

この研修は、「Japan IOT主催 セキュリティ研修 2015」の内容です。

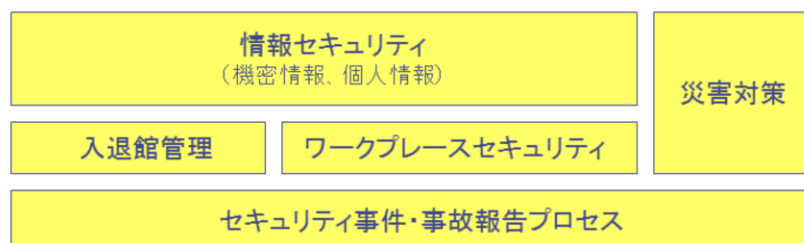
当コンテンツの記載内容はすべて関係者以外へ開示してはならない情報資産です。  
取り扱いには十分注意してください。

始めにセキュリティ研修の教材を学習し、最後に確認クイズを受けてください。

## 学習目標

- ◆ 日本IBMグループの業務に従事する契約社員及び購買取引先社員が、日本IBMグループのセキュリティを正しく理解し、日頃から実践するために、社内のセキュリティおよびプライバシーに関する取組みとルールを学習します。

## 日本IBMグループのセキュリティの概要



(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

本コースは、日本 IBM グループの業務に従事する業務委託先や派遣社員などの購買取引先社員及び契約社員を対象に作成されています。

標準的な学習時間は約30分です。

## 目次

日本IBMグループのセキュリティを正しく理解し、日頃から実践いただくために、以下の内容について学習します。

セクション1 - 2015年度の情報セキュリティ 重点ポイント

セクション2 - 情報の取り扱い

セクション3 - ITセキュリティルール

セクション4 - その他全般のセキュリティ



(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

### セクション1 2015年度の情報セキュリティ 重点ポイント

→ 情報セキュリティの方針や、事件事故の対策について学習します。

### セクション2 情報の取り扱い

→ IBM およびお客様情報の取り扱いを学習します。

### セクション3 ITセキュリティルール

→ 日常業務で使用する IT 機器の使用ルールを学習します。

### セクション4 その他全般のセキュリティ

→ IBM のセキュリティ施策を学習します。

## セクション 1

### 2015年度の情報セキュリティ 重点ポイント

(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

## 日本IBMグループの情報セキュリティマネジメントシステム (ISMS)

### ■情報セキュリティ目的

日本IBMグループは、情報セキュリティ・マネジメント・システム (ISMS) の運用を通じて次のことを達成する

- 日本IBMグループ全体の情報セキュリティ保護レベルの向上
- 日本IBMグループの情報セキュリティにおける信頼性の向上
- 日本IBMグループのノウハウやテクノロジーの活用と蓄積及び事例化

### ■情報セキュリティ方針

日本IBMグループは、情報セキュリティ方針を次のように定める

- ISMSに基づく情報の管理の実践
- お客様との契約、及び法的要件の遵守
- 情報セキュリティにおける責任の遂行

日本IBMグループ統一認証



・規格:  
ISO/IEC27001:2005  
・認証番号:  
IND13.2589U  
・登録認証機関:  
ビューローベリタスジャパン  
株式会社

(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

日本IBM では、2005年にISMS(※)の認証を取得、2009年には日本IBM グループを対象とした統一認証に拡大して、今日まで情報セキュリティを維持・向上させる取り組みを継続しております。

日本IBM グループの業務に従事する皆さんは、変化し複雑化する情報セキュリティの脅威を理解し、お客様や社会をリードするよう期待されていることを十分に自覚し、不注意による情報セキュリティ事故を絶対に起こさないことを認識してください。

※ ISMS (Information Security Management System)

物理セキュリティ分野やITセキュリティ分野などを横断的にマネジメントし、戦略的に情報セキュリティに取り組むシステム。

その国際規格 (ISO/IEC27001:2013) の取得は、公共事業などの入札条件として求められる場合もあります。

## パブリック・クラウド・サービスの業務使用禁止

IBM情報を、公共のサービス、あるいはインターネットサービスプロバイダーのメール、カレンダー、あるいはストレージサービスに、保管、コピー、転送することは禁止されています。

(IBMが管理していないシステム、サービスの例)

- ◆ Gmail、Yahoo、hotmail 等のメール
- ◆ Evernote、dropbox、iCloud 等のストレージ・サービス



業務の情報をメールで送信する等、ビジネス上の

お客様やパートナー様への送信はこれらにはあたりません。(ただしこうした場合にも、送信するファイルにパスワードをかける等の措置が求められます)

もし、外部サービス等を使う必要が発生した場合には、必ず、事前に所属長/派遣先責任者/プロジェクト責任者に相談してください。

(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

## DLP (Data Loss Prevention) による監視

IBMでは、社外への情報漏洩を防止するため、DLP(Data Loss Prevention)を実装し、常にネットワークを監視しています。



### 【DLP で検知された違反事例】

- 多忙な業務を休日も自宅でフォローするため、業務用ワークステーションを持ち帰らずに済むよう業務情報ファイルをNotesメールから自分のYahooメールアドレスに転送した。
- 重要な案件に大至急対応しなければならず、外出先でも検討が行えるようIBM Confidential 情報を自分のスマートフォンに転送した。

(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

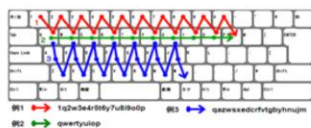
ルール違反の事象を通じて起こりうる情報漏えいを防止するため、DLP のネットワーク検知によるインターネットでの外部向け通信のスキャンが常時、実施されており、IBM グループ社員だけでなく IBM Notes ID を持つ取引先社員に対しても、IBM 業務情報や個人情報を無断で外部のアドレスに転送している事象が発見されています。

DLPで事象が検知された場合には、悪意の有無に拘らず、情報セキュリティ推進からの事情の確認などの調査にご協力いただきます。

## 推測されやすいパスワードの使用禁止、及び 業務使用ワークステーションの持ち出し禁止

下記のような推測されやすいパスワードは絶対に使用しないでください。

- ◆ キーボード配列に従ったもの(例: zaq12wsx)
- ◆ 初期値(例: administrator、password)
- ◆ 単語の一部を記号や数字に置き換えたもの(例: p@ssword、passw0rd)



契約社員及び購買取引先社員については、ワークステーションを社外に持ち出すことは禁止されています。

もし、所属長/プロジェクト責任者の同意を得て、業務上の必要により業務使用ワークステーションを社外に携行するときには、必ず、シャットダウン(電源オフ)してください。

(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

IBMのパスワード・ルールを再度確認し、ワークステーションやサーバーだけでなく、社内システムに対しても、推測されやすいパスワードは使用しないでください。  
(パスワードルール抜粋)

- 少なくとも 8桁
- 英字(大文字／小文字)と非英字(数字、句読点、特殊文字)の混合を含むこと、あるいは、少なくとも2種類の非英字の混合を含むこと
- パスワード中にユーザーIDの文字列を含まない
- IBM管理下でないコンピューター・システムにアクセスする場合は、IBM社内システムに使用するパスワードと同一のパスワードを使用しないこと



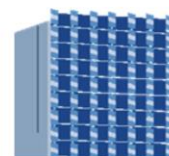
## セキュリティ事件・事故に遭遇した場合

ワークステーション紛失、入館証紛失、メール誤送信など、セキュリティ事件・事故が発生してしまった場合には、「すぐに」所属長か派遣先責任者、もしくはプロジェクト責任者に報告してください。

所属長/派遣先責任者/プロジェクト責任者



事故  
報告書



本社  
セキュリティセンター



ワークステーション  
を紛失した！  
IBMの責任者に報告  
しないと...

その後、「事件・事故報告書」を提出し社内関連部門と連携し処理対応を進めます。

(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

一瞬の油断や不注意により、セキュリティ事故は突然やってきます。

万が一、セキュリティ事故に遭遇したら、判明しだい直ちに、自身の所属長や派遣先責任者もしくはプロジェクト責任者に報告してください。

報告書の提出後は、社内関連部門（セキュリティ、情報セキュリティ推進、法務、労務ほか）の指示に従い、事故の収束まで、契約社員（臨時雇用社員）の場合は当事者と所属長が、また派遣社員や業務委託先社員の場合には当事者と派遣元会社や業務委託先会社にも責任をもって対応いただきます。

## 不審メールを受け取った場合とマルウェアに感染した場合の対応

最近の不審メールは、送信者、件名、本文等を巧妙に装い、真偽の判断が難しいものも多く、細心の注意を払っていても回避が難しいケースもでてきています。不審なメールに添付されたファイルを開いたり、リンクをクリックしないでください。また、ノートメール機能の「Report as SPAM」を使って報告してください。

もしもマルウェアに感染してしまった場合には、

1. 直ちにワークステーションをネットワークから切り離す
2. 所属長/プロジェクト責任者に口頭(電話)で報告する

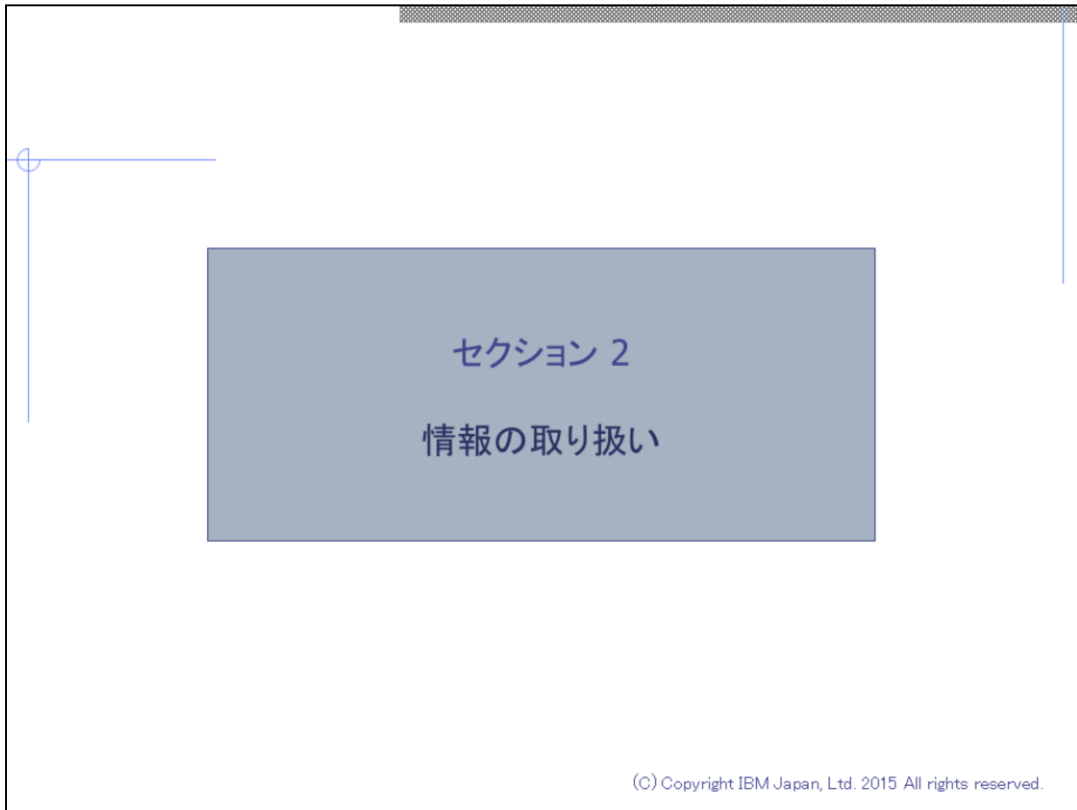
※報告後の対応方法は、IBMからの指示にしたがってください。



(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

受け取る予定のないファイルが添付されているメールや、内容がよくわからないメールは、周りの人に聞く、W3情報を確認するなどしてむやみに添付ファイルを開いたり、リンクをクリックしたりしないようにすることがリスク回避の第一歩です。

もしワークステーションがマルウェアに感染した場合、たとえ重要なファイルであっても感染ワークステーションからファイルを別の記憶媒体に保管することは出来ません。  
(二次感染、三次感染の危険性)



このセクションで指定している日本IBM グループの規定は、セキュリティ&プライバシー・ポータル「情報管理ガイド」に詳しい記載があります。IBMネットワークに接続して業務をする方は、確認してください。

<http://ibmurl.hursley.ibm.com/486I>

## 取り扱う情報の種類

日本IBMグループの情報の分類方法を理解し、情報の種類に応じた管理要件に従って取り扱ってください。

分類	定義	区分	
IBM専有情報	IBM DB内の情報を含む IBMが所有するすべての情報	IBM 機密情報	
		IBM 機密情報以外	
個人情報	日本IBMグループが情報主体から直接取得した個人情報 (従業員およびお客様に関する個人情報)	High	個人顧客情報、法人担当者センシティブ情報、社員センシティブ情報
		Mid	法人担当者関連情報 / 法人担当者コンタクト情報 / 社員関連情報
		Low	社員コンタクト情報
お客様情報	お客様からお預かりした情報	機密保持契約に基づき開示された情報	
		受領者が外部に開示すべきでないと判断した情報	
		上記以外のお客様情報	
個人情報	委託先としてお客様から開示された個人情報	特則/覚書等の個人情報に関わる契約に基づき開示された情報	

(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

私たちは日常の業務においてさまざまな情報を取り扱っています。その情報の種類によって管理要件が異なるため、情報の種類を正しく判別する事が重要です。

### 【 IBM専有情報 】

日本IBM グループが所有する情報はIBM 専有情報であり、その多くは機密情報です。

IBM 専有情報を第三者(再委託先など)に開示や提供する場合には、定められた手続きを守ってください。とくに機密情報の場合は、日本IBM グループの「機密情報管理規定」に従い、必ずその情報の所有者に開示や提供の可否を確認してください。

業務上、インターネットで送付する必要がある場合には、必ず暗号化しなければなりません。

## 取り扱う情報の種類

日本IBMグループの情報の分類方法を理解し、情報の種類に応じた管理要件に従って取り扱ってください。

分類	定義	区分	
IBM専有情報	IBM DB内の情報を含む IBMが所有するすべての情報	IBM 機密情報	
		IBM 機密情報以外	
個人情報	日本IBMグループが情報主体から直接取得した個人情報 (従業員およびお客様に関する個人情報)	High	個人顧客情報、法人担当者センシティブ情報、社員センシティブ情報
		Mid	法人担当者関連情報 / 法人担当者コンタクト情報 / 社員関連情報
		Low	社員コンタクト情報
お客様情報	お客様からお預かりした情報	機密保持契約に基づき開示された情報	
		受領者が外部に開示すべきでないと判断した情報	
		上記以外のお客様情報	
個人情報	委託先としてお客様から開示された個人情報	特則/覚書等の個人情報に関わる契約に基づき開示された情報	

(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

### 【お客様情報】

IBMは、お客様から機密情報や個人情報をお預かりする際には、機密保持契約や個人情報取扱いに関する特則/覚書等を交わし、お客様と合意したセキュリティ管理要件に基づき厳密に扱います。

IBMからこれらの情報の開示を受ける場合は、契約に基づき取り扱いルールを遵守してください。

業務上、インターネットで送付する必要のある場合には、必ず暗号化しなければなりません。

## 個人情報とは何か(国内法による定義)

### 個人情報とは — 個人情報保護法より

- ✓ 生存する個人に関する情報
- ✓ 特定の個人を識別できるもの

例: 氏名、住所、生年月日、性別、eメール・アドレス、社員番号他



### 個人データとは — 個人情報保護法より

- ✓ 容易に検索でき、体系化された個人情報
- ✓ 個人情報データベースを構成する個人情報

例: 住所録を構成するデータ(媒体を問わない)



#### 取得

- ✓ 利用目的の通知、公開

e-mailでセミナーのご案内を送付いたします。



#### 管理

- ✓ 適切な安全管理
- ✓ 正確性の確保
- ✓ 委託先の監督

~~漏えい・流出・盗難~~



#### 利用

- ✓ 適切な開示
- ✓ 目的内での利用

開示通知書に基づいています！



(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

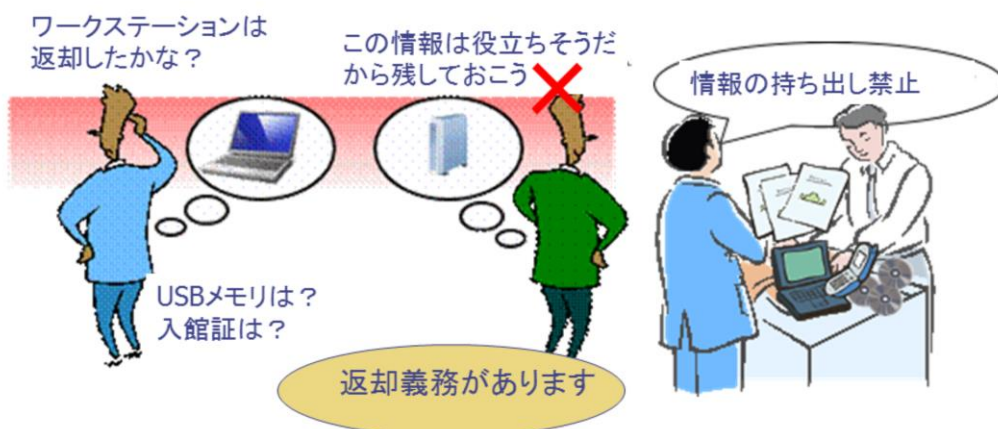
IBM は IBM 社員、お客様、ビジネスパートナー等すべての個人情報を各国の法律に基づき適切に取り扱うことを求めています。具体的な取り扱いは、IBM社員の指示に従ってください。

個人情報に関する不明点は 所属長/プロジェクト責任者へ問合せください。



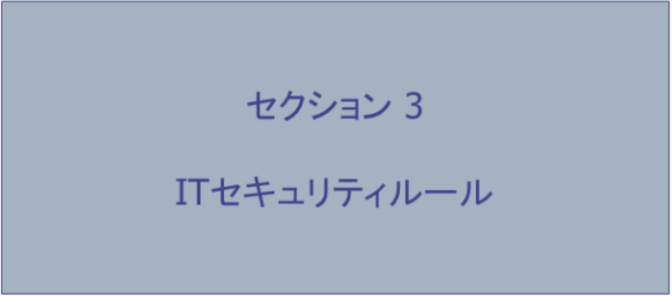

## 退職時(プロジェクト離任時)の情報資産返却

退職時、離任時には、情報や資産(ワークステーション、外部記憶媒体、入館証、書類等)を確実に返却してください。



(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

IBM との契約を終了する場合、業務で使用した情報と資産(ワークステーション、携帯電話、外部記憶媒体、入館証、書類等)をすべて返却してください。(書類については、プロジェクト立会いの下で廃棄も認められています。)



## セクション 3

### ITセキュリティルール

(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.



## 業務で使用するワークステーション、モバイル機器、外部記憶媒体のルール(1/2)

- ◆ 業務で使用する機器(ワークステーションやモバイル機器)はITCS300を遵守する  
⇒ ITCS300:コンピュータ・セキュリティ&ユース・スタンダード-日本IBM版  
(IBMネットワークに接続して業務をする方は、確認してください)
- ◆ IBMネットワークに接続される、あるいは、IBM業務に使用される全てのワークステーションおよびモバイル機器はエンドポイント登録が必須
- ◆ 承認された暗号化ソリューションによるHDD暗号化を実施
- ◆ ファイル共有ソフト(P2P)は利用禁止
- ◆ 特権ユーザーは、IBM資産または、お客様から提供されたワークステーションでのみ、その作業を実施(原則、業務用ワークステーションとして、Linux ワークステーションを貸与)



(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

ITCS300:コンピュータ・セキュリティ&ユース・スタンダード-日本IBM版  
( URL : <http://ibmurl.hursley.ibm.com/N9VJ> )

## 業務で使用するワークステーション、モバイル機器、外部記憶媒体のルール(2/2)

- ◆ 外部アドレスへのメールの自動転送禁止
- ◆ 外部ストレージへのIBMデータ保管禁止
- ◆ 事業所内でのルーター/テザリングの使用禁止
- ◆ 委託先所有ワークステーションの業務使用は禁止  
⇒ 自社ワークステーションの使用が必要な場合には、必ず、事前に所属長/プロジェクト責任者に相談してください
- ◆ IBMやお客様から貸与された以外の資産(購買取引先貸与資産や個人資産等)の外部記憶媒体を業務に使用することは禁止
- ◆ 外部記憶媒体に書き出しする場合は、暗号化すること
- ◆ 許可なく外部記憶媒体を、IBM事業所やお客様先から持ち出すことは禁止



(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

## ID/パスワードの使用ルール

- ◆ IBMのパスワード・ルールに準拠してください。
- ◆ 個人のIDは他者と共有してはいけません。
- ◆ IBM 管理下でないコンピューター・システムにアクセスする場合は、IBM 社内システムに使用するパスワードと同一のパスワードを使用してはなりません。



(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

本人であることを証明するパスワードを他に漏らしてはなりません。またいかなる他の人とも共用してはなりません。

パスワードは容易に推測される安直なものであってはなりません。また、以下の要件を満足するものでなければなりません。

- ・ 少なくとも 8桁
- ・ 英字(大文字／小文字)と非英字(数字、句読点、特殊文字)の混合を含むこと、あるいは、少なくとも2種類の非英字の混合を含むこと
- ・ パスワード中にユーザーIDの文字列を含まない

IBM機密情報を持つIBM 社内業務システムとアプリケーションでは、ユーザーは、パスワードを最低3ヶ月(90日)毎に変更しなければなりません。

パスワードを変更する場合は、過去2年間に使用したパスワードを再使用せず、新しいパスワードを選択して下さい。

## フリーソフトの使用

危険なぜい弱性の恐れのあるソフトウェアのダウンロードを避けるため、IBM の業務用として承認されているソフトウェア以外は原則使用禁止です。

日々の業務で使用する必要最小限のアプリケーションは、社内 ISSI から提供されています。

フリーソフトの使用の可否は、所属長/プロジェクト責任者に確認してください。



(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

## SNSの利用

- ◆ ブログや Facebook に代表されるSNS(ソーシャル・ネットワーキング・サービス)については、業務使用か否かに関わらず、利用する際は、必ずIBM ソーシャル・コンピューティングのガイドラインを一読し、日本IBMグループの業務を行う者として良識に基づいた活動を行ってください。
- ◆ SNSには、機密情報やお客様情報を掲載してはいけません。



### ◆ SNS の利用に関するガイドライン

<http://www.ibm.com/ibm/jp/about/partner/scg.html>

(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

## セクション 4

### その他全般のセキュリティ

(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.



## 入退館ルール

CASカードによる入退館管理、つまり会社が承認した人だけが入館できるということは、その他のセキュリティ対策が有効であるための大前提です。

- ◆ 事業所内では入館証を見やすい位置に着用してください。
- ◆ 入館証の貸し借りは厳禁です。
- ◆ テールゲート(自身の入館証をリーダーに通さず前の人について入館すること)はしないでください。
- ◆ 協力会社入館証(黄色バッジ)は、IBM事業所内で日常的にIBMの業務を行う場合に発行が許可されます。
- ◆ 入館証を忘れた場合は臨時バッジの貸与を受けて着用してください。

入館証は  
見やすい位置に



入館証の貸し借り  
は、絶対にしない



テールゲートは  
しない、させない



協力会社入館証  
(黄色バッジ)  
見本



(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

入館証は自身を証明するものです。お客様先では、お客様のルールに従い入館証を着用してください。

セキュリティ遵守事項を徹底し、必要がなくなった際は必ず返却してください。

## ワークスペース・セキュリティ

- ◆ 機密情報・個人情報を机の上などに放置しないでください。
- ◆ 長時間離席する場合は、ワークステーションの画面が第三者に閲覧できないようにしてください。
- ◆ 印刷物やファックスは速やかに回収してください。
- ◆ 事業所内での写真撮影、録音は原則禁止です。必要な場合は、所属長/プロジェクト管理者に相談してください。

情報を机の上に放置  
してはいけません。



パスワードが設定された  
スクリーンセーバーを



ファックスや印刷物は、  
速やかに回収



(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

皆さんが就業する場所(ワークスペース)では、ワークスペース・セキュリティ・ルールを遵守し、情報漏えいや盗難を未然に防止することが求められています。

長時間の離席や帰宅の際は、機密情報・個人情報を机の上に放置せず必ず施錠管理してください。

離席する際は、ワークステーションの画面が第三者に閲覧できないように、パスワードが設定されたスクリーンセーバーをかけるかワークステーションの蓋をしめるなど画面を保護してください。

長時間離席時のワークステーション盗難防止として、ワイヤーロックで固定してください。帰宅時は、ワークステーションをキャビネットや引き出しにて施錠管理してください。

印刷物やファックスは速やかに回収してください。長時間放置することは情報漏えいのリスクを高めます。



## 災害対策

大規模地震やパンデミック発生時、全社災害対策本部より出される指示に従い行動してください。プロジェクト、部門単位毎の対応手順および緊急連絡網の有無を確認してください。

### ◆ 日ごろの準備

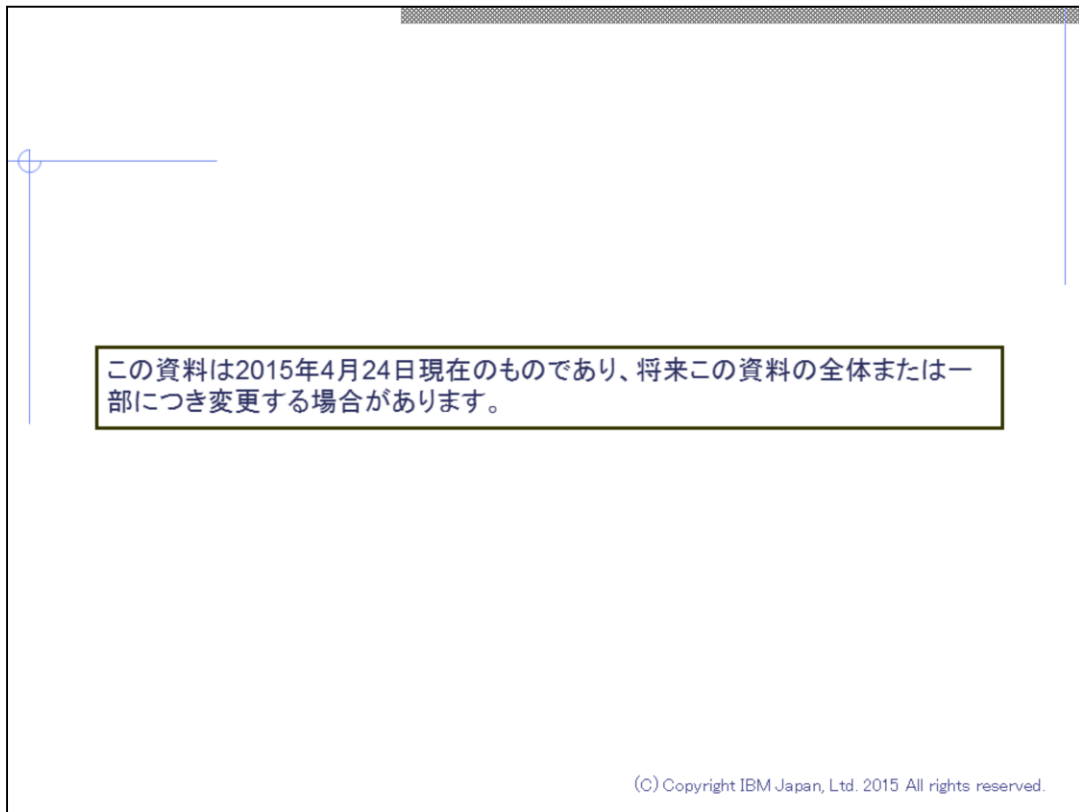
- 自分自身の**緊急連絡先情報**を常に最新にしておきましょう。
- 日本IBMグループ社員専用 **Twitter アカウント (@IBMer\_JP)** をフォローしてください。緊急時にはこのアカウントを用いて社内の方々向けの情報発信を行います。

### ◆ 災害時の行動

- 契約社員（臨時雇用社員）の場合は、直ちに所属長に連絡をとって指示に従ってください。
- 派遣社員、業務委託先社員の場合は、まず「自身の雇用会社」へ連絡をとり指示に従ってください。次にIBM側の派遣先責任者やプロジェクト責任者へ連絡してください。

(C) Copyright IBM Japan, Ltd. 2015 All rights reserved.

日本IBMグループは、さまざまな状況を想定して災害対策を講じています。日ごろから正しい理解の下に準備を行い、有事には適切に行動してください。



これでセキュリティ研修は終了です。

引き続き、理解度を確認するクイズを受けてください。  
クイズは、10問です。9問以上の正解で合格となります。