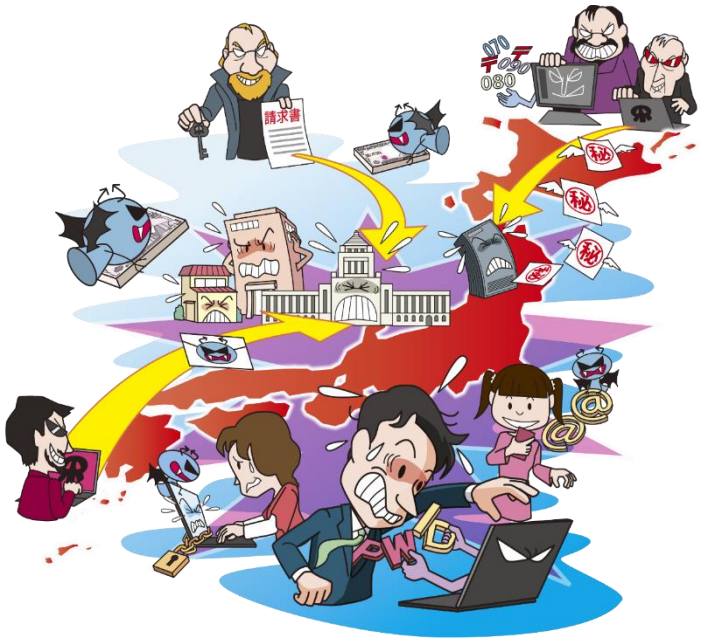
IPA Better Life with IT

「情報セキュリティ10大脅威 2016 ～ 個人編 ～」

～個人と組織で異なる脅威、立場ごとに適切な対応を～



独立行政法人情報処理推進機構（IPA）
技術本部 セキュリティセンター
2016年4月

目次

- 情報セキュリティ10大脅威について
- 1章. 10大脅威の10年史
- 2章. 情報セキュリティ10大脅威 2016
- 3章. 注目すべき脅威や懸念

情報セキュリティ10大脅威 2016

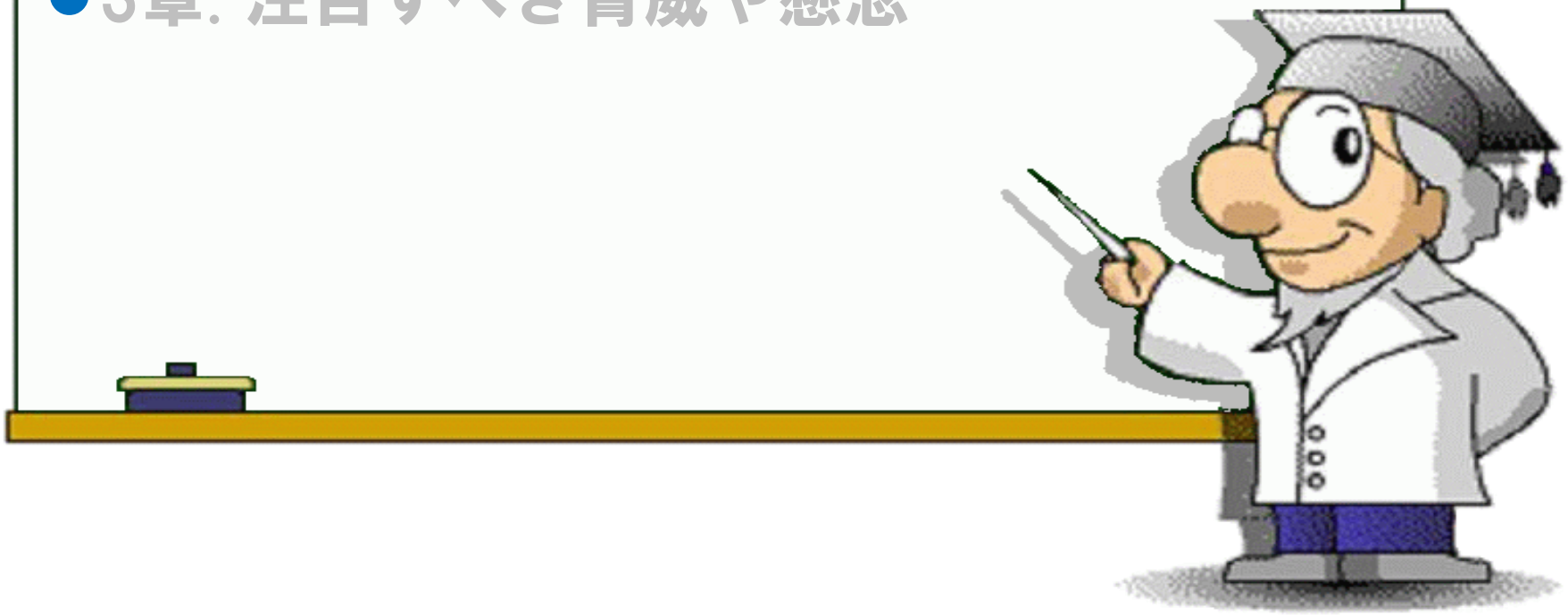
- 10大脅威とは？
  - 2006年よりIPAが毎年発行している資料
  - 「10大脅威選考会」約100名の投票により、情報システムを取巻く脅威を順位付けして解説

情報セキュリティ10大脅威 2016

- 章構成
  - 1章.10大脅威の10年史
    - 過去10年の10大脅威を振り返る
  - 2章.情報セキュリティ10大脅威 2016
    - 脅威の概要と対策について解説
  - 3章.注目すべき脅威や懸念
    - 知っておくべき脅威や懸念を解説

目次

- 情報セキュリティ10大脅威について
- **1章. 10大脅威の10年史**
- 2章. 情報セキュリティ10大脅威 2016
- 3章. 注目すべき脅威や懸念



10大脅威の10年史

10大脅威は10大脅威2006に始まり
10大脅威2015で10年目になりました

過去10年を3期間に分けて振り返る

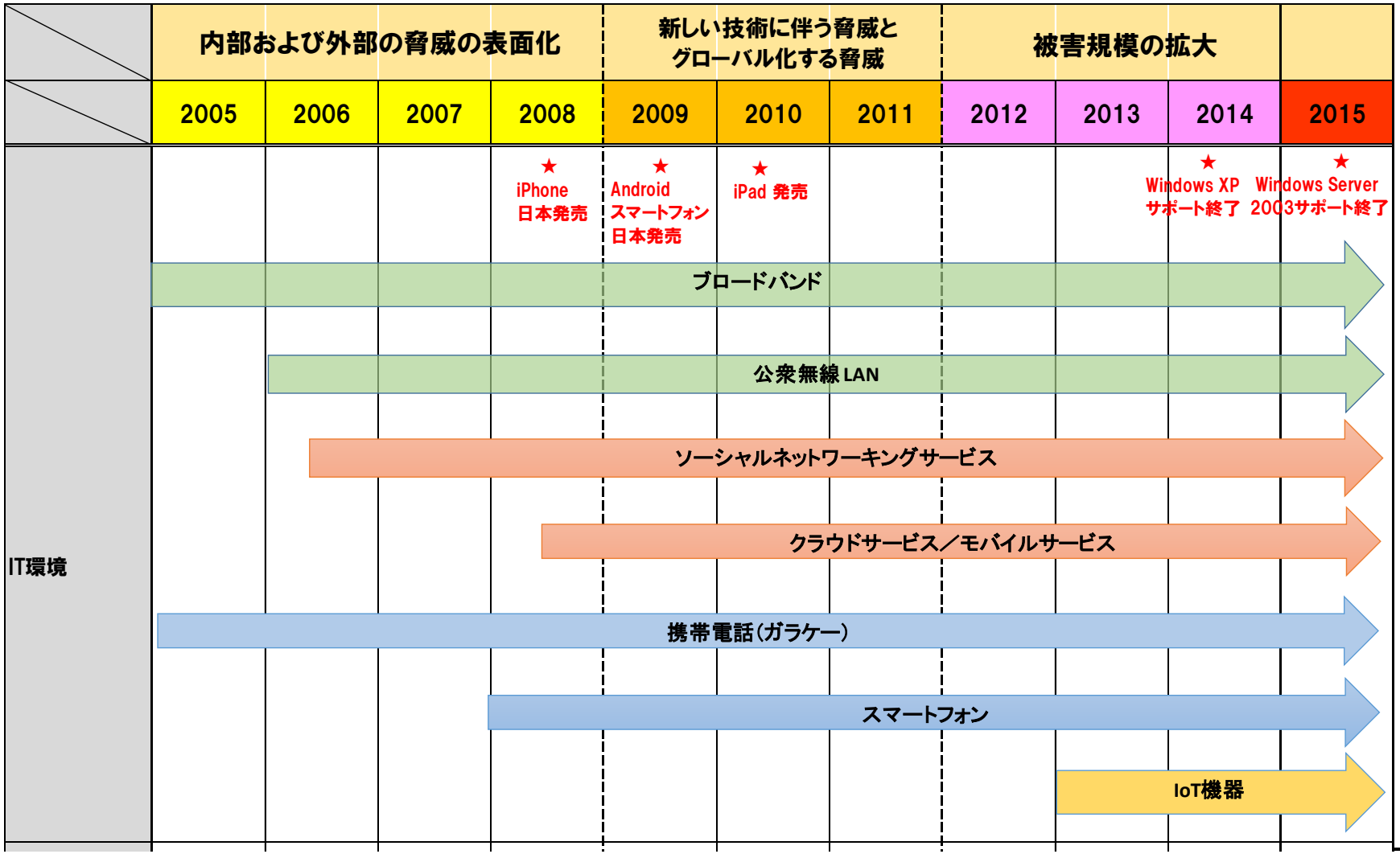
■2005年～2008年の4年間
（10大脅威2006～2009）

■2009年～2011年の3年間
（10大脅威2010～2012）

■2012年～2014年の3年間
（10大脅威2013～2015）

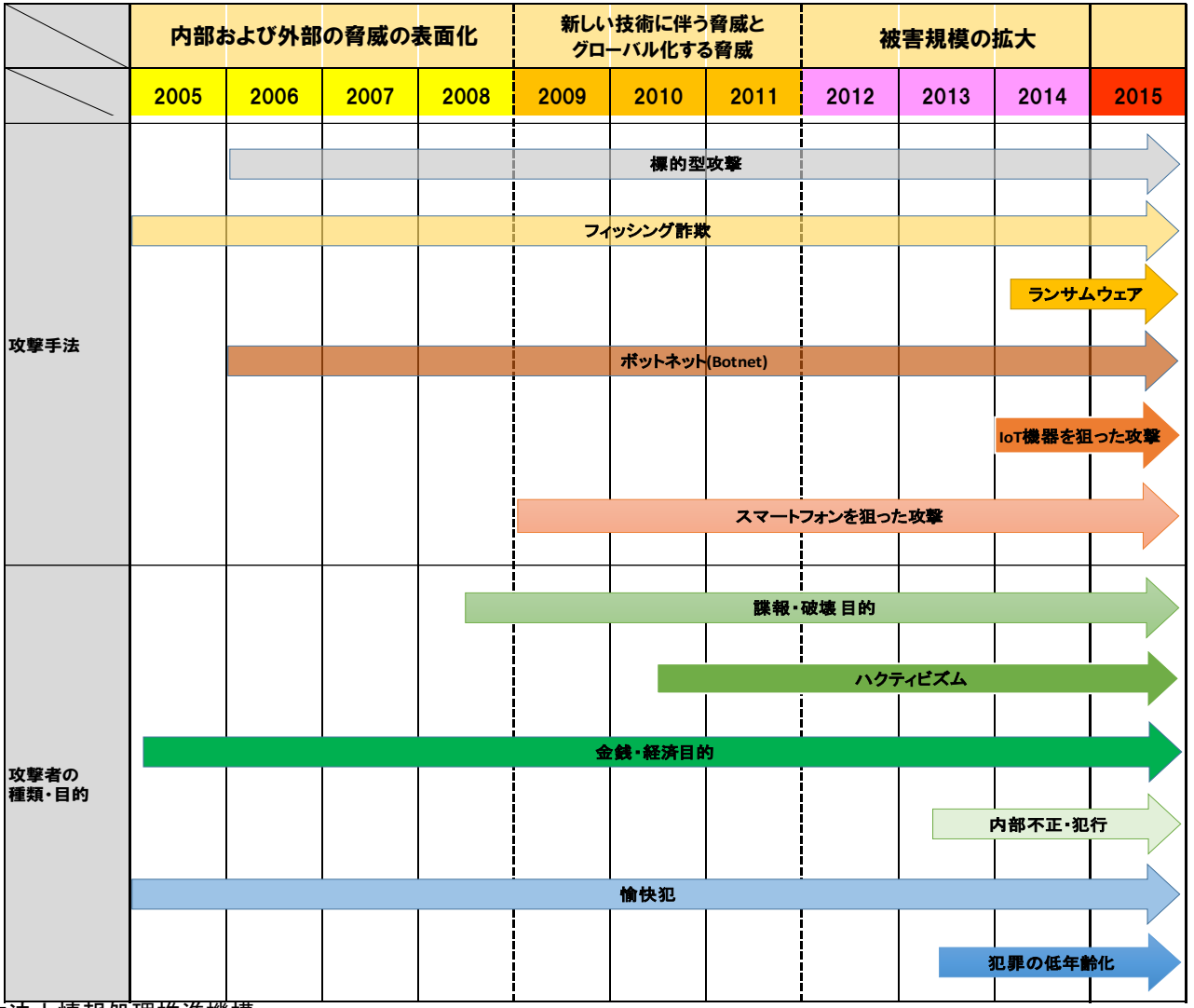
10大脅威の10年史

■ IT環境の変化



10大脅威の10年史

■ 攻撃手法と攻撃の目的



2005年～2008年

凡例：

脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネット バンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン 関連

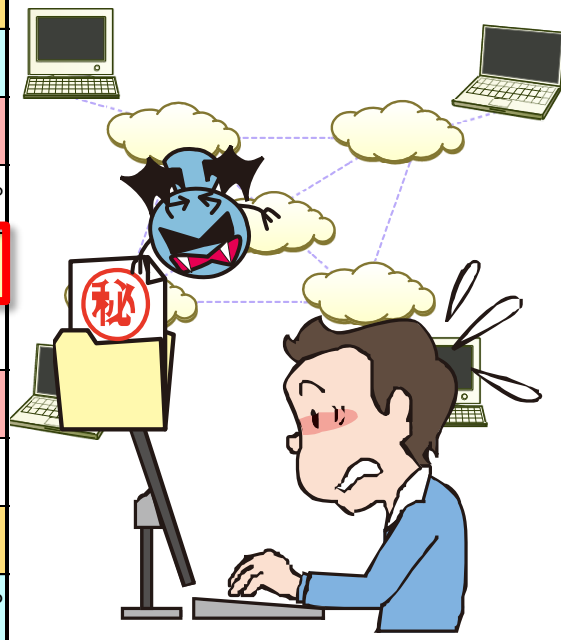
順位	2005年	2006年	2007年	2008年
1位	事件化するSQLインジェクション	漏えい情報のWinnyによる止らない流通	高まる「誘導型」攻撃の脅威	DNSキャッシュポイズニングの脅威
2位	Winnyを通じたウイルス感染による情報漏えいの多発	表面化しづらい標的型（スピア型）攻撃	ウェブサイトを狙った攻撃の広まり	正規ウェブサイトを経由した攻撃の猛威
3位	音楽CDに格納された「ルートキットに類似した機能」の事件化	悪質化・潜在化するボット	恒常化する情報漏えい	巧妙化する標的型攻撃
4位	悪質化するフィッシング詐欺	深刻化するゼロデイ攻撃	巧妙化する標的型攻撃	検知されにくいボット、潜在化するコンピュータウイルス
5位	巧妙化するスパイウェア	ますます多様化するフィッシング詐欺	信用できなくなった正規サイト	恒常化する情報漏えい
6位	流行が続くボット	増え続けるスパムメール	検知されにくいボット、潜在化するコンピュータウイルス	脆弱な無線LAN暗号方式における脅威
7位	ウェブサイトを狙うCSRFの流行	減らない情報漏えい	検索エンジンからマルウェア配信サイトに誘導	誘導型攻撃の顕在化
8位	情報家電、携帯機器などの組込みソフトウェアにひそむ脆弱性	狙われ続ける安易なパスワード	国内製品の脆弱性が頻発	減らないスパムメール
9位	セキュリティ製品の持つ脆弱性	攻撃が急増するSQLインジェクション	減らないスパムメール	組込み製品に潜む脆弱性
10位	ゼロデイ攻撃	不適切な設定のDNSサーバを狙う攻撃の発生	組み込み製品の脆弱性の増加	ユーザIDとパスワードの使いまわしによる危険性
10大脅威名	10大脅威2006	10大脅威2007	10大脅威2008	10大脅威2009

2005年～2008年

凡例：

脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネット バンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン 関連

順位	2005年	2006年	2007年	2008年
1位	事件化するSQLインジェクション	漏えい情報のWinnyによる止らない流通	高まる「誘導型」攻撃の脅威	DNSキャッシュポイズニングの脅威
2位	Winnyを通じたウイルス感染による情報漏えいの多発	表面化しづらい標的型（スピア型）攻撃	ウェブサイトを狙った攻撃の広まり	正規ウェブサイトを経由した攻撃の猛威
3位	音楽CDに格納された「ルートキットに類似した機能」の事件化	悪質化・潜在化するボット	恒常化する情報漏えい	巧妙化する標的型攻撃
4位	悪質化するフィッシング詐欺	深刻化するゼロデイ攻撃	巧妙化する標的型攻撃	検知されにくいボット、潜在化するコンピュータウイルス
5位	巧妙化するスパイウェア	ますます多様化するフィッシング詐欺	信用できなくなった正規サイト	恒常化する情報漏えい
6位	流行が続くボット	増え続けるスパムメール	検知されにくいボット、潜在化するコンピュータウイルス	脆弱な無線LAN暗号方式における脅威
7位	ウェブサイトを狙うCSRFの流行	減らない情報漏えい	検索エンジンからマルウェア配信サイトに誘導	誘導型攻撃の顕在化
8位	情報家電、携帯機器などの組込みソフトウェアにひそむ脆弱性	狙われ続ける安易なパスワード	国内製品の脆弱性が頻発	減らないスパムメール
9位	セキュリティ製品の持つ脆弱性	攻撃が急増するSQLインジェクション	減らないスパムメール	組込み製品に潜む脆弱性
10位	ゼロデイ攻撃	不適切な設定のDNSサーバを狙う攻撃の発生	組み込み製品の脆弱性の増加	ユーザIDとパスワードの使いまわしによる危険性
10大脅威名	10大脅威2006	10大脅威2007	10大脅威2008	10大脅威2009



■ Winnyによる情報漏えい被害拡大

- Antinnyウイルスによる情報漏えいで個人と組織で被害
- Winnyネットワーク上に流出した情報は次々に拡散
- 愉快目的

2005年～2008年

凡例：

脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネット バンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン 関連

順位	2005年	2006年	2007年	2008年
1位	事件化するSQLインジェクション	漏えい情報のWinnyによる止らない流通	高まる「誘導型」攻撃の脅威	DNSキャッシュポイズニングの脅威
2位	Winnyを通じたウイルス感染による情報漏えいの多発	表面化しづらい標的型（スピア型）攻撃	ウェブサイトを狙った攻撃の広まり	正規ウェブサイトを経由した攻撃の猛威
3位	音楽CDに格納された「ルートキットに類似した機能」の事件化	悪質化・潜在化するボット	恒常化する情報漏えい	巧妙化する標的型攻撃
4位	悪質化するフィッシング詐欺	深刻化するゼロデイ攻撃	巧妙化する標的型攻撃	検知されにくいボット、潜在化するコンピュータウイルス
5位	巧妙化するスパイウェア	ますます多様化するフィッシング詐欺	信用できなくなった正規サイト	恒常化する情報漏えい
6位	流行が続くボット	増え続けるスパムメール	検知されにくいボット、潜在化するコンピュータウイルス	脆弱な無線LAN暗号方式における脅威
7位	ウェブサイトを狙うCSRFの流行	減らない情報漏えい	検索エンジンからマルウェア配信サイトに誘導	誘導型攻撃の顕在化
8位	情報家電、携帯機器などの組込みソフトウェアにひそむ脆弱性	狙われ続ける安易なパスワード	国内製品の脆弱性が頻発	減らないスパムメール
9位	セキュリティ製品の持つ脆弱性	攻撃が急増するSQLインジェクション	減らないスパムメール	組込み製品に潜む脆弱性
10位	ゼロデイ攻撃	不適切な設定のDNSサーバを狙う攻撃の発生	組み込み製品の脆弱性の増加	ユーザIDとパスワードの使いまわしによる危険性
10大脅威名	10大脅威2006	10大脅威2007	10大脅威2008	10大脅威2009

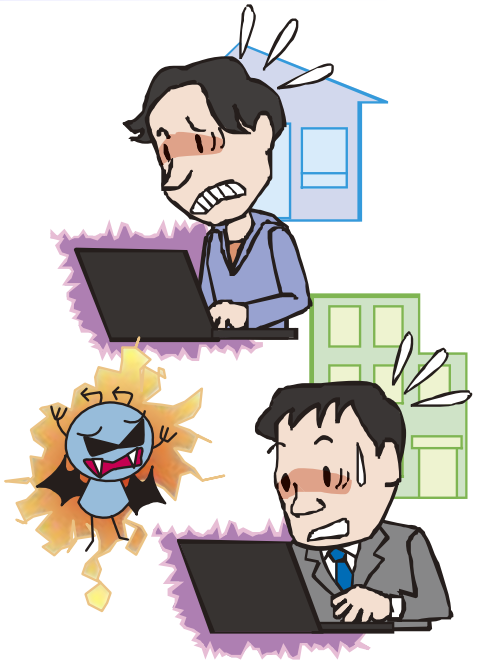
- **狙われる組織の情報、標的型攻撃の登場**
  - ・10年前から存在する標的型攻撃
  - ・2006年以降常に10大脅威に登場

2005年～2008年

凡例：

脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネット バンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン 関連

順位	2005年	2006年	2007年	2008年
1位	事件化するSQLインジェクション	漏えい情報のWinnyによる止らない流通	高まる「誘導型」攻撃の脅威	DNSキャッシュポイズニングの脅威
2位	Winnyを通じたウイルス感染による情報漏えいの多発	表面化しづらい標的型（スピア型）攻撃	ウェブサイトを狙った攻撃の広まり	正規ウェブサイトを経由した攻撃の猛威
3位	音楽CDに格納された「ルートキットに類似した機能」の事件化	悪質化・潜在化するボット	恒常化する情報漏えい	巧妙化する標的型攻撃
4位	悪質化するフィッシング詐欺	深刻化するゼロデイ攻撃	巧妙化する標的型攻撃	検知されにくいボット、潜在化するコンピュータウイルス
5位	巧妙化するスパイウェア	ますます多様化するフィッシング詐欺	信用できなくなった正規サイト	恒常化する情報漏えい
6位	流行が続くボット	増え続けるスパムメール	検知されにくいボット、潜在化するコンピュータウイルス	脆弱な無線LAN暗号方式における脅威
7位	ウェブサイトを狙うCSRFの流行	減らない情報漏えい	検索エンジンからマルウェア配信サイトに誘導	誘導型攻撃の顕在化
8位	情報家電、携帯機器などの組込みソフトウェアにひそむ脆弱性	狙われ続ける安易なパスワード	国内製品の脆弱性が頻発	減らないスパムメール
9位	セキュリティ製品の持つ脆弱性	攻撃が急増するSQLインジェクション	減らないスパムメール	組込み製品に潜む脆弱性
10位	ゼロデイ攻撃	不適切な設定のDNSサーバを狙う攻撃の発生	組み込み製品の脆弱性の増加	ユーザIDとパスワードの使いまわしによる危険性
10大脅威名	10大脅威2006	10大脅威2007	10大脅威2008	10大脅威2009



■ 10年以上前から存在する脆弱性にかかわる脅威

- 脆弱性の脅威は今も昔も変わっていない
- 狙われるのはウェブサイトやクライアントのソフトウェア

2009年～2011年

凡例：

脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネット バンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン 関連

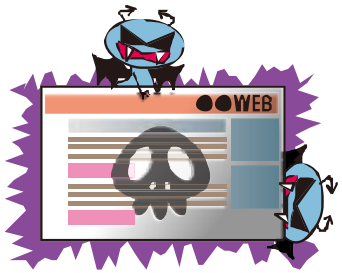
順位	2009年	2010年	2011年
1位	変化を続けるウェブサイト改ざんの手口	「人」が起こしてしまう情報漏えい	機密情報が盗まれる！？新しいタイプの攻撃
2位	アップデートしていないクライアントソフト	止らない！ウェブサイトを経由した攻撃	予測不能の災害発生！引き起こされた業務停止
3位	悪質なウイルスやボットの多目的化	定番ソフトウェアの脆弱性を狙った攻撃	特定できぬ、共通思想集団による攻撃
4位	対策をしていないサーバ製品の脆弱性	狙われだしたスマートフォン	今もどこかで･･･更新忘れのクライアントソフトを狙った攻撃
5位	あわせて事後対応を！情報漏えい事件	複数の攻撃を組み合わせた新しいタイプの攻撃	止らない！ウェブサイトを狙った攻撃
6位	被害に気づけない標的型攻撃	セキュリティ対策不備がもたらすトラブル	続々発覚、スマートフォンやタブレットを狙った攻撃
7位	深刻なDDoS攻撃	携帯電話向けウェブサイトのセキュリティ	大丈夫！？電子証明書に思わぬ落とし穴
8位	正規のアカウントを悪用される攻撃	攻撃に気づけない標的型攻撃	身近に潜む魔の手･･･あなたの職場は大丈夫？
9位	クラウド･コンピューティングのセキュリティ問題	クラウド･コンピューティングのセキュリティ	危ない！アカウントの使いまわしが被害を拡大！
10位	インターネットインフラを支えるプロトコルの脆弱性	ミニブログサービスやSNSの利用者を狙った攻撃	使用者情報の不適切な取扱いによる信用失墜
10大脅威名	10大脅威2010	10大脅威2011	10大脅威2012

2009年～2011年

凡例：

脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネット バンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン 関連

順位	2009年	2010年	2011年
1位	変化を続けるウェブサイト改ざんの手口	「人」が起こしてしまう情報漏えい	機密情報が盗まれる！？新しいタイプの攻撃
2位	アップデートしていないクライアントソフト	止らない！ウェブサイトを経由した攻撃	予測不能の災害発生！引き起こされた業務停止
3位	悪質なウイルスやボットの多目的化	定番ソフトウェアの脆弱性を狙った攻撃	特定できぬ、共通思想集団による攻撃
4位	対策をしていないサーバ製品の脆弱性	狙われだしたスマートフォン	今もどこかで・・・更新忘れのクライアントソフトを狙った攻撃
5位	あわせて事後対応を！情報漏えい事件	複数の攻撃を組み合わせた新しいタイプの攻撃	止らない！ウェブサイトを狙った攻撃
6位	被害に気づけない標的型攻撃	セキュリティ対策不備がもたらすトラブル	続々発覚、スマートフォンやタブレットを狙った攻撃
7位	深刻なDDoS攻撃	携帯電話向けウェブサイトのセキュリティ	大丈夫！？電子証明書に思わぬ落とし穴
8位	正規のアカウントを悪用される攻撃	攻撃に気づけない標的型攻撃	身近に潜む魔の手・・・あなたの職場は大丈夫？
9位	クラウド・コンピューティングのセキュリティ問題	クラウド・コンピューティングのセキュリティ	危ない！アカウントの使いまわしが被害を拡大！
10位	インターネットインフラを支えるプロトコルの脆弱性	ミニブログサービスやSNSの利用者を狙った攻撃	使用者情報の不適切な取扱いによる信用失墜
10大脅威名	10大脅威2010	10大脅威2011	10大脅威2012



- **猛威を振るうガンブラー被害、懸念される脆弱性の脅威**
  - ・ウェブサイトが改ざんされ、利用者にウイルスが感染
  - ・ウイルス感染には脆弱性を悪用
  - ・2011年には収束

2009年～2011年

凡例：

脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネット バンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン 関連

順位	2009年	2010年	2011年
1位	変化を続けるウェブサイト改ざんの手口	「人」が起こしてしまう情報漏えい	機密情報が盗まれる！？新しいタイプの攻撃
2位	アップデートしていないクライアントソフト	止らない！ウェブサイトを経由した攻撃	予測不能の災害発生！引き起こされた業務停止
3位	悪質なウイルスやボットの多目的化	定番ソフトウェアの脆弱性を狙った攻撃	特定できぬ、共通思想集団による攻撃
4位	対策をしていないサーバ製品の脆弱性	狙われだしたスマートフォン	今もどこかで･･･更新忘れのクライアントソフトを狙った攻撃
5位	あわせて事後対応を！情報漏えい事件	複数の攻撃を組み合わせた新しいタイプの攻撃	止らない！ウェブサイトを狙った攻撃
6位	被害に気づけない標的型攻撃	セキュリティ対策不備がもたらすトラブル	続々発覚、スマートフォンやタブレットを狙った攻撃
7位	深刻なDDoS攻撃	携帯電話向けウェブサイトのセキュリティ	大丈夫！？電子証明書に思わぬ落とし穴
8位	正規のアカウントを悪用される攻撃	攻撃に気づけない標的型攻撃	身近に潜む魔の手･･･あなたの職場は大丈夫？
9位	クラウド･コンピューティングのセキュリティ問題	クラウド･コンピューティングのセキュリティ	危ない！アカウントの使いまわしが被害を拡大！
10位	インターネットインフラを支えるプロトコルの脆弱性	ミニブログサービスやSNSの利用者を狙った攻撃	使用者情報の不適切な取扱いによる信用失墜
10大脅威名	10大脅威2010	10大脅威2011	10大脅威2012

■ 現実化した事業継続の必要性

- 2011年3月11日の東日本大震災により企業に甚大な被害
- BCP（事業継続計画）の考え方に注目

2009年～2011年

凡例：

脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネット バンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン 関連

順位	2009年	2010年	2011年
1位	変化を続けるウェブサイト改ざんの手口	「人」が起こしてしまう情報漏えい	機密情報が盗まれる！？新しいタイプの攻撃
2位	アップデートしていないクライアントソフト	止らない！ウェブサイトを経由した攻撃	予測不能の災害発生！引き起こされた業務停止
3位	悪質なウイルスやボットの多目的化	定番ソフトウェアの脆弱性を狙った攻撃	特定できぬ、共通思想集団による攻撃
4位	対策をしていないサーバ製品の脆弱性	狙われだしたスマートフォン	今もどこかで･･･更新忘れのクライアントソフトを狙った攻撃
5位	あわせて事後対応を！情報漏えい事件	複数の攻撃を組み合わせた新しいタイプの攻撃	止らない！ウェブサイトを狙った攻撃
6位	被害に気づけない標的型攻撃	セキュリティ対策不備がもたらすトラブル	続々発覚、スマートフォンやタブレットを狙った攻撃
7位	深刻なDDoS攻撃	携帯電話向けウェブサイトのセキュリティ	大丈夫！？電子証明書に思わぬ落とし穴
8位	正規のアカウントを悪用される攻撃	攻撃に気づけない標的型攻撃	身近に潜む魔の手･･･あなたの職場は大丈夫？
9位	クラウド･コンピューティングのセキュリティ問題	クラウド･コンピューティングのセキュリティ	危ない！アカウントの使いまわしが被害を拡大！
10位	インターネットインフラを支えるプロトコルの脆弱性	ミニブログサービスやSNSの利用者を狙った攻撃	使用者情報の不適切な取扱いによる信用失墜
10大脅威名	10大脅威2010	10大脅威2011	10大脅威2012

- **集団によるサイバー攻撃の被害の表面化**
  - **・複数の国や組織の人間で構成されたハクティビストによる社会的･政治的な主張を目的としたサイバー攻撃の被害**
  - **・ウェブサイトを改ざんやサービス妨害で攻撃**

2012年～2014年

凡例：

脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネット バンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン 関連

順位	2012年	2013年	2014年
1位	クライアントソフトの脆弱性を突いた攻撃	標的型メールを用いた組織へのスパイ・諜報活動	インターネットバンキングやクレジットカード情報の不正利用
2位	標的型諜報攻撃の脅威	不正ログイン・不正利用	内部不正による情報漏えい
3位	スマートデバイスを狙った悪意あるアプリの横行	ウェブサイトの改ざん	標的型攻撃による諜報活動
4位	ウイルスを使った遠隔操作	ウェブサービスからの利用者情報の漏えい	ウェブサービスへの不正ログイン
5位	金銭窃取を目的としたウイルスの横行	オンラインバンキングからの不正送金	ウェブサービスからの顧客情報の窃取
6位	予期せぬ業務停止	悪意あるスマートフォンアプリ	ハッカー集団によるサイバーテロ
7位	ウェブサイトを狙った攻撃	SNSへの不適切な情報公開	ウェブサイトの改ざん
8位	パスワード流出の脅威	紛失や設定不備による情報漏えい	インターネット基盤技術を悪用した攻撃
9位	内部犯行	ウイルスを使った詐欺・恐喝	脆弱性公表に伴う攻撃
10位	フィッシング詐欺	サービス妨害	悪意のあるスマートフォンアプリ
10大脅威名	10大脅威2013	10大脅威2014	10大脅威2015

2012年～2014年

凡例：

脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネット バンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン 関連

順位	2012年	2013年	2014年
1位	クライアントソフトの脆弱性を突いた攻撃	標的型メールを用いた組織へのスパイ・諜報活動	インターネットバンキングやクレジットカード情報の不正利用
2位	標的型諜報攻撃の脅威	不正ログイン・不正利用	内部不正による情報漏えい
3位	スマートデバイスを狙った悪意あるアプリの横行	ウェブサイトの改ざん	標的型攻撃による諜報活動
4位	ウイルスを使った遠隔操作	ウェブサービスからの利用者情報の漏えい	ウェブサービスへの不正ログイン
5位	金銭窃取を目的としたウイルスの横行	オンラインバンキングからの不正送金	ウェブサービスからの顧客情報の窃取
6位	予期せぬ業務停止	悪意あるスマートフォンアプリ	ハッカー集団によるサイバーテロ
7位	ウェブサイトを狙った攻撃	SNSへの不適切な情報公開	ウェブサイトの改ざん
8位	パスワード流出の脅威	紛失や設定不備による情報漏えい	インターネット基盤技術を悪用した攻撃
9位	内部犯行	ウイルスを使った詐欺・恐喝	脆弱性公表に伴う攻撃
10位	フィッシング詐欺	サービス妨害	悪意のあるスマートフォンアプリ
10大脅威名	10大脅威2013	10大脅威2014	10大脅威2015

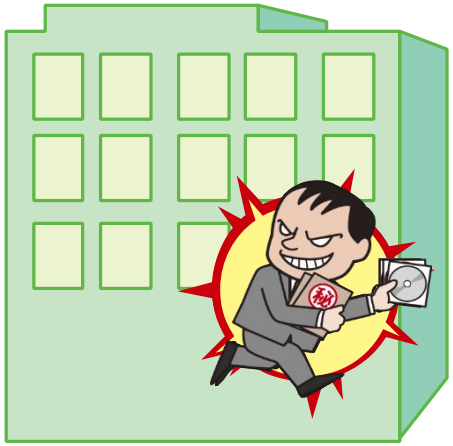
- **金銭被害拡大、狙われるインターネットバンキング・クレジットカード**
  - **インターネットバンキングやクレジットカード情報の不正利用**
  - **総被害額は、2012年が約4,800万円、2013年が約14億600万円、2014年が約29億1,000万円**

2012年～2014年

凡例：

脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネット バンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン 関連

順位	2012年	2013年	2014年
1位	クライアントソフトの脆弱性を突いた攻撃	標的型メールを用いた組織へのスパイ・諜報活動	インターネットバンキングやクレジットカード情報の不正利用
2位	標的型諜報攻撃の脅威	不正ログイン・不正利用	内部不正による情報漏えい
3位	スマートデバイスを狙った悪意あるアプリの横行	ウェブサイトの改ざん	標的型攻撃による諜報活動
4位	ウイルスを使った遠隔操作	ウェブサービスからの利用者情報の漏えい	ウェブサービスへの不正ログイン
5位	金銭窃取を目的としたウイルスの横行	オンラインバンキングからの不正送金	ウェブサービスからの顧客情報の窃取
6位	予期せぬ業務停止	悪意あるスマートフォンアプリ	ハッカー集団によるサイバーテロ
7位	ウェブサイトを狙った攻撃	SNSへの不適切な情報公開	ウェブサイトの改ざん
8位	パスワード流出の脅威	紛失や設定不備による情報漏えい	インターネット基盤技術を悪用した攻撃
9位	内部犯行	ウイルスを使った詐欺・恐喝	脆弱性公表に伴う攻撃
10位	フィッシング詐欺	サービス妨害	悪意のあるスマートフォンアプリ
10大脅威名	10大脅威2013	10大脅威2014	10大脅威2015



■ 内部犯行により持ち出される個人情報

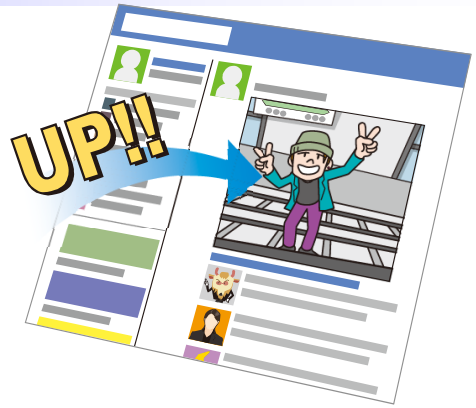
- 内部犯行により個人情報が漏えい
- 権限がある従業員がその権限を使って個人情報を窃取
- 顧客への補償として200億円を用意したケースも

2012年～2014年

凡例：

脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネット バンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン 関連

順位	2012年	2013年	2014年
1位	クライアントソフトの脆弱性を突いた攻撃	標的型メールを用いた組織へのスパイ・諜報活動	インターネットバンキングやクレジットカード情報の不正利用
2位	標的型諜報攻撃の脅威	不正ログイン・不正利用	内部不正による情報漏えい
3位	スマートデバイスを狙った悪意あるアプリの横行	ウェブサイトの改ざん	標的型攻撃による諜報活動
4位	ウイルスを使った遠隔操作	ウェブサービスからの利用者情報の漏えい	ウェブサービスへの不正ログイン
5位	金銭窃取を目的としたウイルスの横行	オンラインバンキングからの不正送金	ウェブサービスからの顧客情報の窃取
6位	予期せぬ業務停止	悪意あるスマートフォンアプリ	ハッカー集団によるサイバーテロ
7位	ウェブサイトを狙った攻撃	SNSへの不適切な情報公開	ウェブサイトの改ざん
8位	パスワード流出の脅威	紛失や設定不備による情報漏えい	インターネット基盤技術を悪用した攻撃
9位	内部犯行	ウイルスを使った詐欺・恐喝	脆弱性公表に伴う攻撃
10位	フィッシング詐欺	サービス妨害	悪意のあるスマートフォンアプリ
10大脅威名	10大脅威2013	10大脅威2014	10大脅威2015



■ 軽率な情報配信行為による脅威

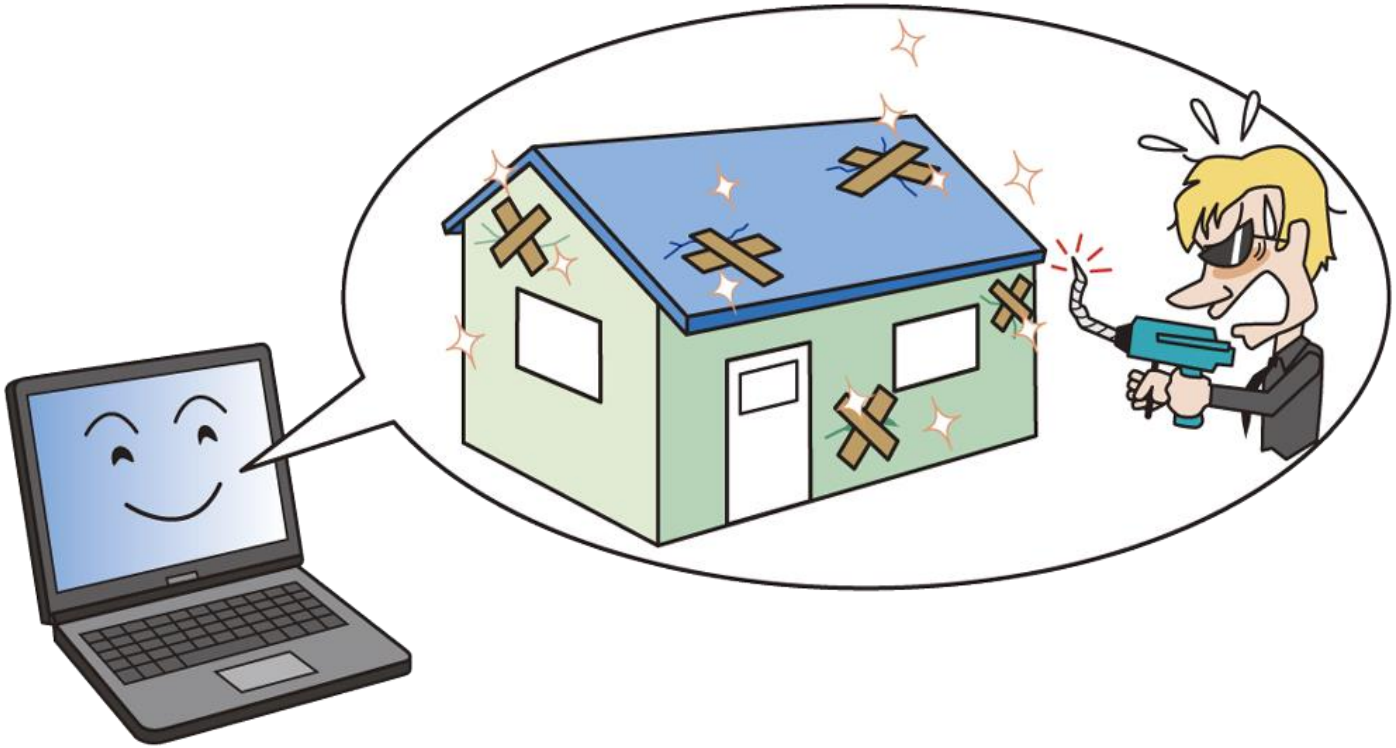
- 若者や従業員による軽率な行為や発言を配信し、炎上
- 被害を受けた企業には倒産等、甚大な被害を受けるケースも
- 当人も多額の賠償金や降格、停職等の処分がされている

情報セキュリティ対策の基本

情報セキュリティ対策の基本
ソフトウェアの更新
ウイルス対策ソフトの導入
パスワード・認証の強化
設定の見直し
脅威・手口を知る

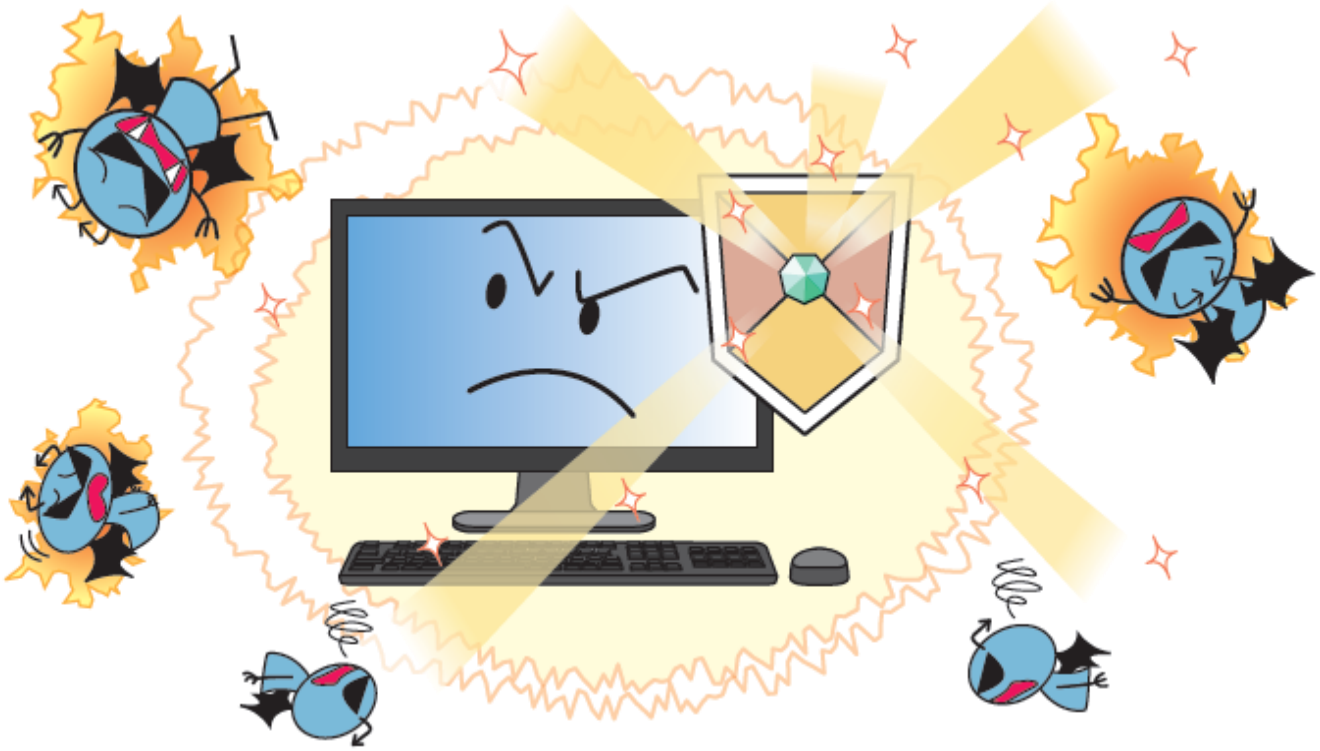
10大脅威の順位は毎年変動するが、
　上記の基本的な対策の必要性は長年変わらない
IT利用者には「**自発的な対策の実施**」が求められている

ソフトウェアの更新



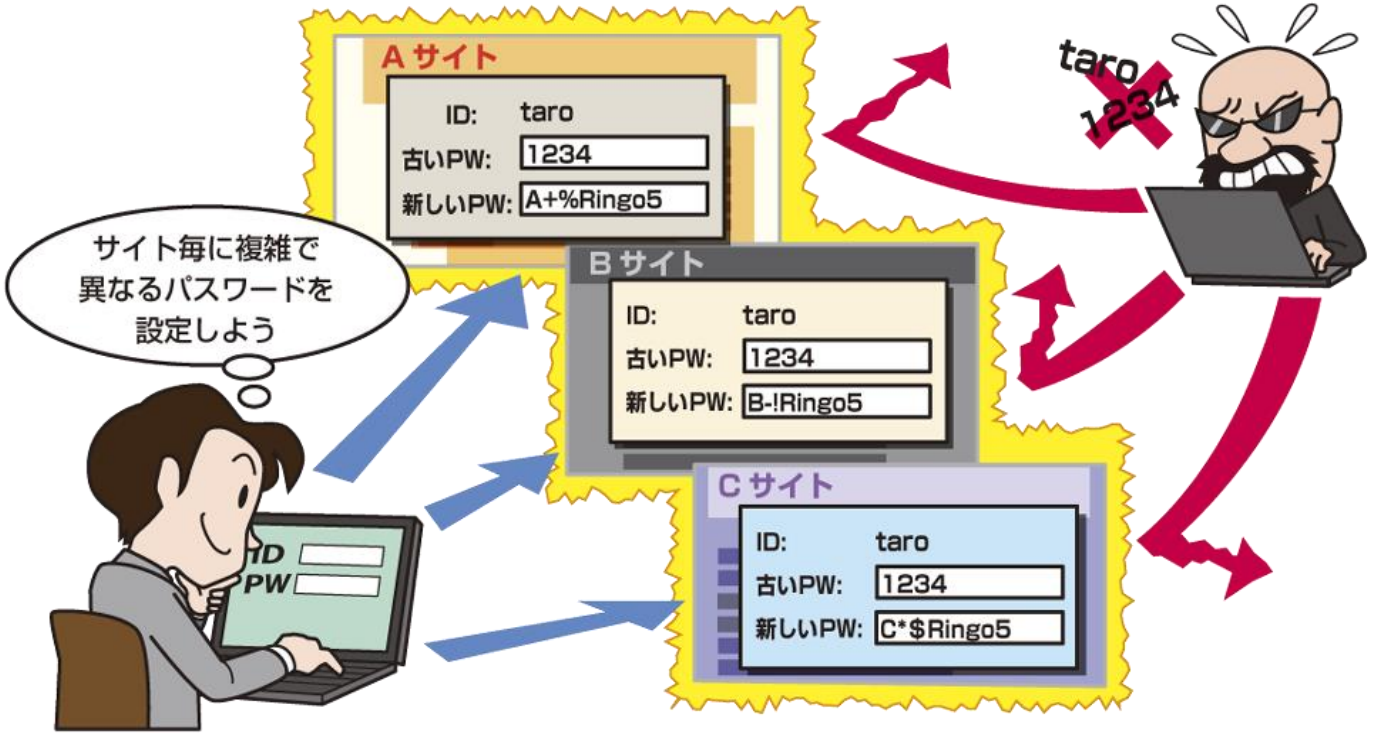
- ソフトウェアの欠陥である脆弱性は、
  ソフトウェアを更新して根本的に解消する

ウイルス対策ソフトの導入



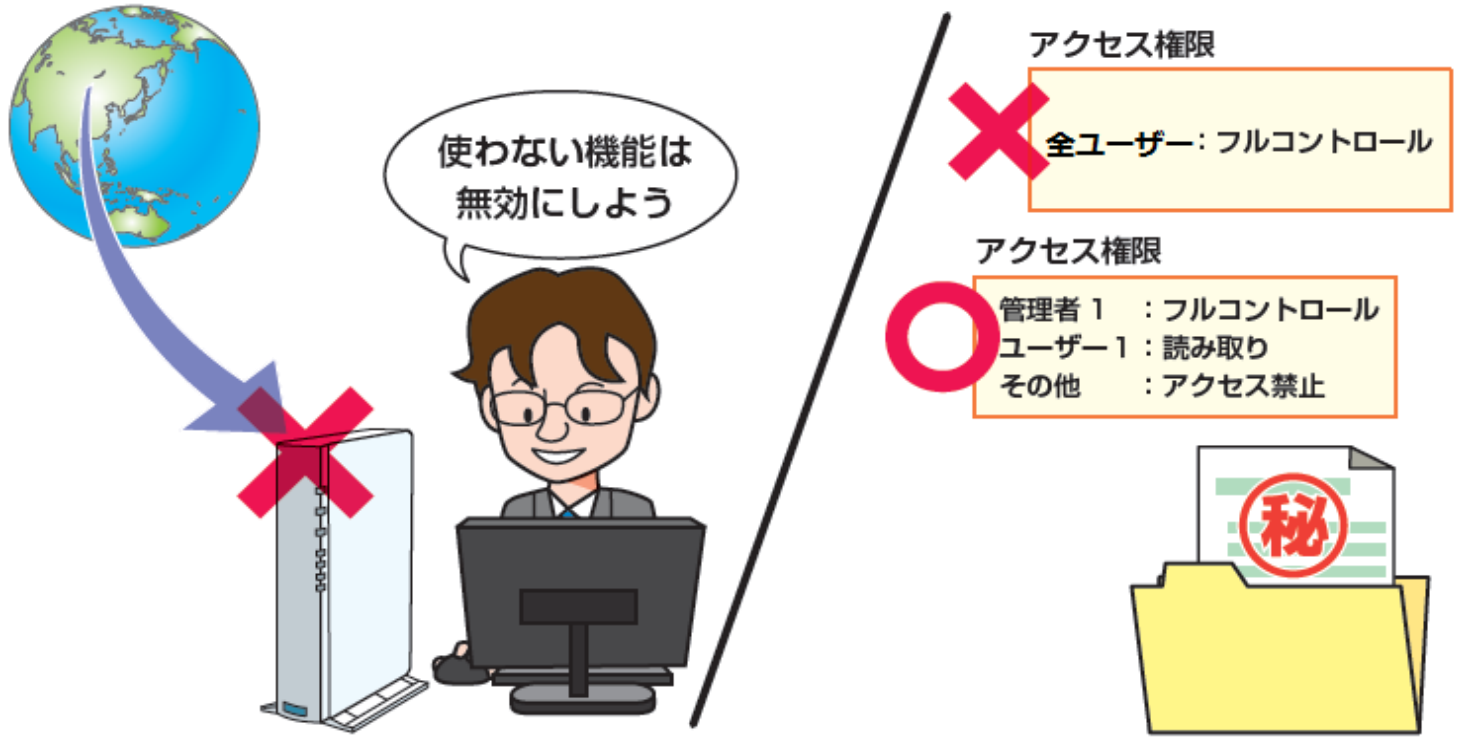
- ウイルス対策ソフトを導入し、
  流行しているウイルスの感染を未然に防ぐ

パスワードの適切な管理と認証の強化



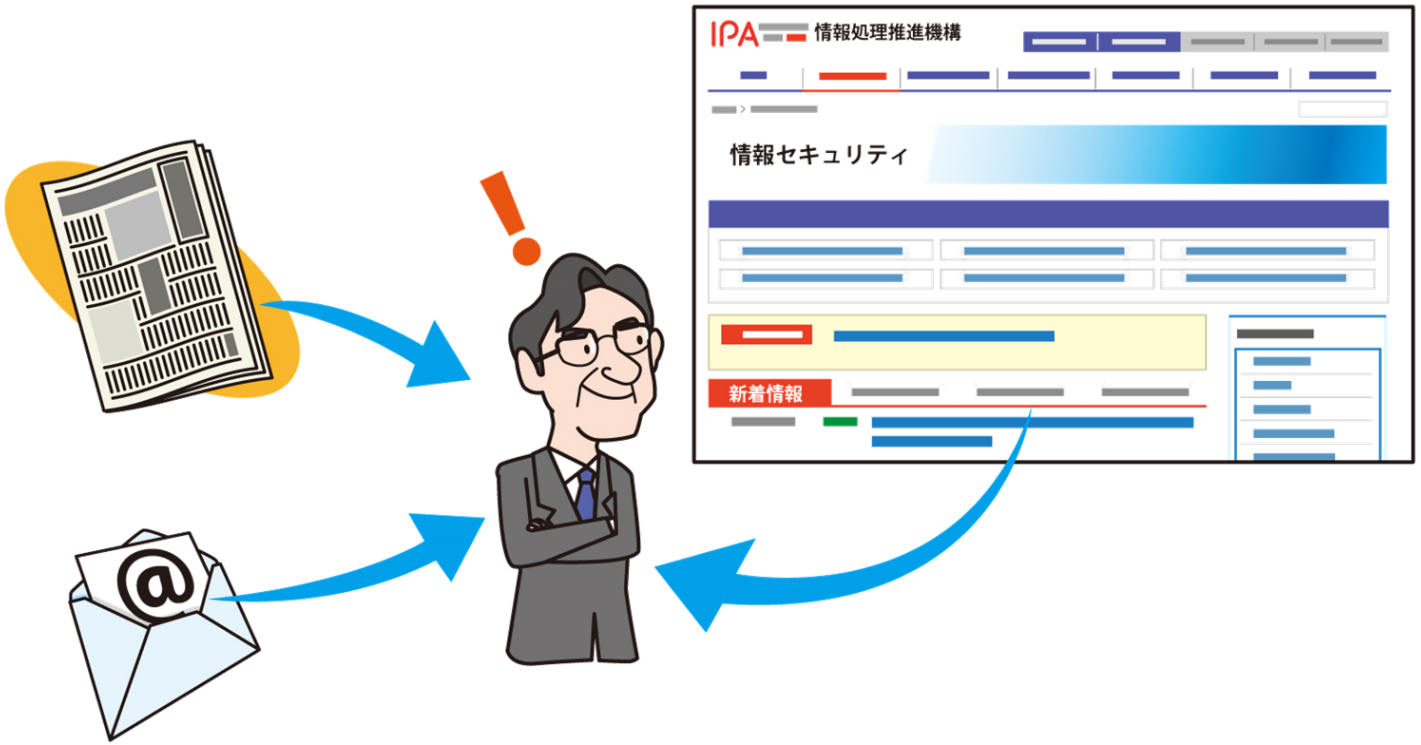
- 推測されにくい
  「記号・英数字」を含む「十分な文字数」のパスワードを設定
- 複数のウェブサービスでパスワードを使い回さない
- 二要素認証等、強い認証方式が利用できれば利用する

設定の見直し



- 不要な設定は無効にする
- フォルダや顧客管理システム等への
  アクセス制限を適切に行う

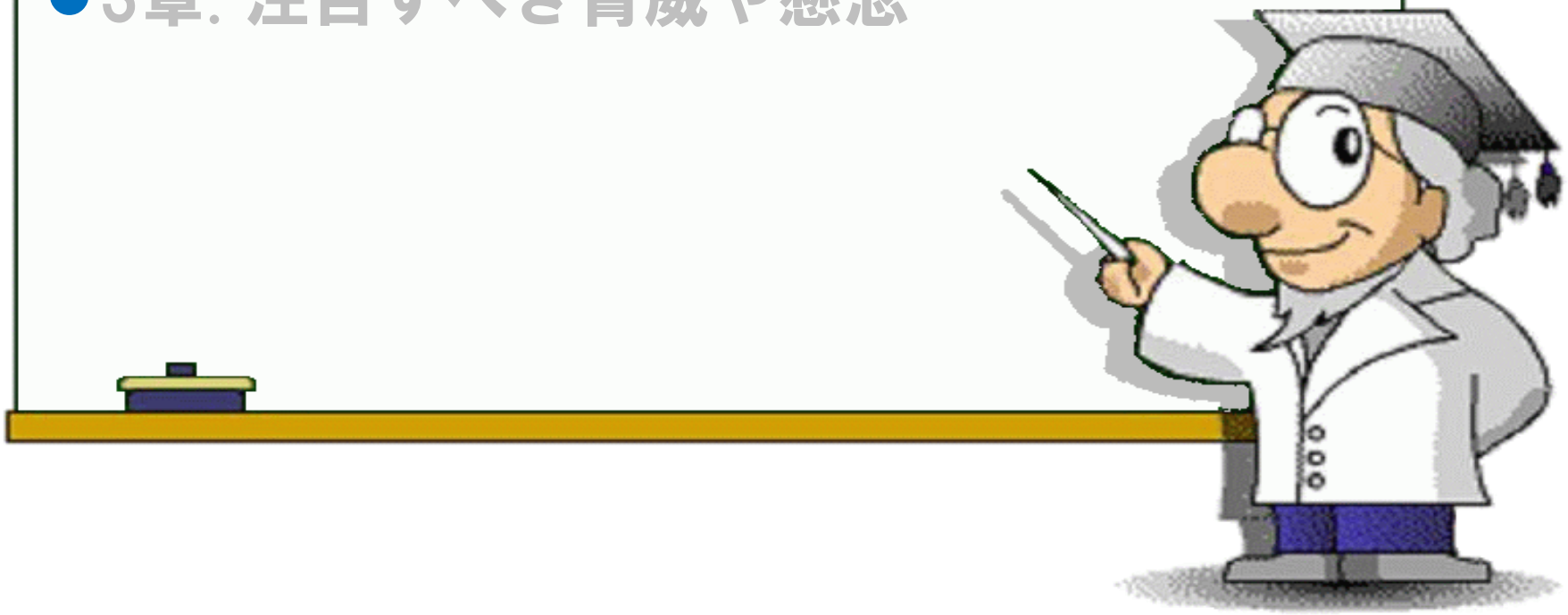
脅威や手口を知る



- 新聞やインターネット等から情報を自発的に収集し、被害に遭わないよう手口を事前に知る

目次

- 情報セキュリティ10大脅威について
- 1章. 10大脅威の10年史
- **2章. 情報セキュリティ10大脅威 2016**
- 3章. 注目すべき脅威や懸念



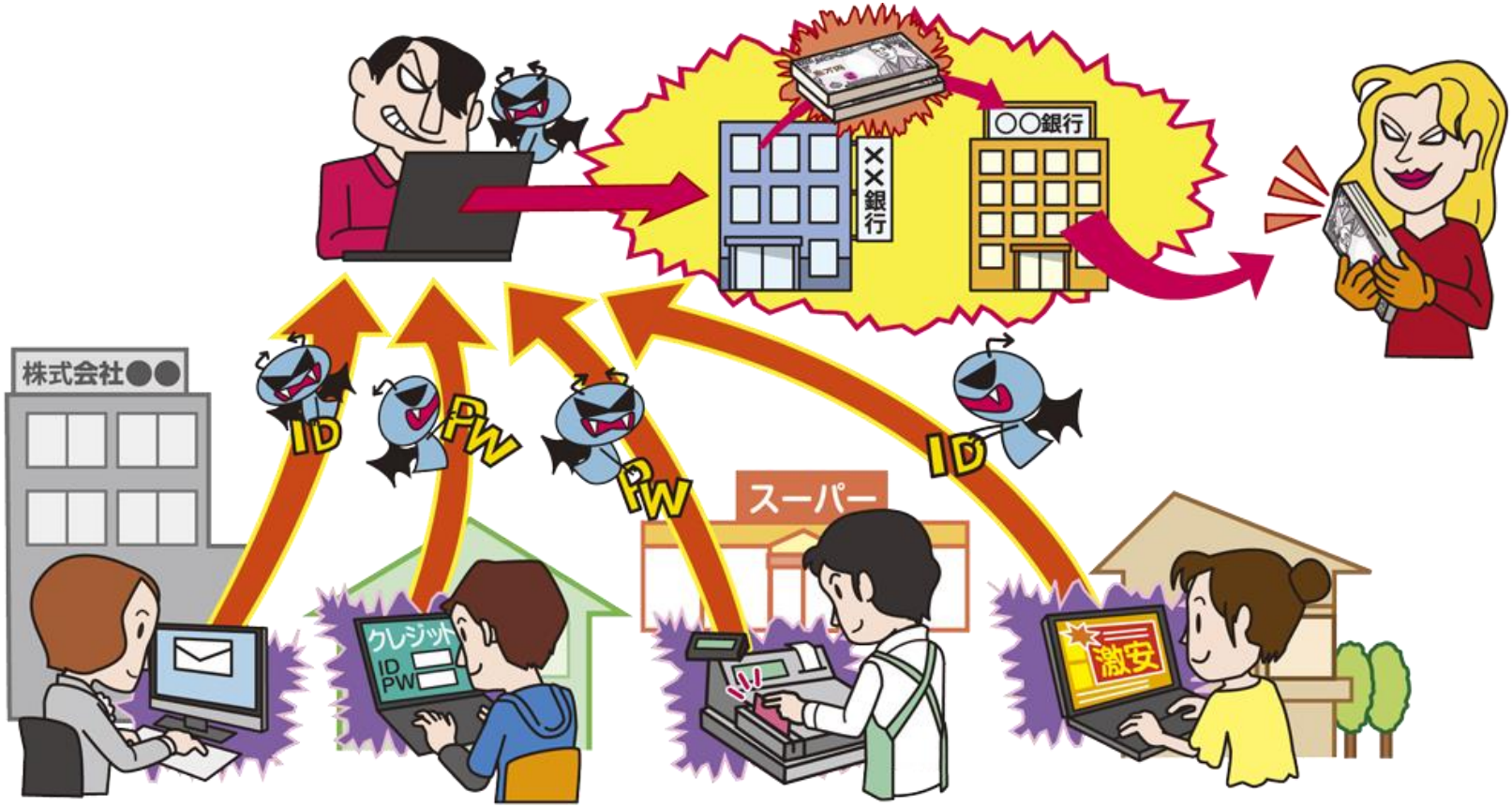
情報セキュリティ10大脅威 2016
（個人：5位まで抜粋）

IPA

順位	脅威
1位	インターネットバンキングや クレジットカード情報の不正利用
2位	ランサムウェアを使った詐欺・恐喝
3位	審査をすり抜け公式マーケットに 紛れ込んだスマートフォンアプリ
4位	巧妙・悪質化するワンクリック請求
5位	ウェブサービスへの不正ログイン

【1位】インターネットバンキングやクレジットカード情報の不正利用

～拡大する攻撃対象、様々な手段で金銭取引の重要な情報を収集～

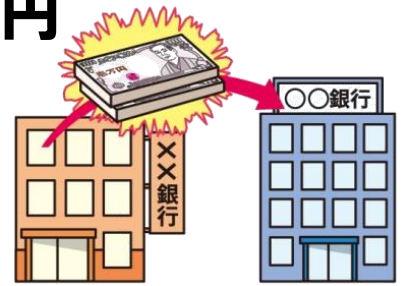


- ウイルスやフィッシング詐欺により認証情報が窃取され、不正送金される

【1位】インターネットバンキングやクレジットカード情報の不正利用

～拡大する攻撃対象、様々な手段で金銭取引の重要な情報を収集～

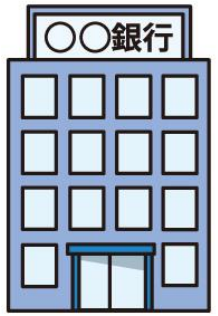
- 手口/影響
  - ウイルスに感染したパソコンが不正送金の被害に遭う
  - フィッシング詐欺により入力した認証情報が窃取される
- 2015年の事例/傾向
  - 不正送金被害が急増
    - 日本のインターネットバンキング利用者を狙う
      ウイルスが横行！
    - 2015年の被害額は30億7,300万円、
      2014年は29億1,000万円
      昨年に引き続き法人口座も被害！
      都銀や地銀から信用金庫や信用組合等
      地域の金融機関へも被害が拡大



【1位】インターネットバンキングやクレジットカード情報の不正利用

～拡大する攻撃対象、様々な手段で金銭取引の重要な情報を収集～

- **対策一覧**
  - **利用者**
    - OS・ソフトウェアの更新
    - ウイルス対策ソフトの導入
    - 事例や手口を知る
    - 二要素認証等の強い認証方式の利用
  - **銀行/カード運営会社**
    - 利用者への事例や手口の情報提供
    - 二要素認証等の強い認証方式の提供



銀行が提供する二要素認証や
専用のウイルス対策ソフトがあれば活用！

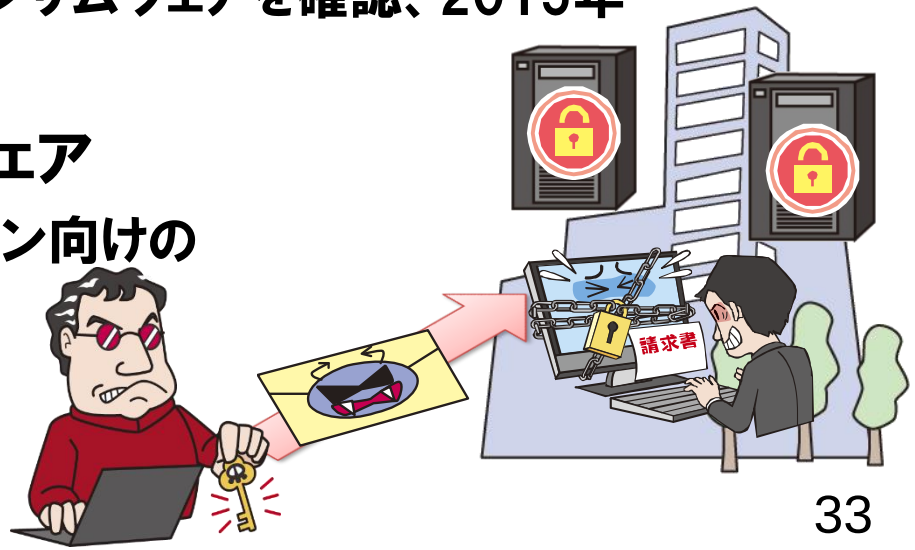
【2位】ランサムウェアを使った詐欺・恐喝

～日本人を標的にしたランサムウェアが日本上陸～

- ランサムウェアにより、PC内のファイルが暗号化され、ファイル復元に身代金を要求
- 日本語対応やスマートフォンを標的とする等、巧妙化

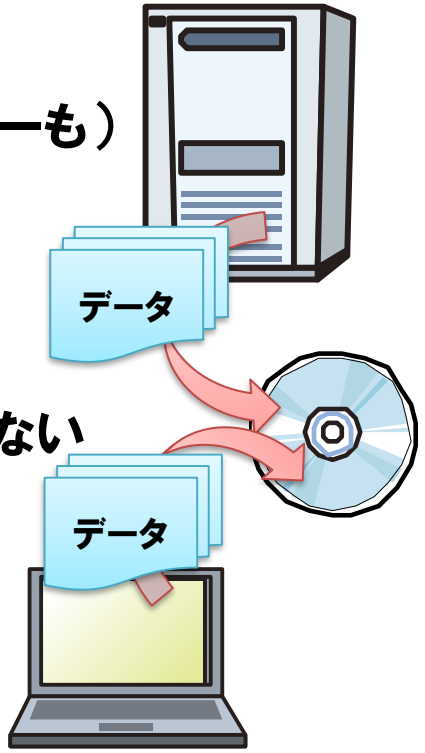
【2位】ランサムウェアを使った詐欺・恐喝
～日本人を標的にしたランサムウェアが日本上陸～

- 手口/影響
  - メールの添付ファイルやリンクからランサムウェア感染
  - ウェブからランサムウェアに感染(脆弱性等を悪用)
  - 感染すると感染したPCだけではなく、共有サーバー等にも影響
- 2015年の事例/傾向
  - ランサムウェアの日本語化・被害拡大
    - 2014年末に日本語対応のランサムウェアを確認、2015年から問い合わせ急増
  - スマートフォン向けランサムウェア
    - 端末のロックを行うスマートフォン向けのランサムウェアが登場



【2位】ランサムウェアを使った詐欺・恐喝
～日本人を標的にしたランサムウェアが日本上陸～

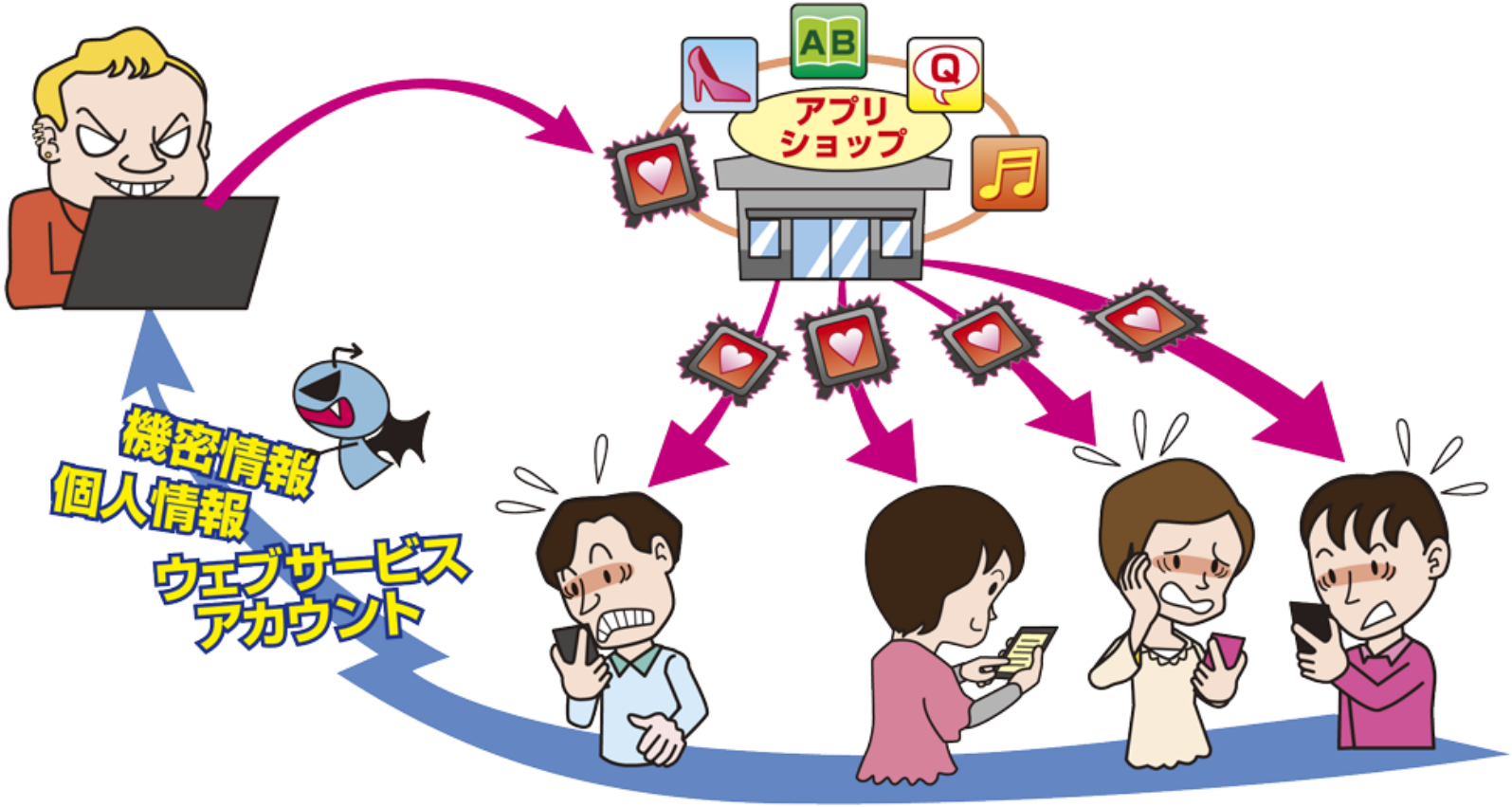
- 対策一覧
  - PC利用者
    - 定期的なバックアップ（PCだけではなく、共有サーバーも）
      また、復元できるかの事前の確認
    - OS・ソフトウェアの更新
    - ウイルス対策ソフトの導入・更新
    - メールの添付ファイル・リンクのURLを不用意に開かない
  - スマートフォン利用者
    - ウイルス対策ソフトの導入・更新



定期的なバックアップ、
併せて脆弱性対策もすることで安全に

【3位】審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ

～蔓延する悪意あるスマートフォンアプリ、公式マーケットのアプリにも注意を～



- スマホ内の電話帳等の情報が第三者に送信される
- 公式マーケット内にあるアプリにも悪意あるアプリが存在

【3位】審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ

～蔓延する悪意あるスマートフォンアプリ、公式マーケットのアプリにも注意を～

- 手口/影響
  - 悪意あるアプリを公式マーケット等に公開して誘導
  - アップデートで悪意のあるアプリに豹変
  - 別のアプリを勝手にインストール
  - 端末内の情報窃取や盗聴・盗撮

- 2015年の事例/傾向
  - AndroidやAppleの公式マーケットに悪意あるアプリ
    - 信頼できると思われていた公式マーケットに悪意あるアプリ、特にAppleについてはアプリの審査があり安全と思われていたが信頼が揺らいだ

対策一覧

スマートフォン利用者

- 信頼できるアプリかどうかを確認
- アクセス権限の確認
- OSやアプリは最新版を利用
- ウイルス対策ソフトの導入

アプリのインストールは慎重に！
公式マーケットからでも注意を

【4位】巧妙・悪質化するワンクリック請求

～被害者を欺く手口はますます悪質に～

- 有料サイトの利用料等、金銭を不正に請求するワンクリック請求の被害
- シャッター音が鳴る等、不安を煽る巧妙な手口の登場

【4位】巧妙・悪質化するワンクリック請求
～被害者を欺く手口はますます悪質に～

- 手口/影響
  - メールのリンク等から悪意あるサイトに誘導し、請求画面を表示させる
  - 騙して悪意あるソフトウェアやスマホアプリをインストールさせ、金銭を要求する
- 2015年の事例/傾向
  - アダルトサイトの解約料で1,813万円の不正請求
    - スマートフォンでアダルトサイト閲覧中に請求画面を表示
    - 請求画面に従い電話連絡し、金銭を要求された
  - 世間の動向に便乗した詐欺
    - マイナンバー制度に便乗したメールも

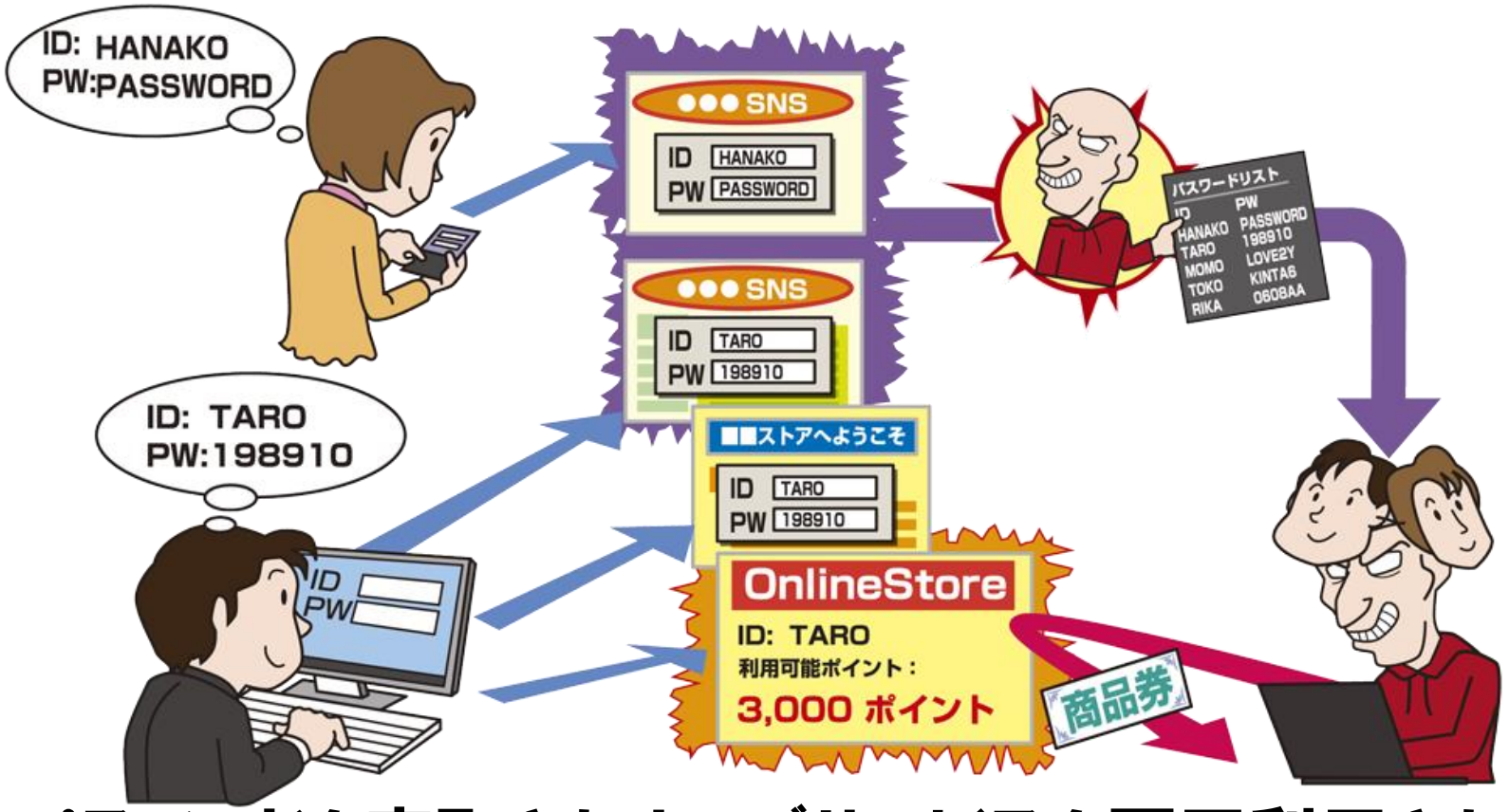
【4位】巧妙・悪質化するワンクリック請求
～被害者を欺く手口はますます悪質に～

- 対策一覧
  - ウェブサービスの利用者
    - 怪しいソフトウェアは利用しない
    - 怪しいサイト・メールは開かない
    - 事例・手口の情報収集

※購入の意思がないのであれば
金銭を要求されても、慌てず請求に応じない

怪しいソフトウェアの利用や怪しいサイトへの
アクセスは控え、万が一要求されても冷静に

【5位】ウェブサービスへの不正ログイン
～パスワードの適切な設定、管理を～

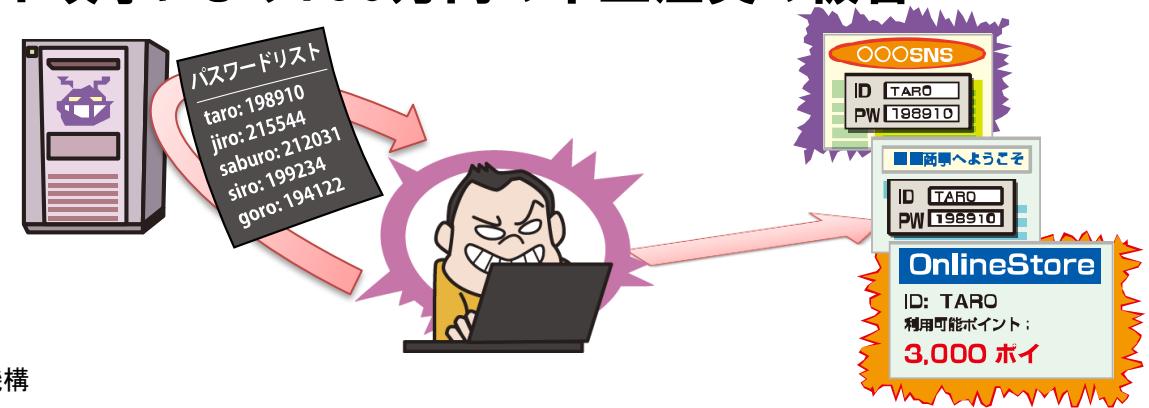


- パスワードを窃取されウェブサービスを不正利用される
- 複数サービスでパスワードを使い回すユーザーが被害に

【5位】ウェブサービスへの不正ログイン
～パスワードの適切な設定、管理を～

- 手口/影響
  - パスワードの推測
  - パスワードリスト攻撃（別サービスから窃取したIDやパスワード）
  - サービスに不正ログインされ、
    個人情報の窃取やポイントを不正利用される

- 2015年の事例/傾向
  - オンラインショッピングへの不正ログイン
    - パスワードリスト攻撃により160万円の不正注文の被害



【5位】ウェブサービスへの不正ログイン
～パスワードの適切な設定、管理を～

- 対策一覧
  - ウェブサービス利用者
    - 推測されにくく、長いパスワードを設定する
    - パスワードを使い回さない
    - 二要素認証等の強い認証方式の利用
    - ログイン履歴の確認
  - ウェブサービス提供ベンダー
    - 安全なウェブサービスの提供
    - 複雑なパスワード設定を要求（少ない文字数や記号無しの拒否等）
    - 二要素認証等の強い認証方式の提供
    - セキュリティ対策の徹底

**パスワードは推測されにくいものを設定し、
複数のサービスで使い回さない**

10大脅威2016(個人)と情報セキュリティ対策の基本との対応

順位	脅　威	ソフトウェアの更新	ウイルス対策ソフト	パスワードの強化	設定の見直し	手口を知る
1位	インターネットバンキングやクレジットカード情報の不正利用	○	○	○		○
2位	ランサムウェアを使った詐欺・恐喝	○	○			○
3位	審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ		○			○
4位	巧妙・悪質化するワンクリック請求					○
5位	ウェブサービスへの不正ログイン	○	○	○		○

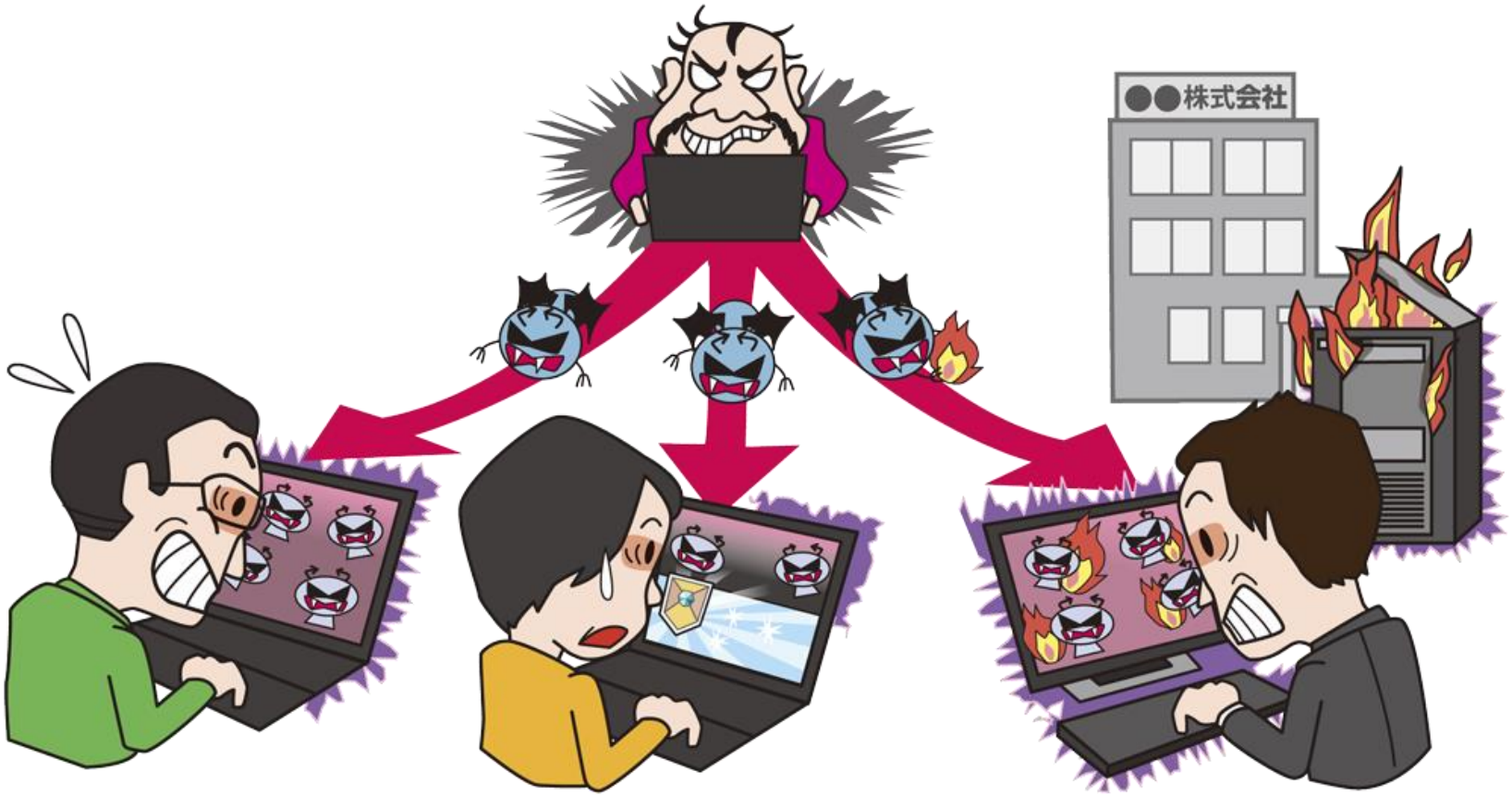
凡例：○ 対策効果あり、または部分的に効果あり

目次

- 情報セキュリティ10大脅威について
- 1章. 10大脅威の10年史
- 2章. 情報セキュリティ10大脅威 2016
- **3章. 注目すべき脅威や懸念**
  1. サポートの終了したソフトウェアを継続使用する危険性
  2. 証明書の導入・設定不備や検証不備に起因する脅威と対策
  3. マイナンバーの管理・運用の重要性

1．サポートの終了したソフトウェアを継続使用する危険性

～サーバーOSやブラウザも最新版の利用へ移行を～



- **サポートが終了したソフトウェアを継続利用することで様々な被害を受ける可能性がある**

脆弱性を悪用されてウイルス感染、不正アクセス、踏み台、等

1．サポートの終了したソフトウェアを継続使用する危険性
～サーバーOSやブラウザも最新版の利用へ移行を～

- 相次ぐ主要OS・ソフトウェアのサポート終了
  - Windows Server 2003
    - 2015年7月15日（日本時間）サポート終了
  - Internet Explorer
    - 2016年1月13日（日本時間）サポートポリシー変更
    - 各Windows OSで利用可能な最新版のみサポート

- 移行できない利用者
  - 未だに使われる2014年サポート終了のWindows XP
    - インターネットアクセスしているOSの内、10.93％がWindows XP
  - Windows Server 2003を継続利用
    - サーバー運用管理者の約半数がサポート終了後にWindows Server 2003を利用し続けると回答

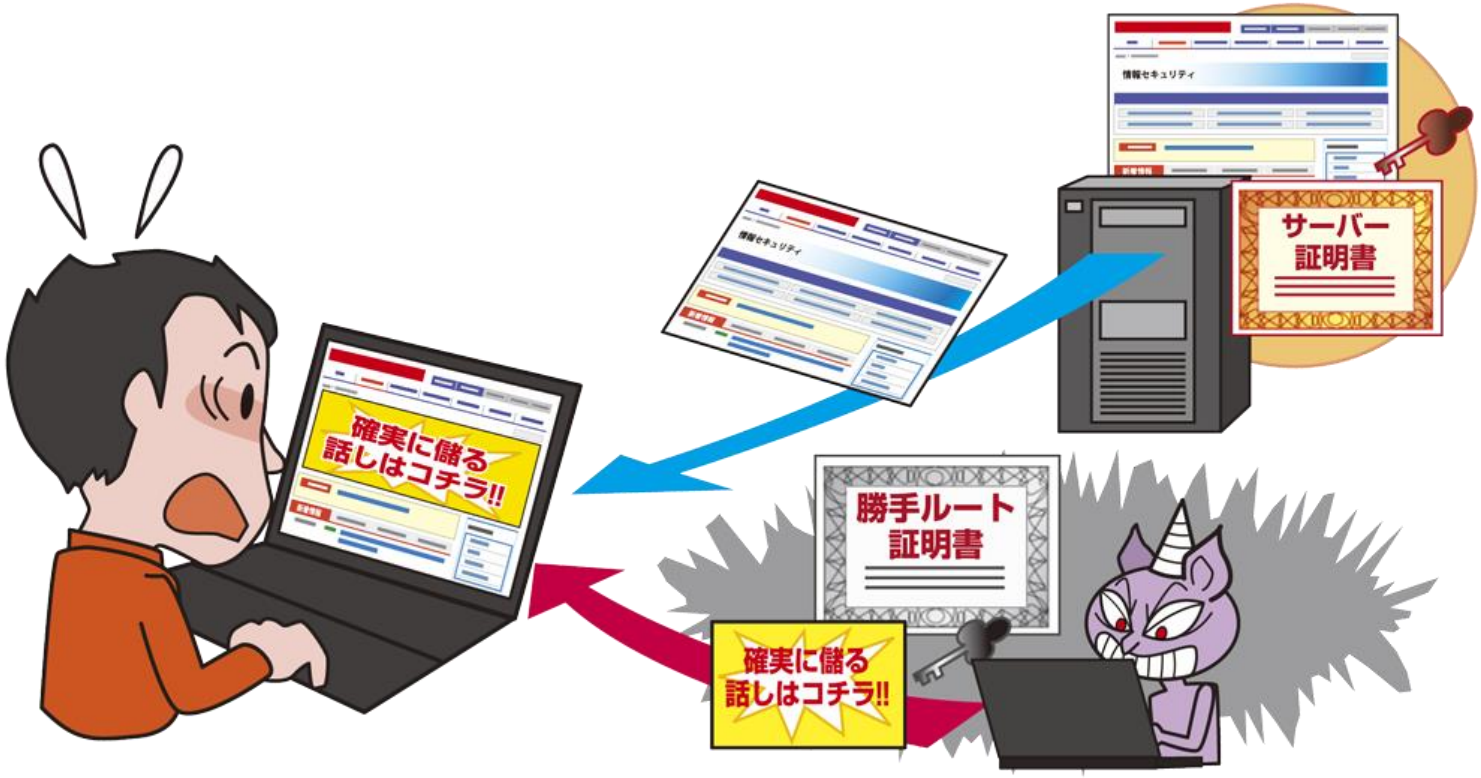
1．サポートの終了したソフトウェアを継続使用する危険性
～サーバーOSやブラウザも最新版の利用へ移行を～

- 最新版への移行を
  - 移行できない場合はリスク緩和策
    - ネットワークに繋がっていない環境で利用する、等
    - ただし、脆弱性が解消される訳ではないため、早急な移行を
  - 組織においては計画的な移行を
    - 互換性の問題により移行できないケースを想定し、以下を考慮
      （１）特定の製品やバージョンに依存しない
      （２）ソフトウェア製品のライフサイクル

- 今後のサポート終了予定
  - SQL Server 2005 : 2016年4月12日
  - Windows Vista : 2017年4月11日
  - Office 2007 : 2017年10月10日
  - Windows 7 : 2020年1月14日
  - Windows Server 2008 R2 : 2020年1月15日

2. 証明書の導入・設定不備や検証不備に起因する脅威と対策

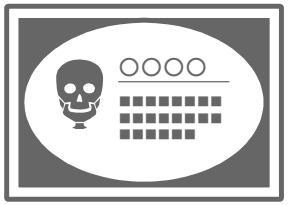
～ルート証明書の強制インストールに御用心～



- 公開鍵証明書の仕組みを悪用して広告を表示する機能に脆弱性が存在
- 第三者に悪用されると通信内容の解読や悪意あるソフトウェアをインストールされる、等の可能性

2. 証明書の導入・設定不備や検証不備に起因する脅威と対策
～ルート証明書の強制インストールに御用心～

- **勝手ルート証明書問題（Superfish）**
  - **大手PC開発ベンダーのPCに不正広告の機能が存在**
    - 認証局発行ではない自己署名証明書を、OS内にルート証明書としてインストール
    - PCで共通の秘密鍵を利用
    - 上記を利用し、TLSで保護されたサイトに無理矢理広告を挿入
  - **影響**
    - 盗聴・改ざん防止されたコンテンツをかきかえる機能自体が不正行為
    - 共通の秘密鍵なため、第三者が悪用すると通信内容の解読、悪意のあるソフトウェアの強制インストール等が可能となる危険性
- **勝手ルート証明書問題、再び（Superfish2.0）**
  - **別の大手PC開発ベンダーでも**
    - 遠隔サポートサービス提供用の機能に同様の問題
    - 秘密鍵は暗号化されていたが、誰でも推測可能であった



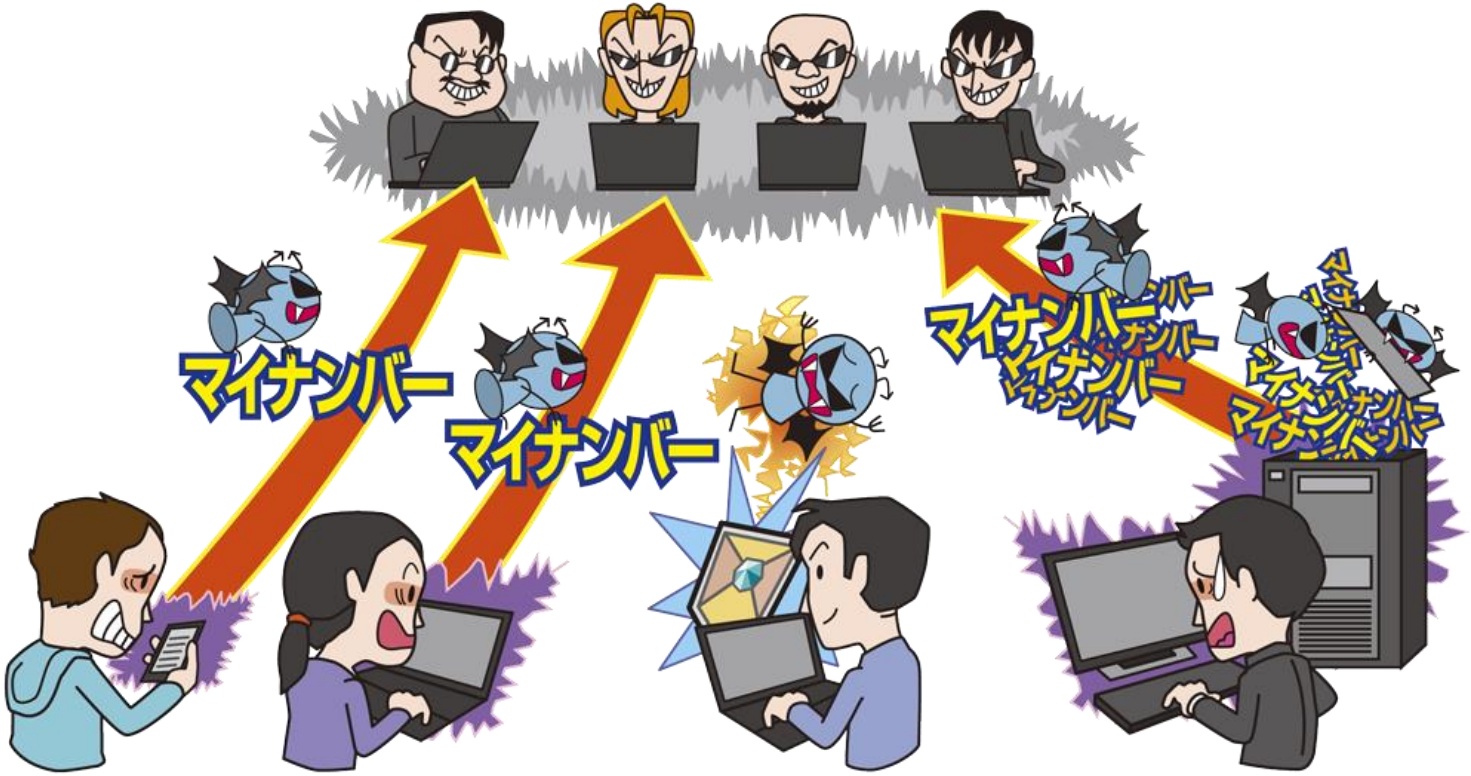
2. 証明書の導入・設定不備や検証不備に起因する脅威と対策
～ルート証明書の強制インストールに御用心～

- 事業者が注意すべきこと
  - 認証局発行でない自己署名証明書をルート証明書にインストールするソフトウェアを開発・配布しない
  - 秘密鍵を他者に配布することで動作するソフトウェアを開発・配布しない
  - 証明書に関する問題が発見された場合、速やかに脆弱性情報を公開すると共に、更新プログラム等の解決策を提供

- 利用者として注意すべきこと
  - 最新情報の収集に努め、更新プログラム等が提供された場合、早急に適用する
  - 不審なソフトウェアはインストールしない

3. マイナンバーの管理・運用の重要性

～他者のマイナンバーを預かる事業者等は厳重な管理を～



- 人為的誤りやIT（情報技術）上の誤りを原因とするマイナンバーの漏えい（未遂を含む）が一部で発生
- 自身のマイナンバーを適切に管理し、他者のマイナンバーを預かる関係者は厳重な管理・運用が必要

3. マイナンバーの管理・運用の重要性
～他者のマイナンバーを預かる事業者等は厳重な管理を～

- マイナンバーの漏えい
  - 人為的・物理的/IT(情報技術)上の誤りによる漏えい
    - マイナンバー通知カードの誤配達、マイナンバーが印刷された公文書の誤交付・誤送付等
    - 自動交付機の設定不備により、記載不要の住民票にマイナンバーを印刷・交付等

- 漏えいが発生すると
  - 米国では(社会保障番号)
    - 漏えいした番号による「なりすまし」事件が大きな問題
    - 銀行口座開設、クレジットカードの作成と利用、住所変更等が可能
    - 合衆国政府のデータベースから2,150万人分の漏えい事件も
  - 日本ではマイナンバーは漏えいしても安全
    - 原則、顔写真付き身分証明書等を用いた本人確認実施
    - マイナンバー単独の漏えいではなりすましは発生しない

3. マイナンバーの管理・運用の重要性

～他者のマイナンバーを預かる事業者等は厳重な管理を～

- 個人として注意すべきこと
  - 趣旨と提示範囲の理解
    - マイナンバーは、法令に定められた社会保障・税・災害対策の行政手続のためのみに提示、等制度の趣旨と開示範囲が決まっている
  - 保存・送信する場合
    - PC等に電子化して保存する場合は、情報自体を暗号化し、端末操作にパスワード入力や指紋認証等の本人確認を必須となるように設定
    - メール等のネットワーク経由で送信する場合、暗号化や改ざん防止を
- 事業者が注意すべきこと
  - 特定個人情報の取扱いに関するガイドラインを遵守
    - 法令に定められた利用制限、厳重な管理、提供・収集の制限を実施
  - 継続的なセキュリティ対策の見直し・実施
  - 業種別の個別のガイドラインへの遵守も
    - 金融業務にかかわる事業者や行政機関・地方公共団体等

本資料に関する詳細な内容は

- 以下のページのPDF資料をご覧ください。

情報セキュリティ10大脅威 2016
https://www.ipa.go.jp/security/vuln/10threats2016.html


IPA
Better Life
with IT