日以内に対処してください。
ご対応いただけない場合は、該当の通信やIT機器をMBJネットワークに接続不可とする等の措置をとる場合もありますので、あらかじめご了承ください。

脆弱性深刻度（CVSSv3 Baseスコア）	対応期日
CVSSv3 9.0 – 10.0 (深刻度：Critical)	MBJからの通知から30日以内
CVSSv3 7.0 – 8.9 (深刻度：High)	MBJからの通知から60日以内

必須項目

7.責任者向け情報セキュリティ対策

6） IT機器の保護：サポート期間

■OSやソフトウェア等のサポート期間

基本的に、全てのOSやファームウェア、ソフトウェア等にはメーカーによるサポート期間が設けられています。

サポート期間中は不具合が見つかったりマルウェアに対する脆弱性が発見されれば無償で更新プログラムやセキュリティパッチが提供されます。サポート期間終了後は不具合などの問い合わせも受け付けてもらえなくなり、セキュリティパッチやアップグレードバージョンも提供されなくなるので、サポートが終了したOSやソフトウェアを搭載したIT機器を使用し続けることはセキュリティの観点からも非常に危険です。

下記の点に考慮し、**サポート期間が終了した製品を利用しないようにしてください**。

- 利用しているPCやサーバーのOSやソフトウェアのバージョンを一覧にして管理してください。
- 各メーカーから提供される情報を適宜確認し、各製品のサポート終了時期を把握してください。
- サポート期限内に後継バージョンへ移行するための対応プロセスを準備して、それに則りバージョン移行をしてください。

必須項目

7.責任者向け情報セキュリティ対策

7）PCの保護：セキュリティワイヤによる固定

■ノートPCの盗難対策

犯行者は機密情報を狙っていなくても、金銭目的でPCを窃取することがあります。
機密情報を保存しているかどうかに関わらず、PCを利用する際には物理的な盗難への対策が必要です。例えば、
以下の対応をしてください。

- ✓ ノートPCは、セキュリティワイヤで固定して使用する。自席で固定するだけでなく、セミナールームや商談スペースなどに移動してノートPCを利用する場合には、IT部からセキュリティワイヤを借りて固定する。
- ✓ 退社時には、ノートPCを施錠された安全な場所に保管する。

- セキュリティワイヤとはコンピュータの盗難や不正な持ち出し、ケーブルや周辺機器の不正な差し込みなどを防止するための金属線でできた固定器具です。
- ケンジントン社のセキュリティワイヤが一般的で、通常のPCのスロットを利用した機器の固定が可能となります。

7.責任者向け情報セキュリティ対策

8）PCの保護：ハードディスクの暗号化

■ハードディスクの盗難

セキュリティワイヤでPCを固定していたとしても、PCからハードディスクを抜き出して他PCでデータを読み取ることが可能です。
防止策はハードディスクを暗号化して、他PC でのデータ読み取りを困難にすることです。
ただし、暗号化したハードディスクの復号化は可能ですので、他の防御策と組み合わせて実施することをお勧めします。

7.責任者向け情報セキュリティ対策

9）ネットワークに接続されたシステム・機器の保護

■セキュリティ設定

昨今のIT技術の進歩により、様々な機器がインターネットに接続されています。
特に、ネットワークカメラ（ネットワーク機能を備えたWebカメラなど）や複合機などが、インターネットを経由して遠隔で第三者により不正アクセスされる事例が報告されています。
情報漏えいを未然に防止するために、以下の対策を実施してください。

- ✓ 解読が困難なパスワードを設定する(初期パスワードのまま使用しない)。
- ✓ 認証機能を有効にする。
- ✓ システムや機器へのアクセスが必要なIPアドレスなどを制限する。
- ✓ ソフトウエアを定期的にアップデートする。

※なお、システム・機器の設定方法は、利用している製品によって異なります。対策の実施にあたりましては、システム・機器のマニュアルを参照する、もしくは製品の提供業者に確認をすることをお勧めします。

7.責任者向け情報セキュリティ対策

必須項目

10）IT資産管理

■保有資産の把握

会社のPCやモバイルデバイス、記憶媒体(USBメモリ等)などのIT資産利用状況を常に把握しておくことを推奨します。以下のような情報を記載したIT資産管理台帳を保有し、定期的に確認し更新してください。
IT資産管理台帳にて下記の情報をあらかじめ把握をしておくことで、盗難や紛失が発生した際に、被害状況を特定しやすくなります。

IT資産管理台帳への記載が必要な情報

- ✓ IT資産種別（PC, モバイル, タブレットなど）
- ✓ 機器名
- ✓ 管理担当者
- ✓ 機器の設置場所
- ✓ IPアドレス
- ✓ 購入時期

必須項目

7.責任者向け情報セキュリティ対策

11）システムへのアクセスと認証

■ システムユーザーIDの改廃

異動・退職等によりIDの削除や変更が必要になった場合は、所定の手順に従い変更・削除申請をしてください。

ID変更・削除申請は、異動・退職後7日以内に実施してください。

■システムユーザーID棚卸

退職者のユーザーID削除申請など適切なユーザーID管理がされていない場合、情報漏洩などのセキュリティ事故につながる可能性があるため、各システムのアクセス権を持つ従業員の把握、定期的な見直しが必要です。

MBJでは、定期的にシステムユーザーIDの棚卸を実施しますので、システムユーザーID棚卸の依頼を受けましたら期限内に対応してください。

7.責任者向け情報セキュリティ対策

必須項目

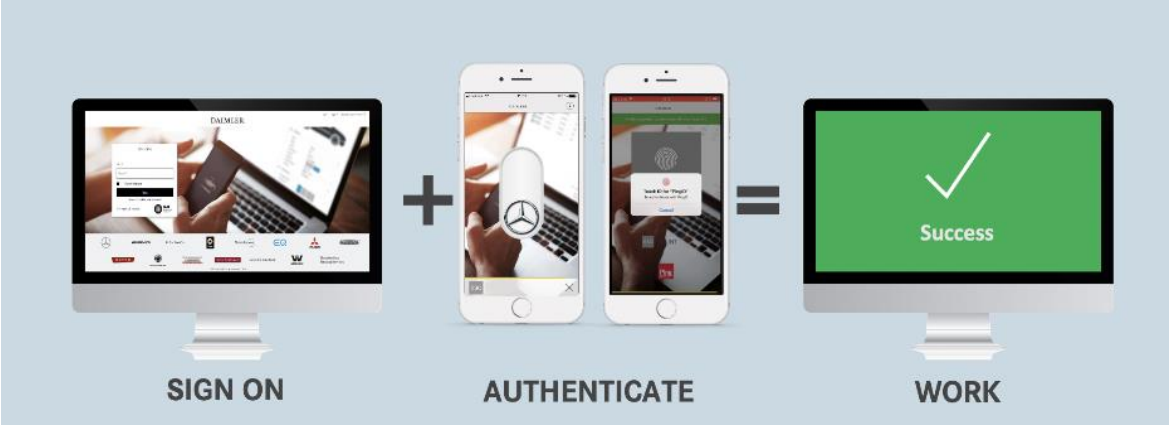
11）システムへのアクセスと認証

■ 多要素認証

メルセデス・ベンツ社のシステムのうち、機密性が高い情報を取り扱うシステムでは多要素認証*が導入されています。

多要素認証システムが導入されているシステムにログインするためにはID＋パスワードでの認証に加え、認証ツール（スマートフォンにインストールされたアプリケーションなど）での認証が必要となります。

多要素認証が必要なシステムにアクセスできるよう、各ユーザーにて認証ツールの準備を実施してください。



*多要素認証：以下のように2つ以上の要素によって認証をする仕組みのこと
①本人だけが知っていること　②本人だけが所有しているもの　③本人自身の特性
例）銀行ATMでの現金引き出し
　　キャッシュカード＝本人だけが所有しているもの，暗証番号＝本人だけが知っていること

7.責任者向け情報セキュリティ対策

12）クラウドサービスの選択

■クラウドサービスとは

✓ インターネット上に構築された、ファイル共有サービスやメールサービスのこと。

■許可するクラウドサービスの判断基準

✓ ユーザに使用を許可するクラウドサービスは、以下の3つの条件を満たすものとしてください。

1. 万が一問題が発生した場合に責任の所在がはっきりとしているもの。

   例：利用規約に問題発生時の責任所在が明記されている

2. 運用がしっかりしているもの。

   例：ISO 27001, 27017, PCI-DSS等を認定取得している

3. 問題が発生した場合に原因が特定できるもの。

   例： Google Appsの場合はUnlimitedを選択（管理者はメールデータの全バックアップを取ることが出来ます。つまり、情報漏えいが発生した場合にも、Unlimitedであればバックアップしたメールから、誰が情報を漏えいさせたかの特定が可能になるなど、原因の追跡が可能となります）

- 無料のものは問題発生時の対応が十分で無いため、使用しないでください。
- 外部委託業者や協力会社が運営するクラウドサービスの場合、契約時に問題発生時の責任の所在を明確にするとともに、問題発生時の対応についても明確に文書で書かれているか確認してください。

なお、MBJではクラウドサービスにおけるリスク評価を実施して認可されたもののみを利用することが可能です。
MBJとの業務上クラウドサービスを利用する必要がある場合は、まずMBJ担当者と相談してください。

お問合せ先

本ガイドラインについて、不明点などあれば下記の連絡先までお問い合わせください。

販売店様のお問い合わせ先：ITサービスデスク

メールアドレス：itsd_jpdlr@mercedes-benz.com

電話番号：0120-987-972

サービス時間：8:00 – 21:00（土日祝含む）

その他パートナーの皆様は、不明点がございましたら担当のMBJ正社員までお問い合わせください。

付録

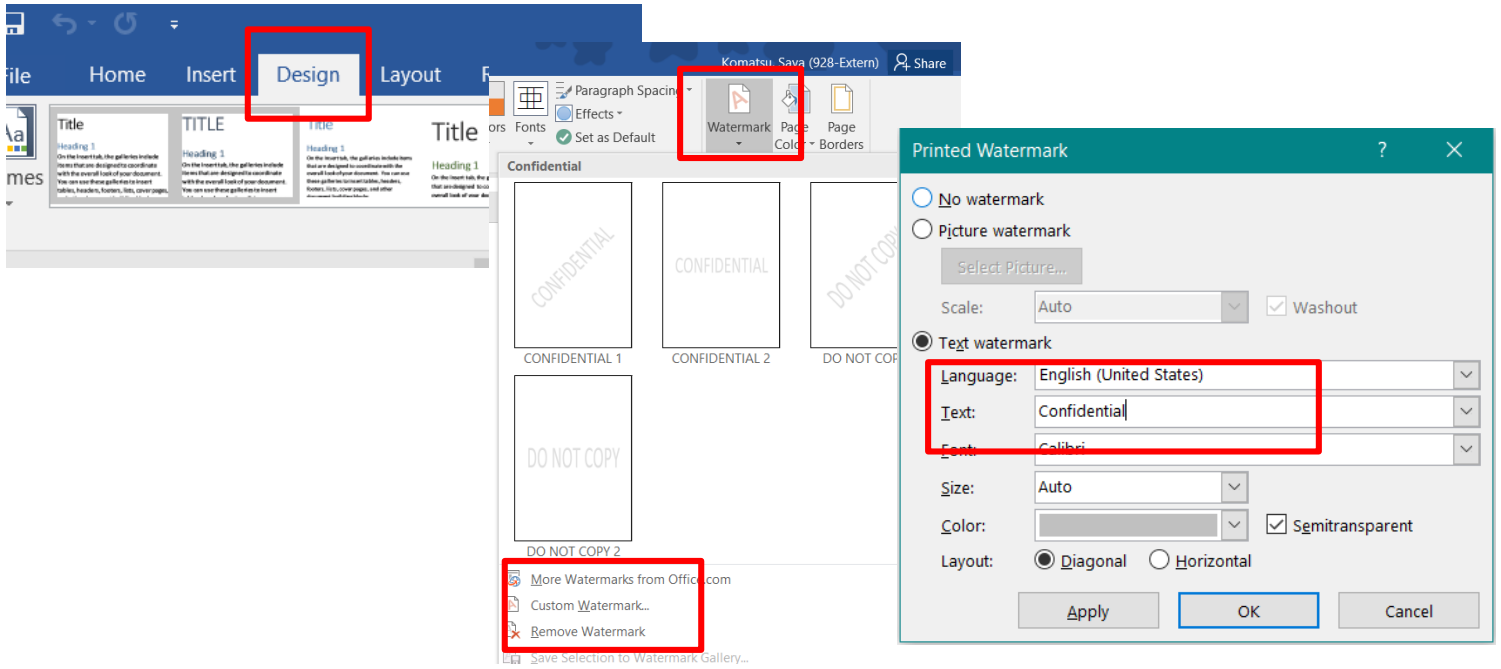
ラベリングの方法（例）

■ラベリングとは、文書に情報資産区分を明記することです。

■文書の表紙、各ページのフッター・ヘッターに Internal / Confidential / Secret と記載してください。

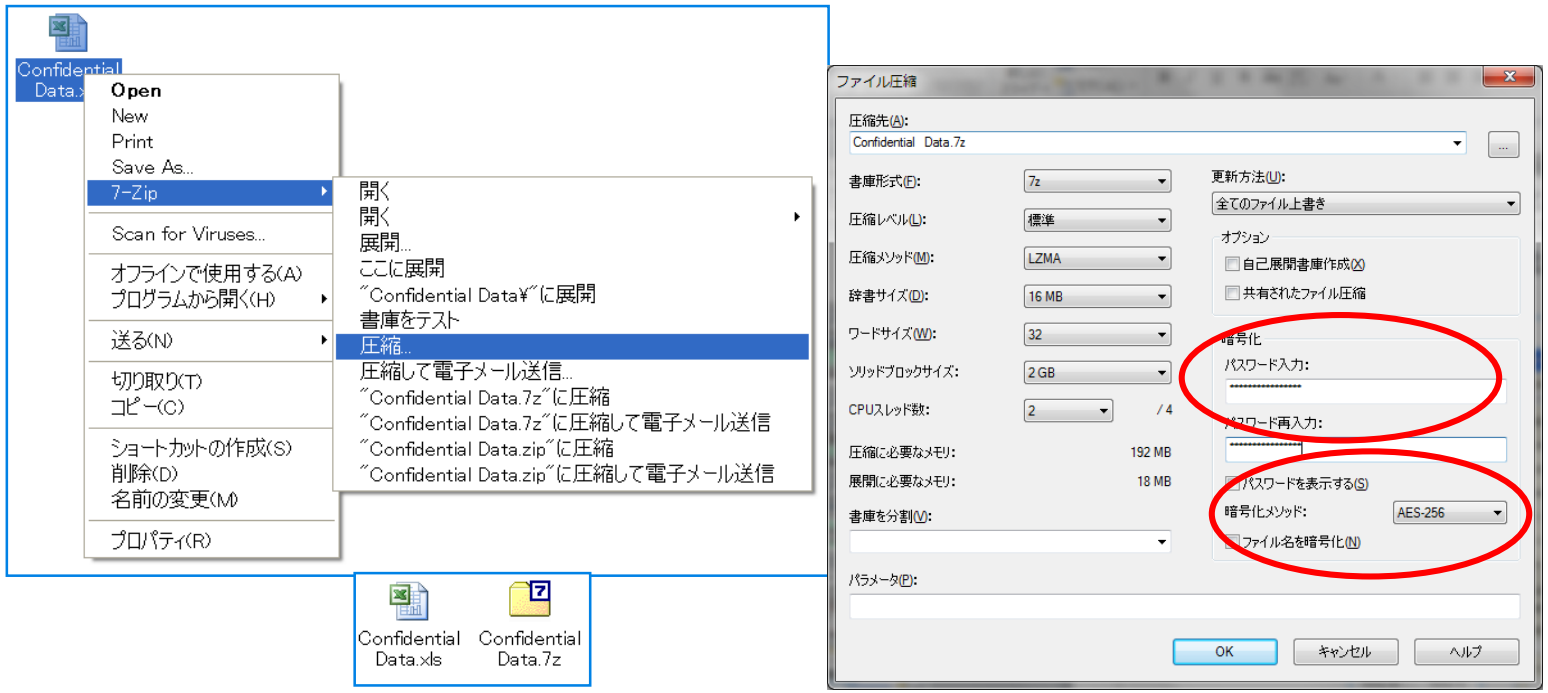
■本文のすかしにラベリングを行う方法は下記のとおりです。

✓ 【Office2016の場合】デザイン→透かし→ユーザー設定の透かし→テキストに区分内容を記載



暗号化の方法（例）

- 7-Zipを利用して、ファイルの暗号化ができます。
  - ✓ ファイルを右クリックし、「7-Zip」→「圧縮」を選択します。
  - ✓ 「ファイル圧縮」画面の右下の「暗号化」項目にて、「パスワード入力」のボックスにパスワードを入力（推奨8文字以上）し 、暗号化メソッドはAES-256を選択してOK ボタンを押下します。元のファイルが格納されているフォルダに暗号化ファイルが作成されます。



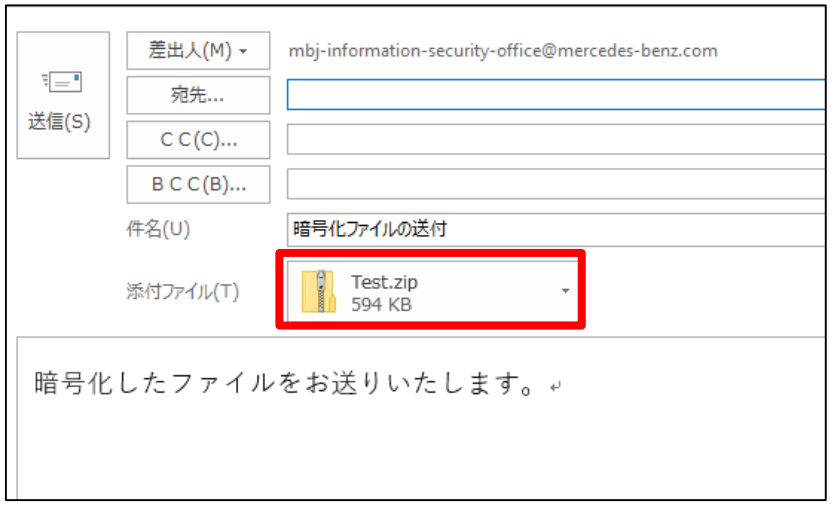
安全に機密情報を電子メールで送付する方法（例）

Confidential（機密）情報を 社外の人に提供する必要がある場合には、データを暗号化したうえで送付してください。

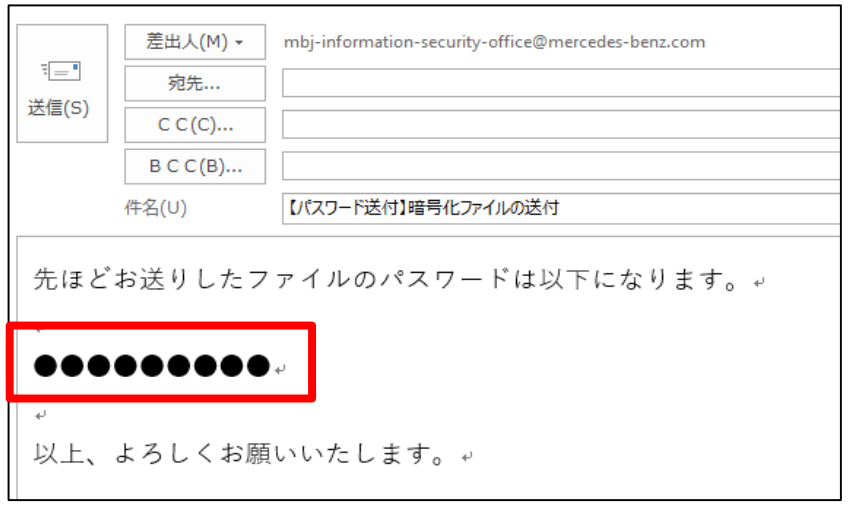
＜手順＞

1. 前項のファイルの暗号化方法（例）に従い 7-Zip でファイルを暗号化をする。
   - 7-Zipが利用できない場合には Office 製品（Excel/Word）のパスワード設定を行う。
2. 暗号化したファイルを送付する。
   - 電子メールの1通目に暗号化したファイルを添付する。
   - 電子メールの2通目もしくは電話などの別の手段で開封用パスワード情報を連絡する。

＜1通目＞



＜2通目＞



メルセデス・ベンツ社従業員と安全に機密情報を授受する方法

メルセデス・ベンツ社従業員（メルセデス・ベンツ社のメールアカウント保有者）から個人情報などの機密情報を共有する場合も暗号付きメールにて安全に情報を送付いたします。

メルセデス・ベンツ社従業員から送信された暗号付きメールはWebMailというツールを利用することで、ビジネスパートナーの皆様にも安全に受信していただくことが可能となります。

また、このツールを用いて、メルセデス・ベンツ社従業員へ暗号化メールを送付することもできます。

WebMailの利用方法につきましては、別途マニュアルがございますのでそちらをご参照ください。

ウイルス対策ソフトウェア（例）

■ 下記参考に会社に合った信頼できるメーカーの製品を使用してください。

ウイルス対策ソフトウェアベンダー（例）

No	メーカー	製品名例
1	マカフィー	マカフィーアンチウイルス等
2	シマンテック	ノートン360スタンダード等
3	Microsoft	Microsoft Defender（有償機能有り）等
4	トレンドマイクロ	ウイルスバスタークラウド等

（製品名は 2022/6/21 時点の情報）