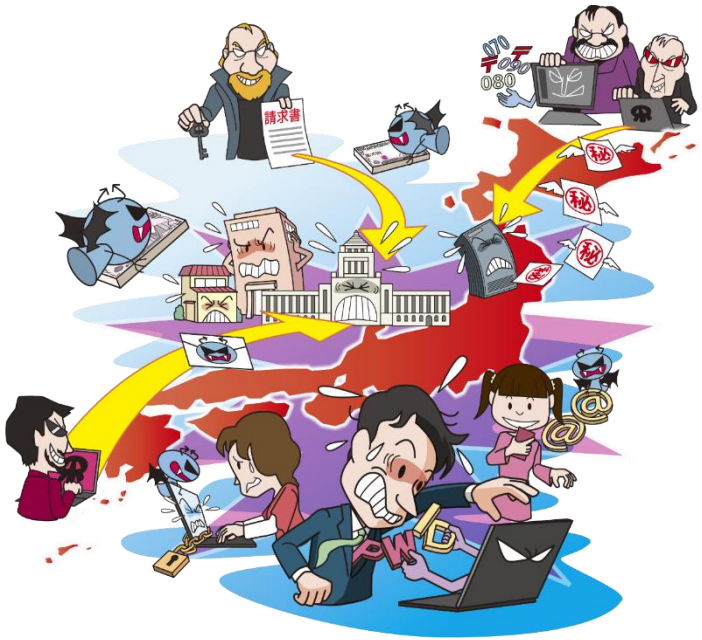
IPA Better Life with IT

「情報セキュリティ10大脅威 2016 ～ 組織編 ～」

～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

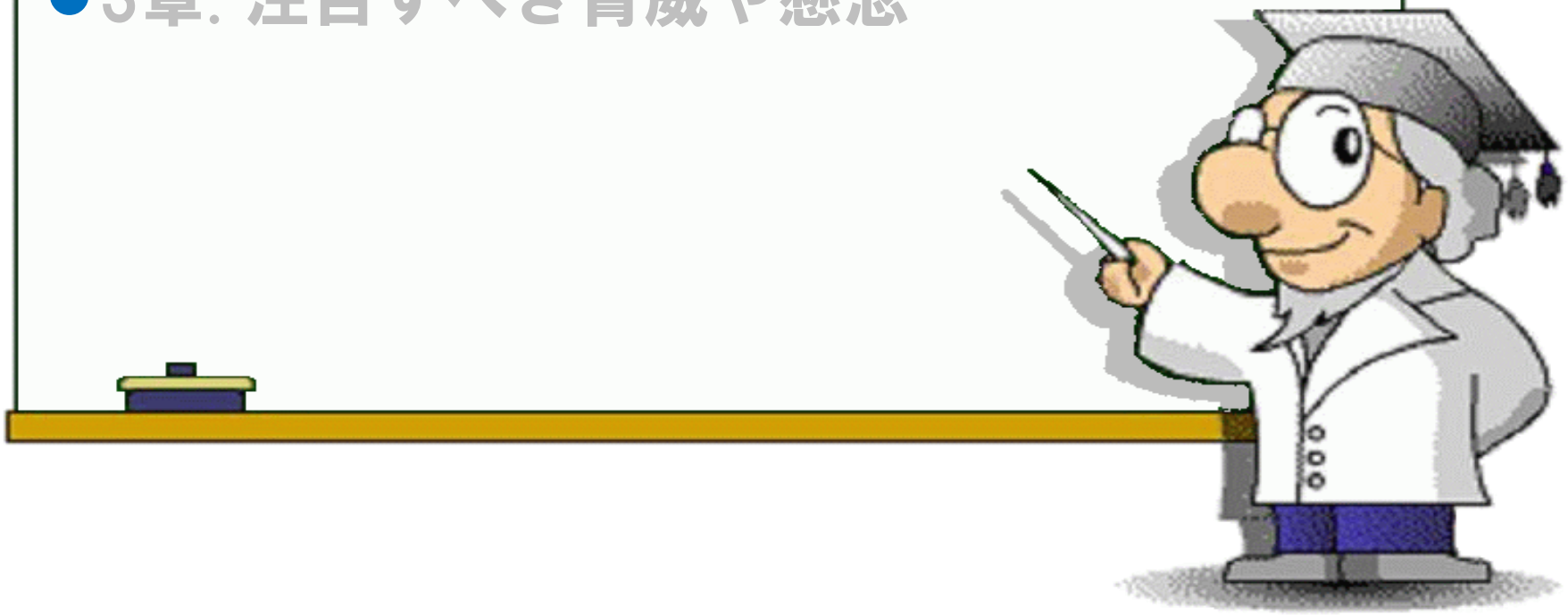
- 10大脅威とは？
  - 2006年よりIPAが毎年発行している資料
  - 「10大脅威選考会」約100名の投票により、情報システムを取巻く脅威を順位付けして解説

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

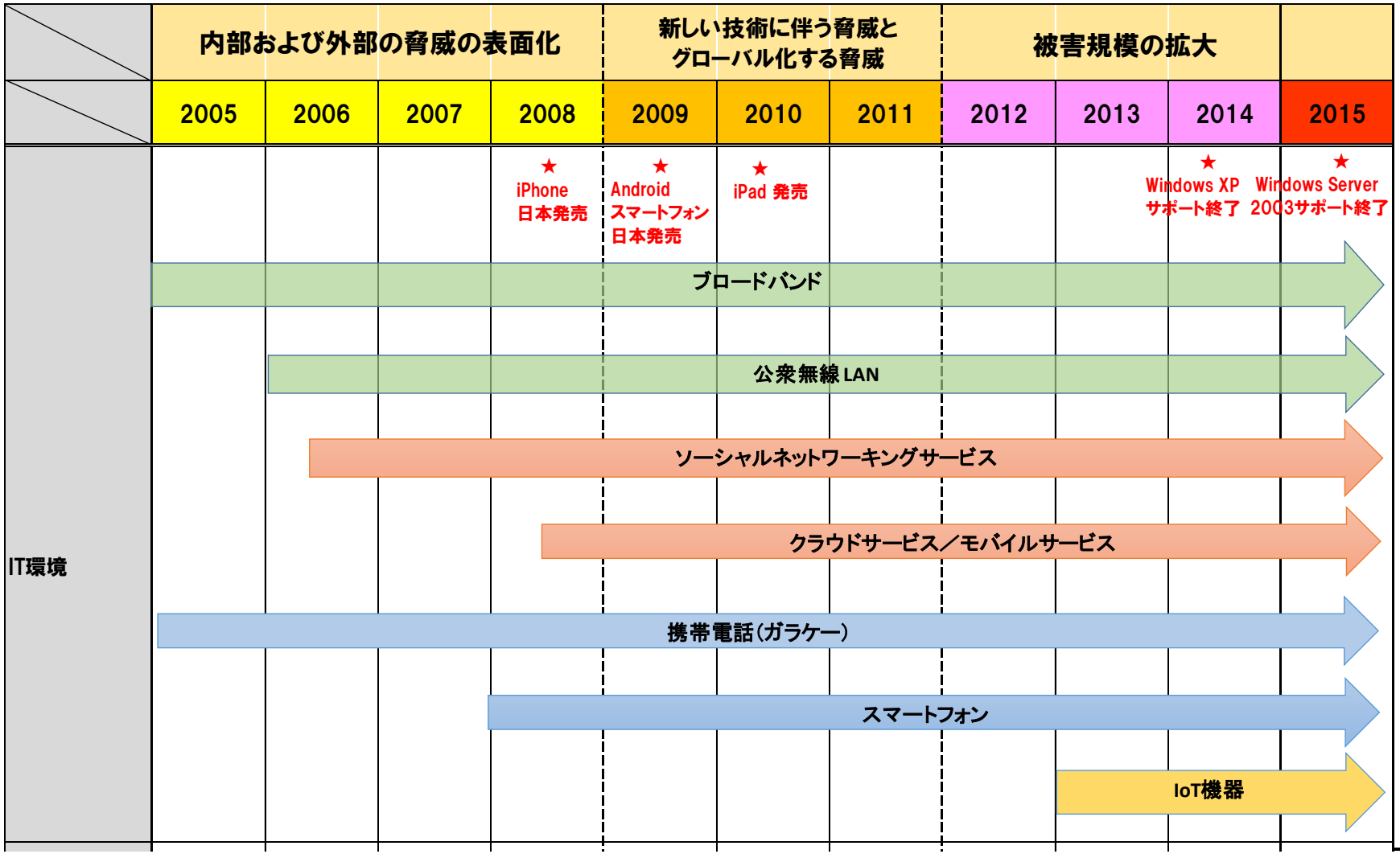
■2005年～2008年の4年間
（10大脅威2006～2009）

■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）

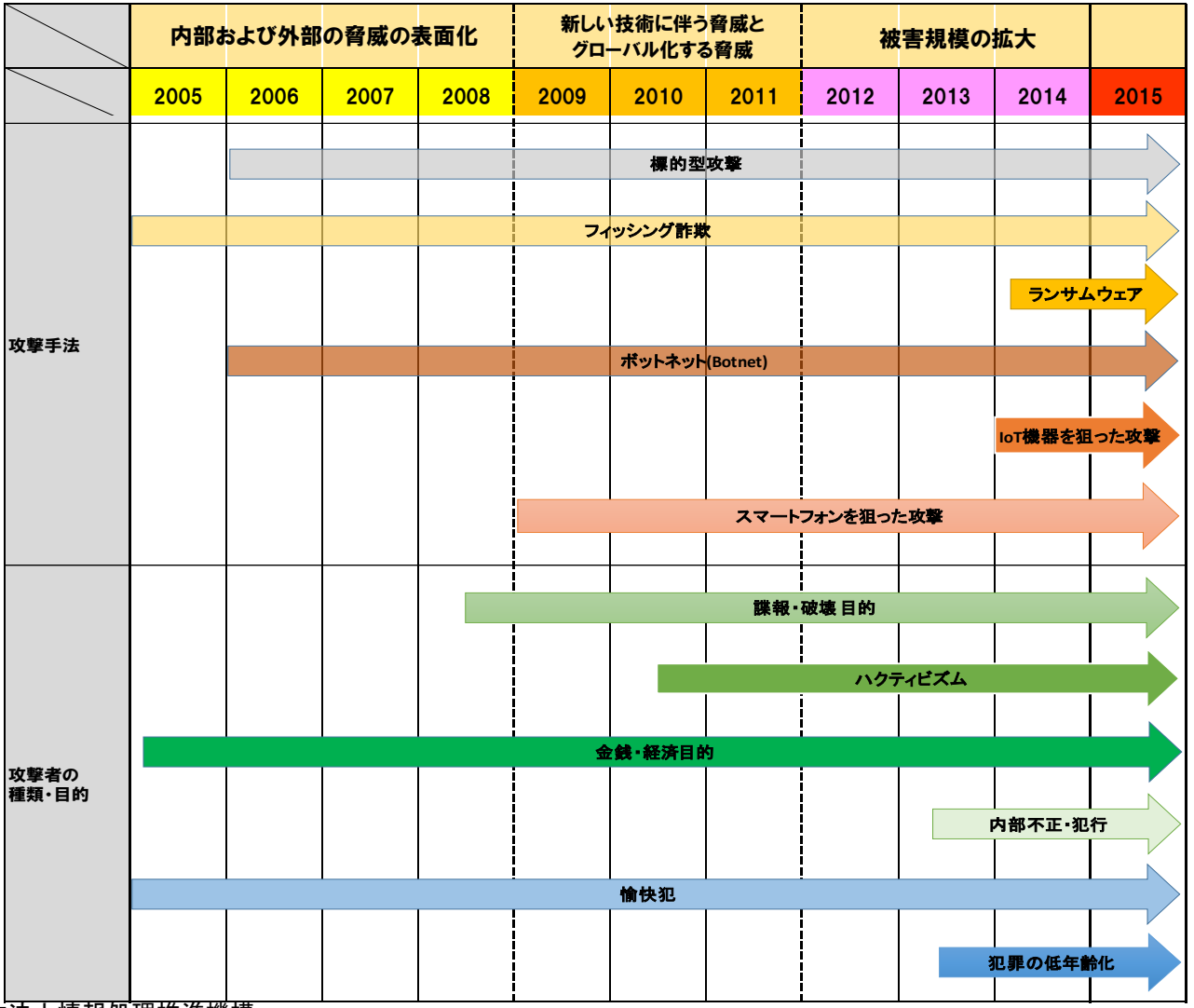
10大脅威の10年史

■ 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

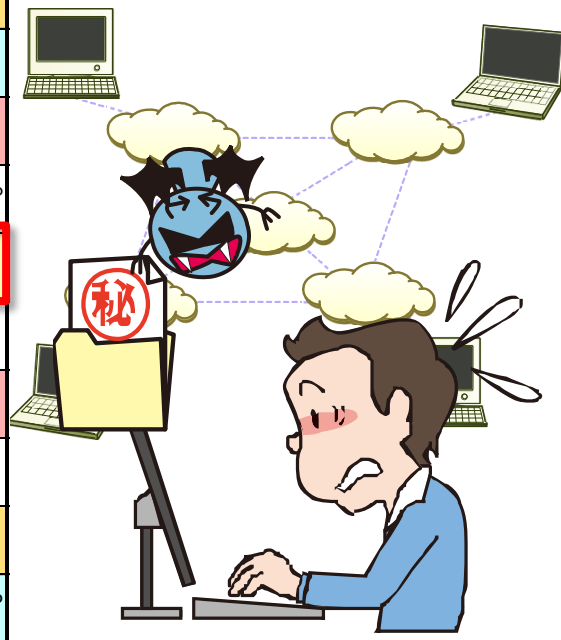
順位	2005年	2006年	2007年	2008年
1位	事件化するSQLインジェクション	漏えい情報のWinnyによる止らない流通	高まる「誘導型」攻撃の脅威	DNSキャッシュポイズニングの脅威
2位	Winnyを通じたウイルス感染による情報漏えいの多発	表面化しづらい標的型（スピア型）攻撃	ウェブサイトを狙った攻撃の広まり	正規ウェブサイトを経由した攻撃の猛威
3位	音楽CDに格納された「ルートキットに類似した機能」の事件化	悪質化・潜在化するボット	恒常化する情報漏えい	巧妙化する標的型攻撃
4位	悪質化するフィッシング詐欺	深刻化するゼロデイ攻撃	巧妙化する標的型攻撃	検知されにくいボット、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

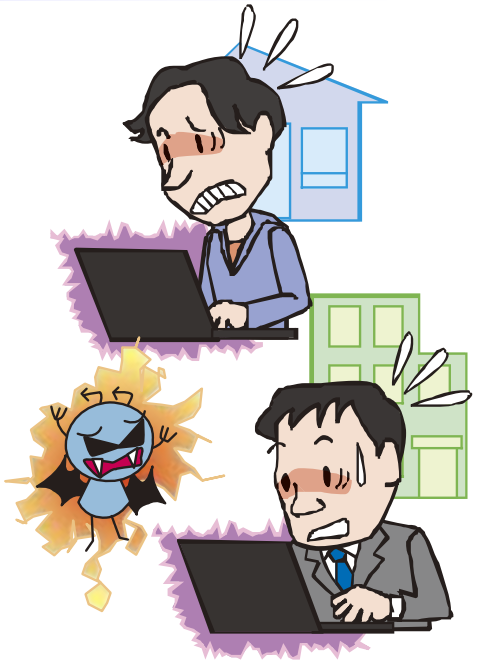
- **狙われる組織の情報、標的型攻撃の登場**
  - ・10年前から存在する標的型攻撃
  - ・2006年以降常に10大脅威に登場

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

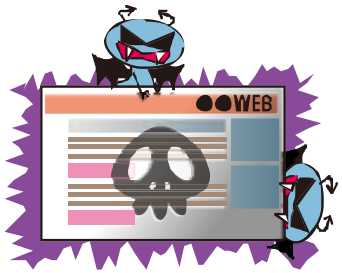
順位	2009年	2010年	2011年
1位	変化を続けるウェブサイト改ざんの手口	「人」が起こしてしまう情報漏えい	機密情報が盗まれる！？新しいタイプの攻撃
2位	アップデートしていないクライアントソフト	止らない！ウェブサイトを経由した攻撃	予測不能の災害発生！引き起こされた業務停止
3位	悪質なウイルスやボットの多目的化	定番ソフトウェアの脆弱性を狙った攻撃	特定できぬ、共通思想集団による攻撃
4位	対策をしていないサーバ製品の脆弱性	狙われだしたスマートフォン	今もどこかで･･･更新忘れのクライアントソフトを狙った攻撃
5位	あわせて事後対応を！情報漏えい事件	複数の攻撃を組み合わせ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

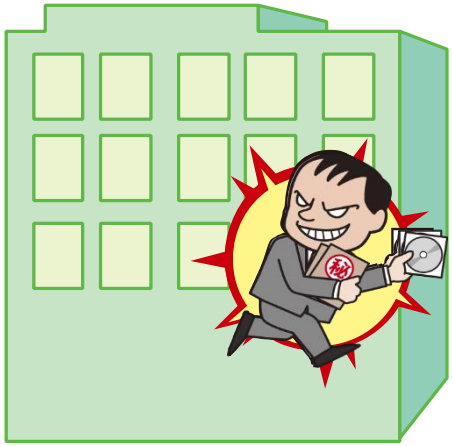
- **金銭被害拡大、狙われるインターネットバンキング・クレジットカード**
  - **インターネットバンキングやクレジットカード情報の不正利用**
  - **総被害額は、2012年が約4,800万円、2013年が約14億600万円、2014年が約29億1,000万円**

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

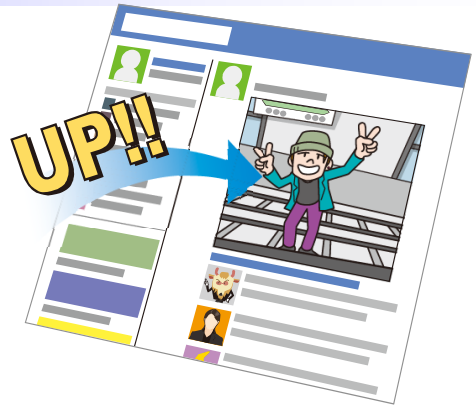
- 内部犯行により個人情報が漏えい
- 権限がある従業員がその権限を使って個人情報を窃取
- 顧客への補償として200億円を用意したケースも

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

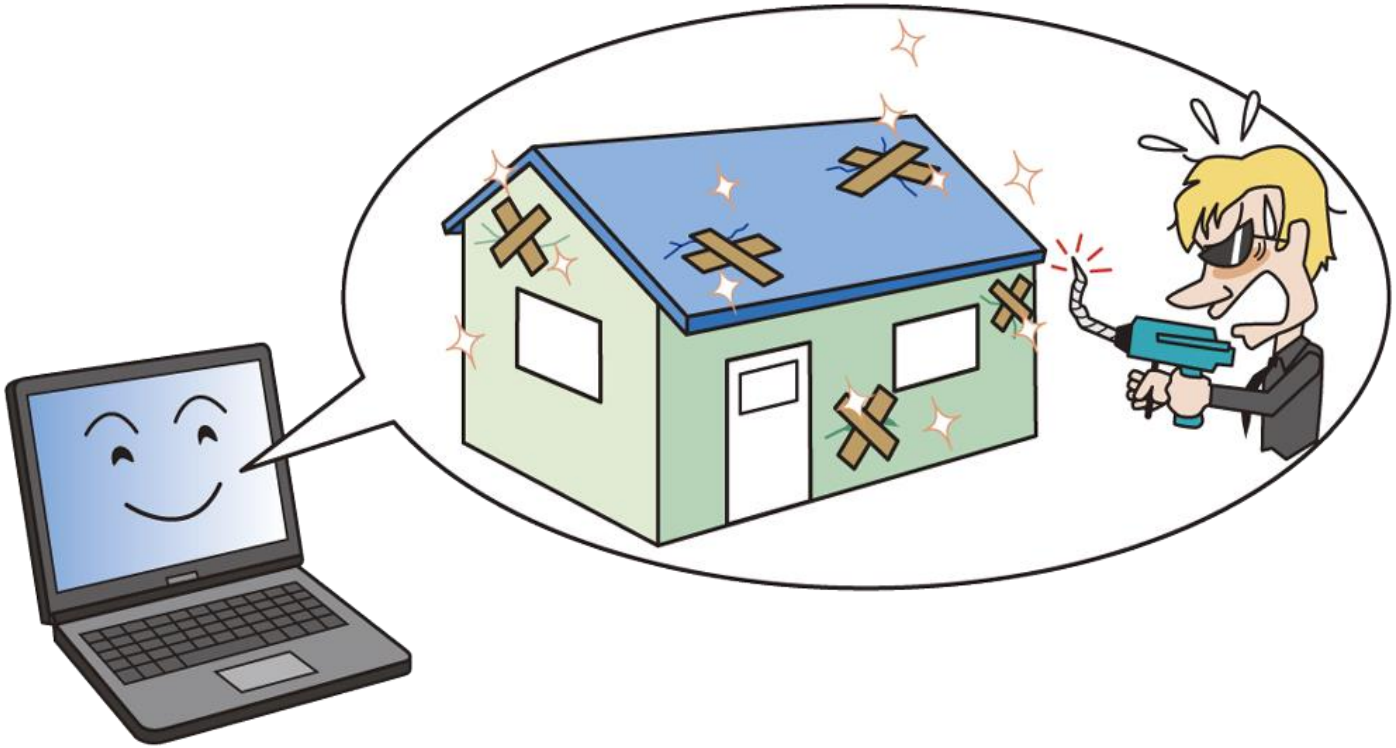
- 若者や従業員による軽率な行為や発言を配信し、炎上
- 被害を受けた企業には倒産等、甚大な被害を受けるケースも
- 当人も多額の賠償金や降格、停職等の処分がされている

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

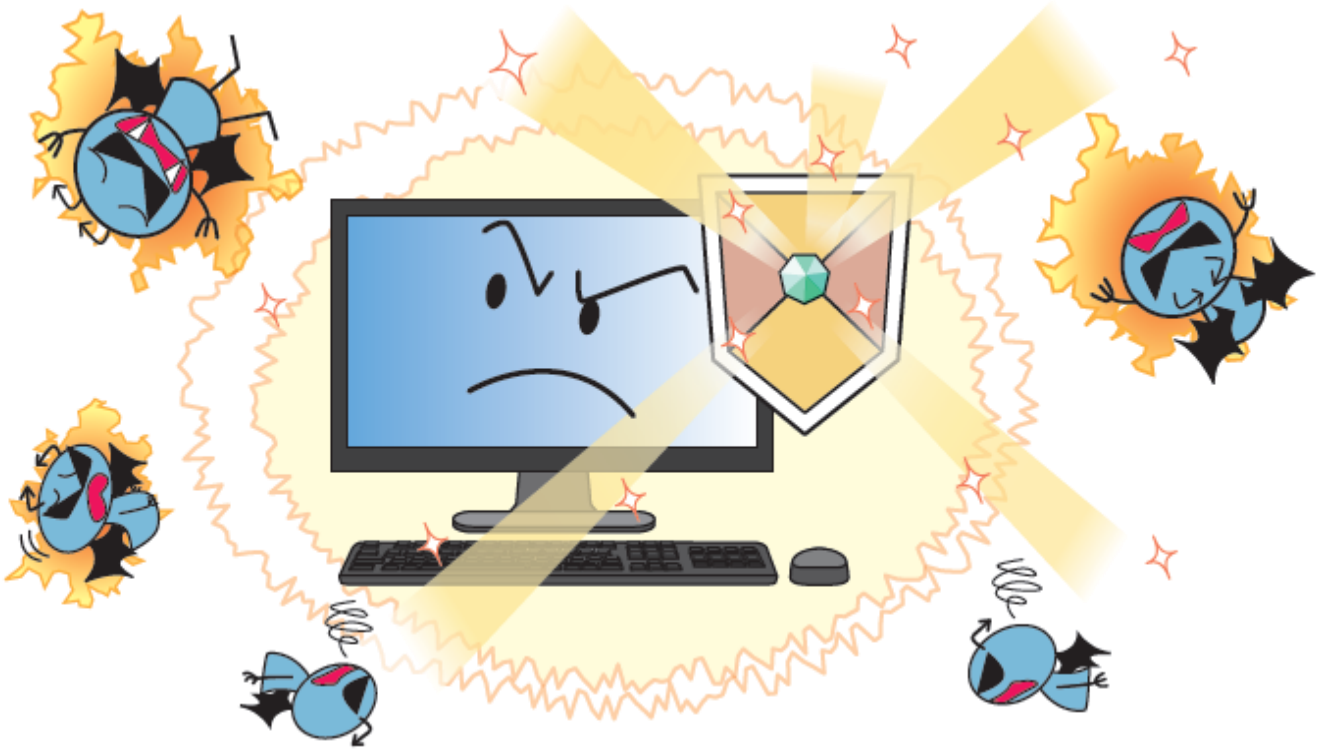
10大脅威の順位は毎年変動するが、
　上記の基本的な対策の必要性は長年変わらない
IT利用者には「**自発的な対策の実施**」が求められている

ソフトウェアの更新



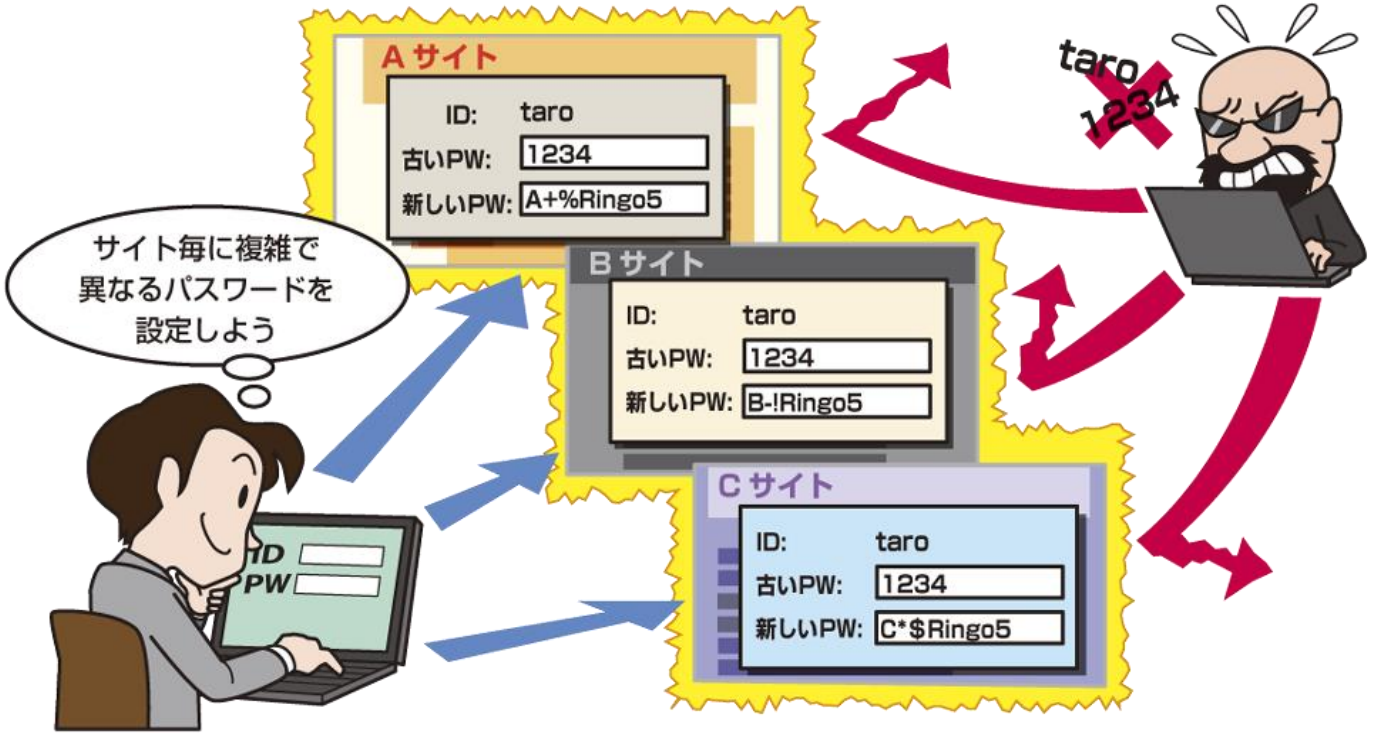
- ソフトウェアの欠陥である脆弱性は、
  ソフトウェアを更新して根本的に解消する

ウイルス対策ソフトの導入



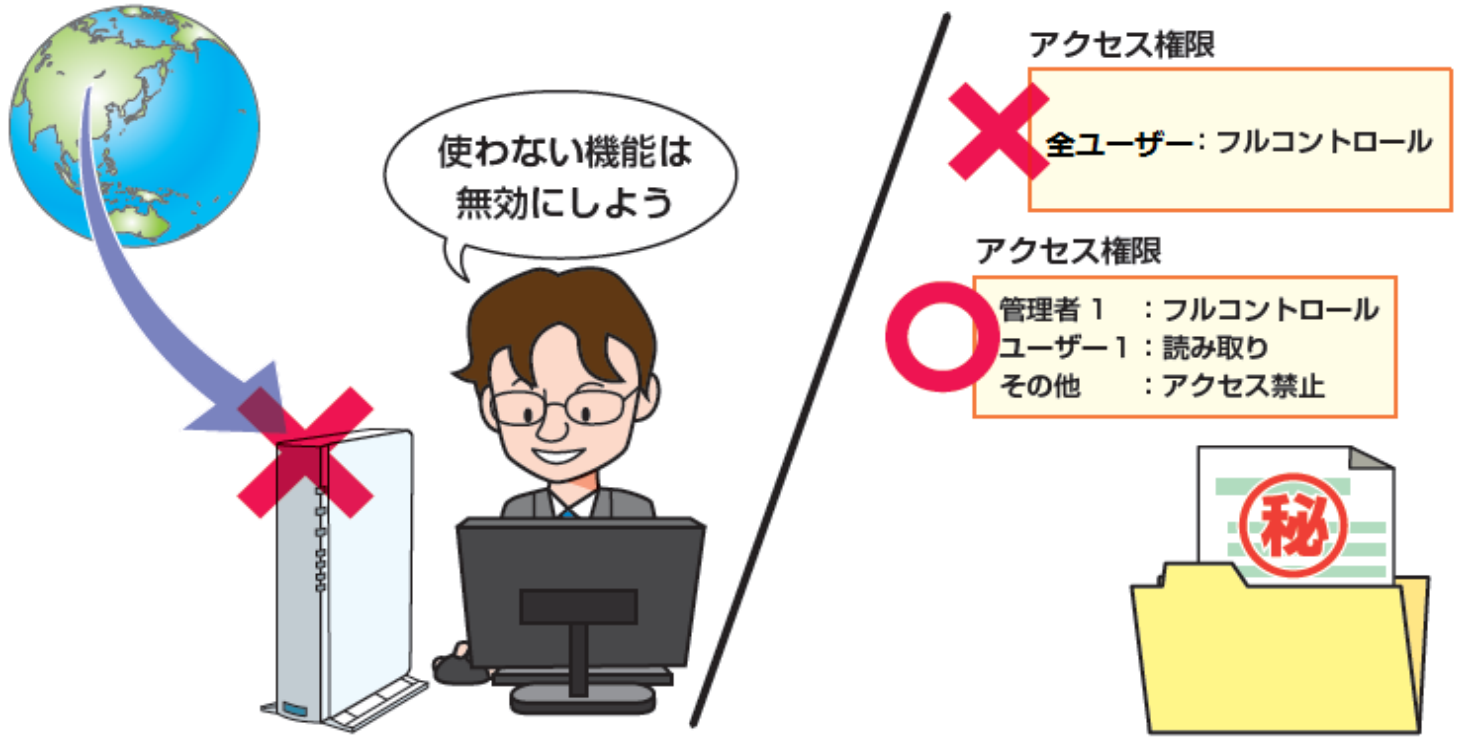
- ウイルス対策ソフトを導入し、
  流行しているウイルスの感染を未然に防ぐ

パスワードの適切な管理と認証の強化



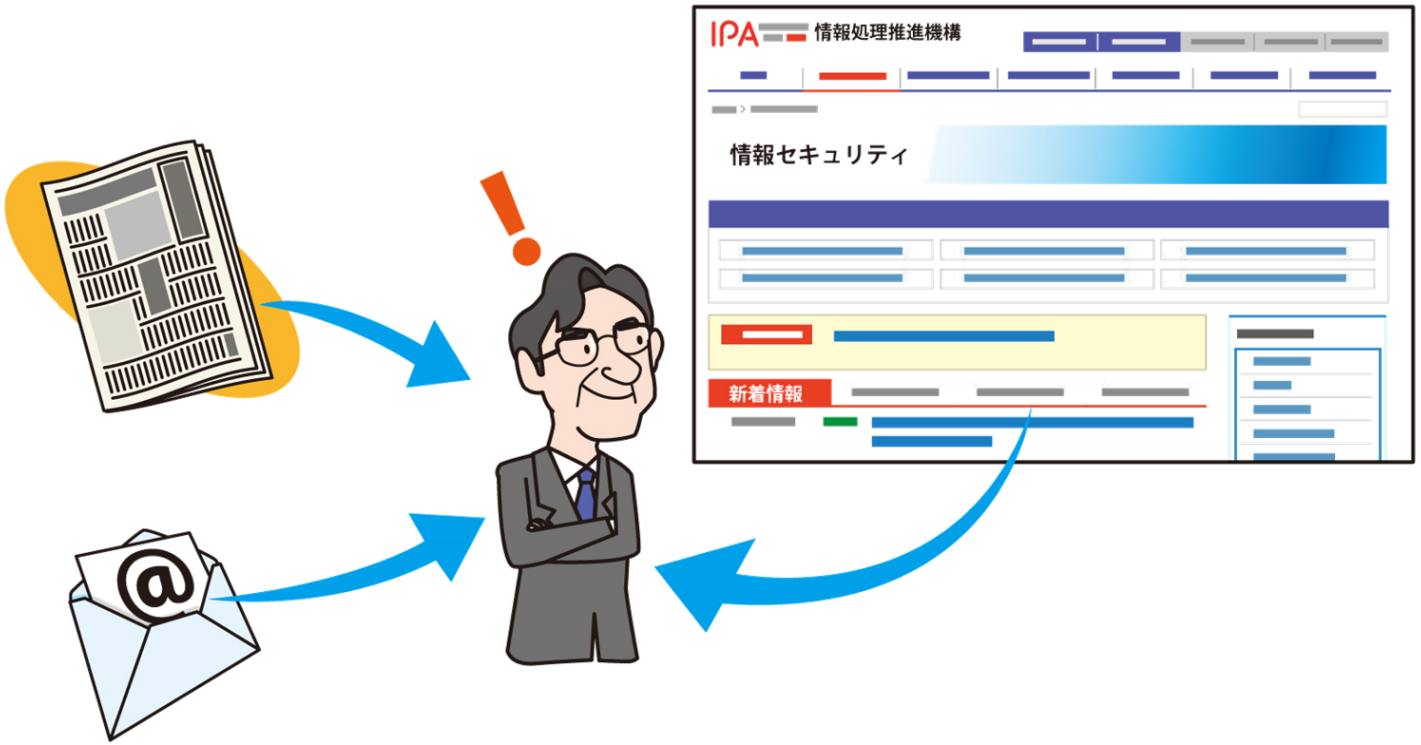
- 推測されにくい
  「記号・英数字」を含む「十分な文字数」のパスワードを設定
- 複数のウェブサービスでパスワードを使い回さない
- 二要素認証等、強い認証方式が利用できれば利用する

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

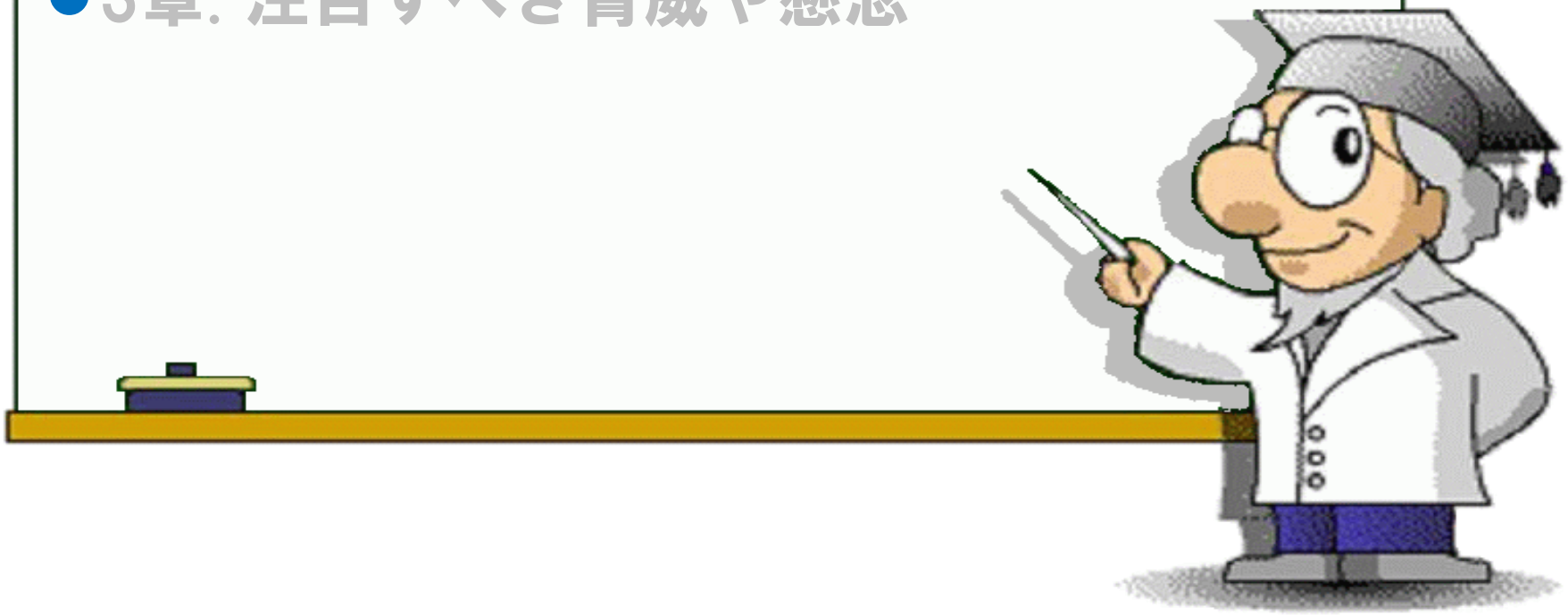
脅威や手口を知る



- 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

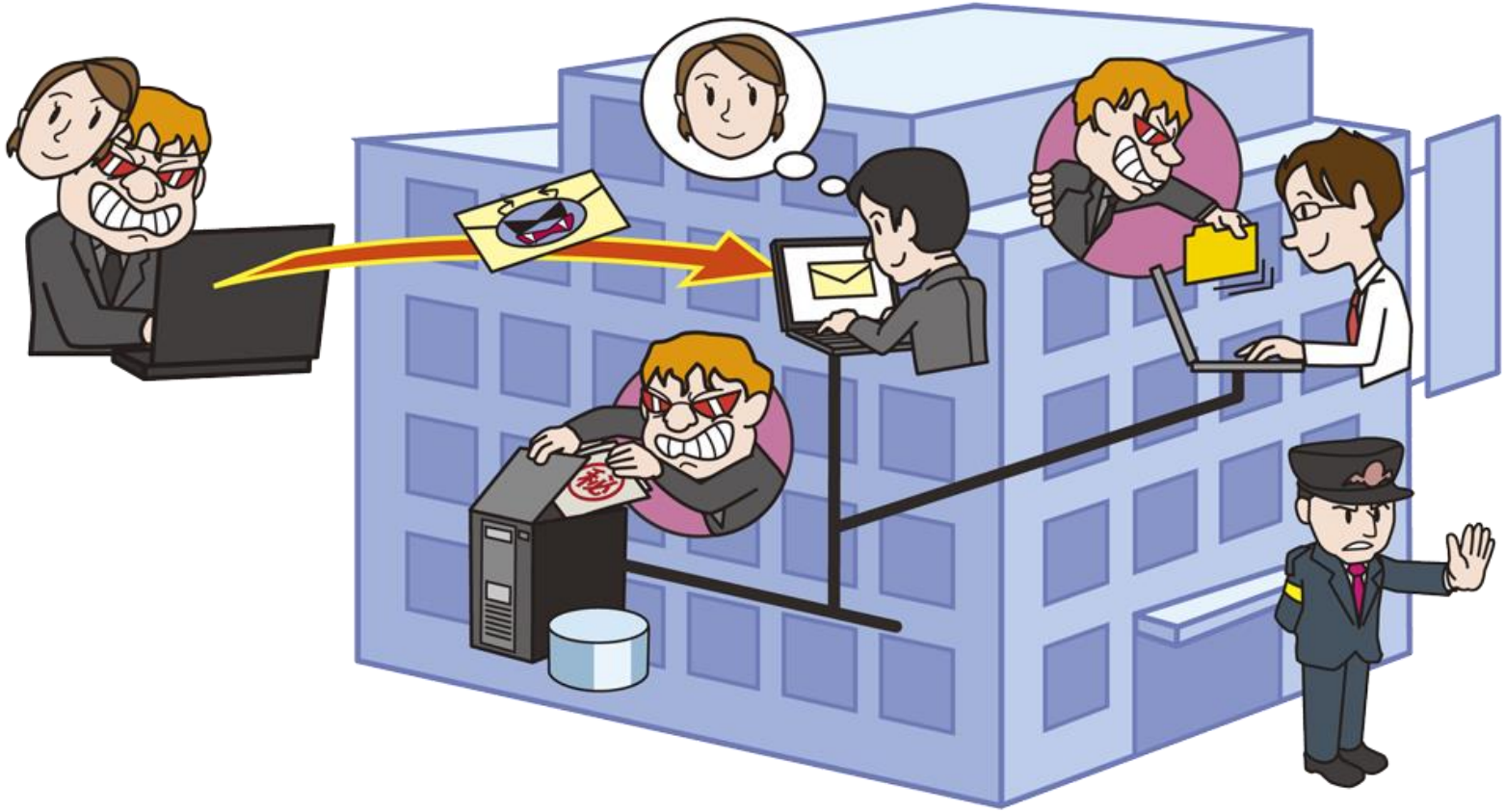


情報セキュリティ10大脅威 2016
（組織：5位まで抜粋）

順位	脅威
1位	標的型攻撃による情報流出
2位	内部不正による情報漏えいとそれに伴う業務停止
3位	ウェブサービスからの個人情報の窃取
4位	サービス妨害攻撃によるサービスの停止
5位	ウェブサイトの改ざん

【1位】標的型攻撃による情報流出

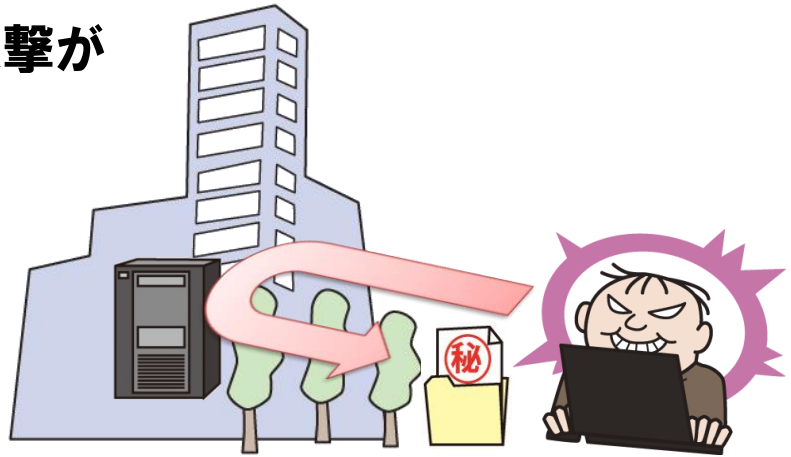
～多くの組織や企業が標的型攻撃のターゲットに！～



- ネット経由のスパイ活動により企業・組織の情報が流出
- 取引先や関連会社を踏み台にして本丸を狙うことも

【1位】標的型攻撃による情報流出
～多くの組織や企業が標的型攻撃のターゲットに！～

- 侵入手口
  - メールからウイルス感染「ばらまき型」「やり取り型」
  - ウェブからウイルス感染「水飲み場型」
  - 標的組織の関連会社が踏み台に
- 2015年の事例/傾向
  - 日本年金機構約125万件の個人情報の漏えい
    - 複数回の攻撃メール、非公開のメールアドレスにも届く
    - URLや添付ファイルを開くことで感染
    - その後、他の組織でも同様の攻撃が行なわれていることを確認



【1位】標的型攻撃による情報流出
～多くの組織や企業が標的型攻撃のターゲットに！～

IPA

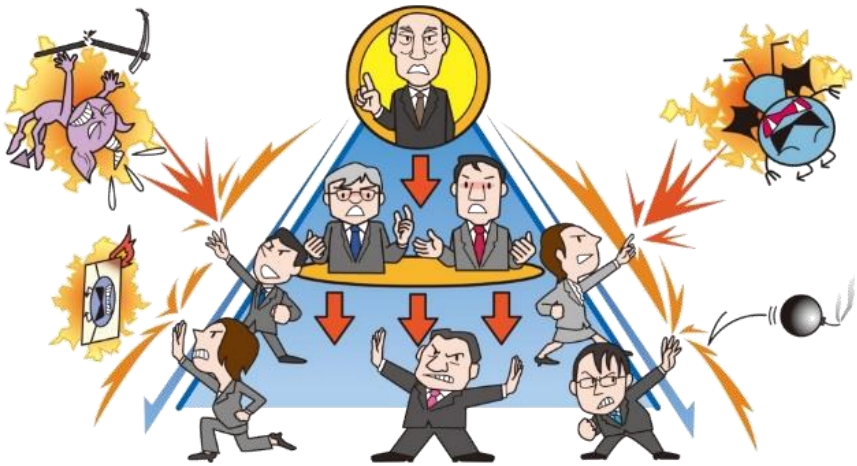
● 対策一覧

■ 経営者層
- 問題に迅速に対応できる体制の構築
- 対策予算の確保と継続的な対策実施

■ システム管理者
- 情報の取扱い・保管状態の確認
- システム設計対策・アクセス制限
- ネットワーク監視・分離

■ セキュリティ担当部署
- セキュリティ教育の実施
- 情報の保管方法ルール策定
- サイバー攻撃に関する情報共有

■ 従業員・職員
- セキュリティ教育の受講
- OS・ソフトウェアの更新
- ウイルス対策ソフトの導入・更新



内部へ侵入されることを想定した多層防御を

【2位】内部不正による情報漏えいと それに伴う業務停止

～内部不正が事業に多大な悪影響を及ぼす～

- 従業員・職員が故意に内部情報を持ち出し私的に利用
- 企業・組織の信用が失墜し、補償・賠償が求められる

【2位】内部不正による情報漏えいとそれに伴う業務停止

～内部不正が事業に多大な悪影響を及ぼす～

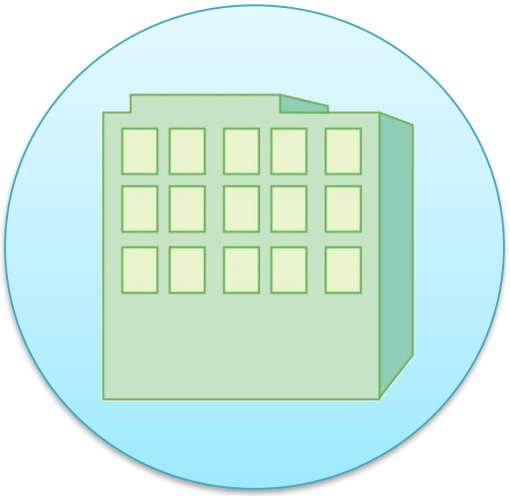
- **発生要因**
  - **職場環境や処遇の不満**
    処遇面（業務多忙、給与や賞与）の不満、
    復讐や個人的な利益の享受を目的とすることも
  - **アクセス権限の不適切な付与**
    必要以上なアクセス権の付与等
  - **システム操作記録と監視の未実施**
    不正に気づきにくく、不正の発覚が遅れる。

- **2015年の事例/傾向**
  - **公的機関から膨大な個人情報漏えい**
    - 元職員が持ち帰った約68万人の有権者情報が漏えい
    - レンタルサーバー上で外部から閲覧可能な状態に

【2位】内部不正による情報漏えいとそれに伴う業務停止

～内部不正が事業に多大な悪影響を及ぼす～

- 対策一覧
  - 組織
    - 情報取扱ポリシー作成および周知徹底・機密保護に関する誓約
    - 資産の把握・体制の整備
    - 情報の取扱教育の実施
    - 重要情報の管理・保護
    - アカウント、権限の管理・定期監査
    - システム操作の記録・監視
  - サービス利用者
    - 情報の管理が適切かを確認



組織一丸となって積極的に対策を推進する体制を

【3位】ウェブサービスからの個人情報の窃取

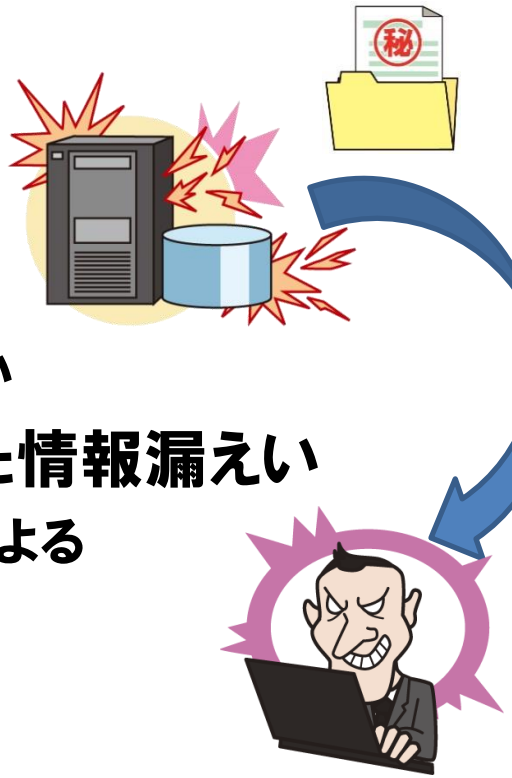
～ハッカー集団による甚大な被害～

- ウェブサービスから個人情報が窃取される事件が多発
- 主義主張を目的とする情報漏えいも

【3位】ウェブサービスからの個人情報の窃取
～ハッカー集団による甚大な被害～

- 手口/影響
  - ソフトウェアやウェブアプリケーションの脆弱性を悪用
  - リモート管理用のサービスからの侵入
  - 顧客情報の窃取やその情報の悪用

- 2015年の事例/傾向
  - アシュレイ・マディソンから情報漏えい
    - ハッカー集団により主義主張を目的に
      3,200万人の会員のアカウント情報が漏えい
  - SQLインジェクションの脆弱性を悪用した情報漏えい
    - 2014年に引き続き、SQLインジェクションによる
      情報漏えいが相次ぐ
    - Web会員情報約21万人分流出の被害も

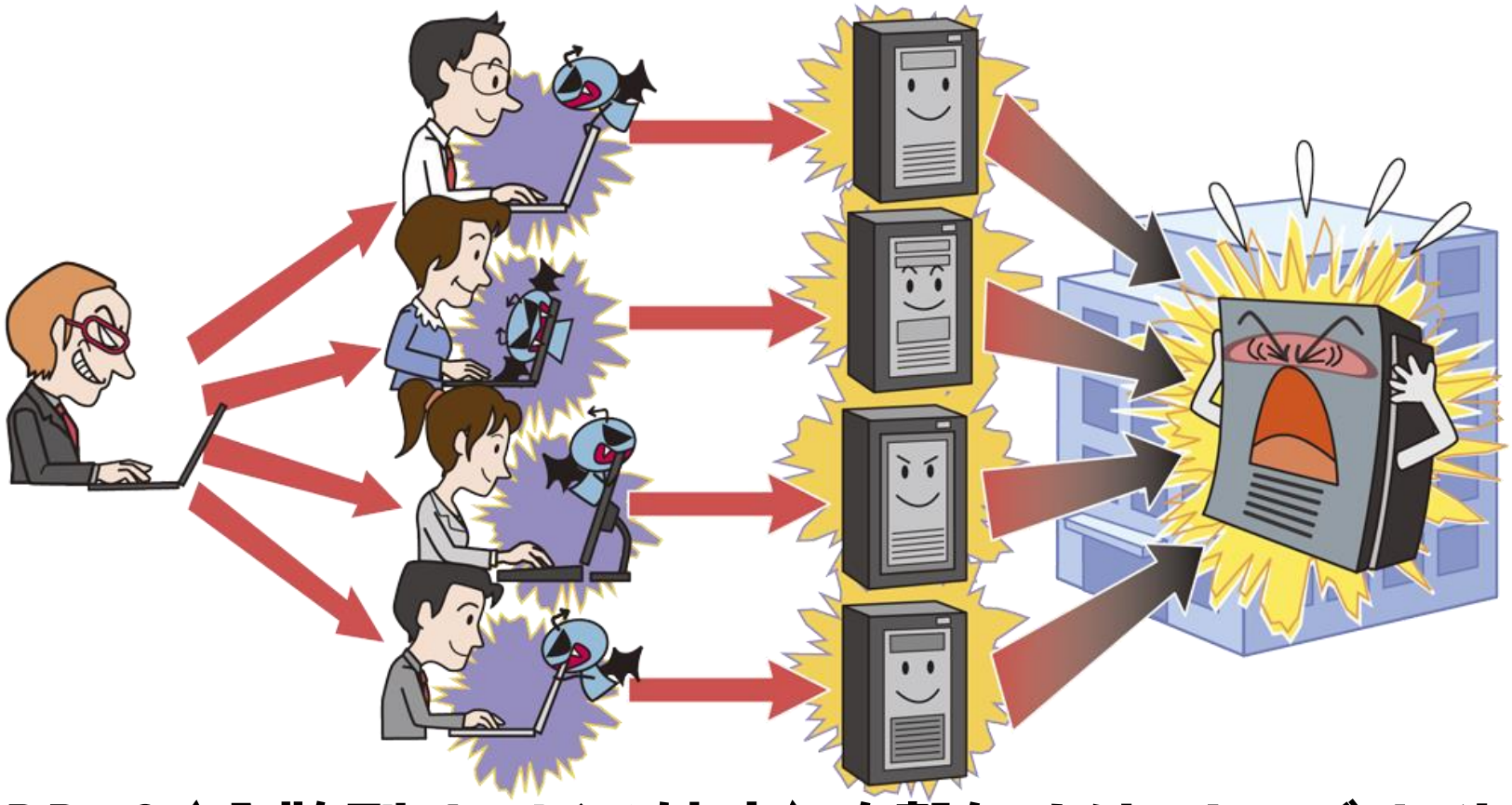


【3位】ウェブサービスからの個人情報の窃取
～ハッカー集団による甚大な被害～

- 対策一覧
  - ウェブサービス運営者
    - セキュアなウェブサービスの構築
      （登録する個人情報も必要最低限に）
    - OS・ソフトウェアの更新
    - WAF・IPSの導入
  - ウェブサービス利用者
    - 不要な情報は極力サイトに登録しない

安全なウェブサービスの構築は
セキュリティを担保した設計と開発が必要

【4位】サービス妨害攻撃によるサービスの停止
～主義主張の誇示や金銭を目的とした猛威を振るうDDoS攻撃～



- DDoS（分散型サービス妨害）攻撃により、ウェブサイトを高負荷状態にして、利用者がアクセスできなくなる被害

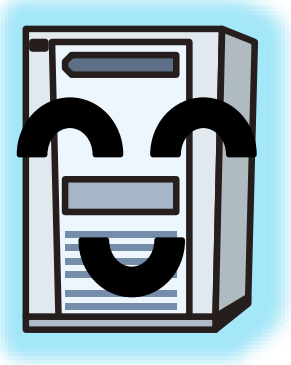
【4位】サービス妨害攻撃によるサービスの停止
～主義主張の誇示や金銭を目的とした猛威を振るうDDoS攻撃～

- 手口/影響
  - DDoS攻撃
    - ボットネットの悪用（ボットネットに攻撃命令をして負荷）
    - リフレクター攻撃（送信元を標的組織に詐称して多量の応答で負荷）
    - DNS水責め攻撃（権威DNSサーバーに負荷）
  - ウェブサイトがアクセス不可となり、業務を妨害される
- 2015年の事例/傾向
  - 厚労省のウェブサイトにDDoS攻撃
    - 安全確認の期間も含め約3日間ウェブサイトを停止
    - 主義主張が目的
  - 金銭目的によるDDoS攻撃
    - 複数の金融系企業でインターネットの取引画面に接続できない状態
    - 攻撃停止のため金銭の支払いを要求

【4位】サービス妨害攻撃によるサービスの停止
～主義主張の誇示や金銭を目的とした猛威を振るうDDoS攻撃～

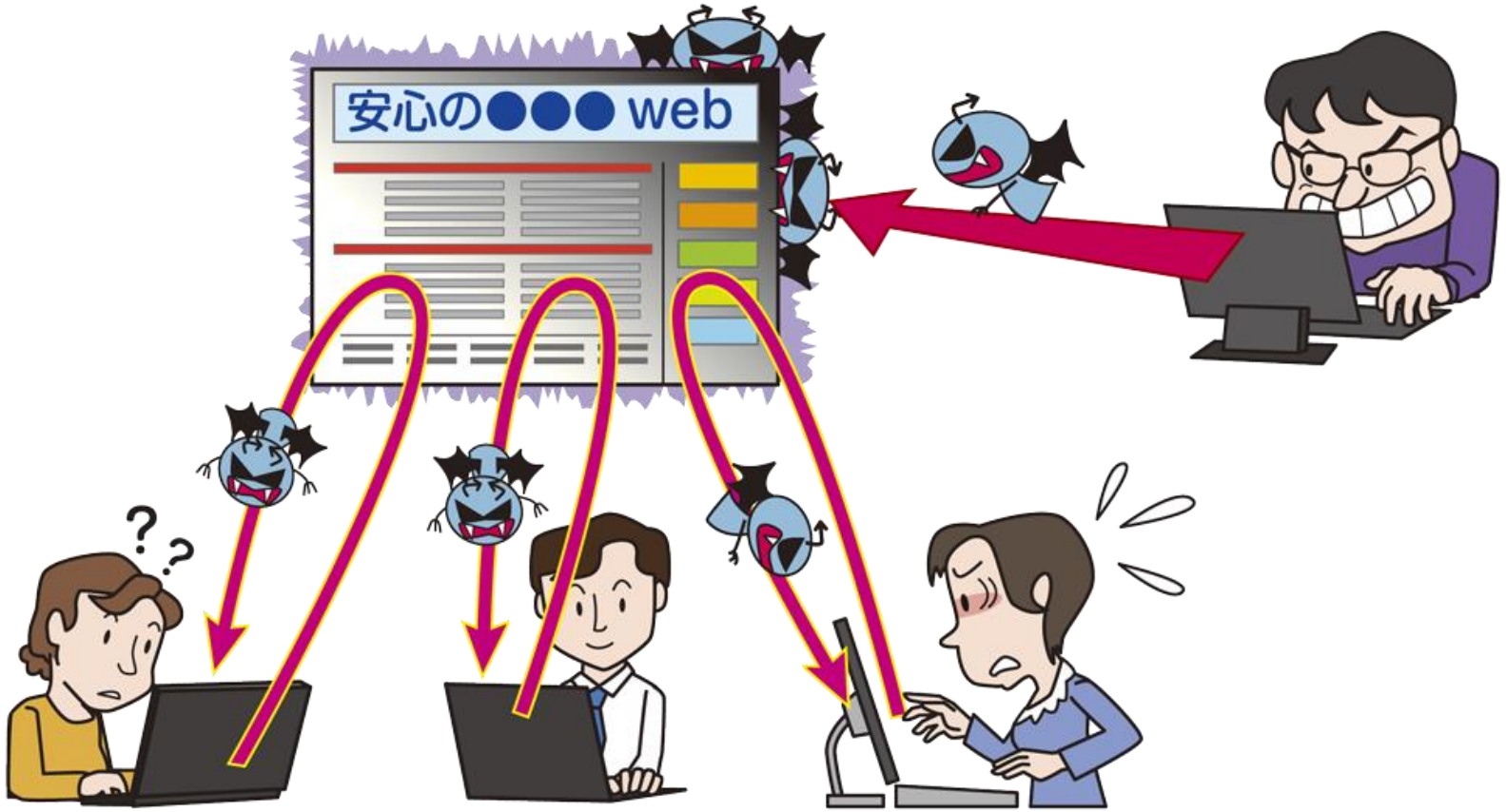
- 対策一覧
  - 個人・組織
    - OS・ソフトウェアの更新

      踏み台にならないため、利用している機器も含めて管理
  - 組織
    - DDoS攻撃の影響を緩和するISP等によるサービスの利用
    - 通信制御（DDoS攻撃元をブロック等）
    - システムの冗長化等の軽減策
    - サイト停止時の代替サーバーの用意



DDoS攻撃の被害にあわないよう
事前に十分なDDoS対策を

【5位】ウェブサイトの改ざん
～引き続き狙われるCMSの脆弱性～



- ウェブサイトを改ざんされてウイルス感染に悪用される
- サイト運営者はウイルス感染に加担した加害者側に

【5位】ウェブサイトの改ざん
～引き続き狙われるCMSの脆弱性～

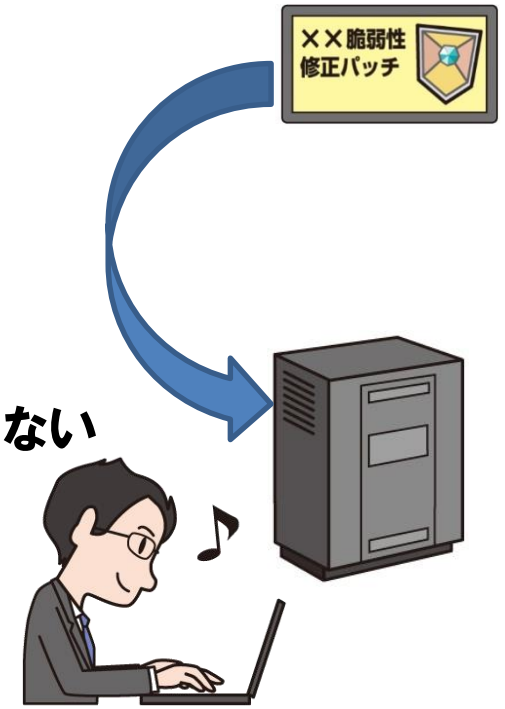
IPA

- 手口/影響
  - ソフトウェアやウェブアプリケーションの脆弱性を悪用
  - リモート管理用のサービスからの侵入
  - 設定不備によるウイルスのアップロード
  - ウイルス感染や
    主義主張・自己顕示に悪用される

- 2015年の事例/傾向
  - 2014年に引き続きコンテンツ管理システム(CMS)が標的に
    - WordPressやMagentoといったCMSやそのプラグインの脆弱性を悪用され多数のサイトが被害に
    - 管理されず放置されているウェブサイトが狙われる

【5位】ウェブサイトの改ざん
～引き続き狙われるCMSの脆弱性～

- 対策一覧
  - ウェブサイト運営者
    - OS・サーバーソフトウェアの更新
    - サーバーソフトウェアの設定の見直し
    - ウェブアプリケーションの脆弱性対策
    - アカウント・パスワードの適切な管理
    - 信頼できないサーバーソフトウェアを利用しない
    - 改ざん検知ソフトウェアの利用
  - ウェブサイト利用者
    - OS・ソフトウェアの更新
    - ウイルス対策ソフトの導入



ウェブサイト運営者は利用しているソフトウェアを適切に管理し、安全な運用を

10大脅威2016(組織)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	標的型攻撃による情報流出	○	○		○	○
2位	内部不正による情報漏えい				○	○
3位	ウェブサービスからの個人情報の窃取	○	○	○	○	○
4位	サービス妨害攻撃によるサービスの停止	△	△	△	○	○
5位	ウェブサイトの改ざん	○	○	○	○	○

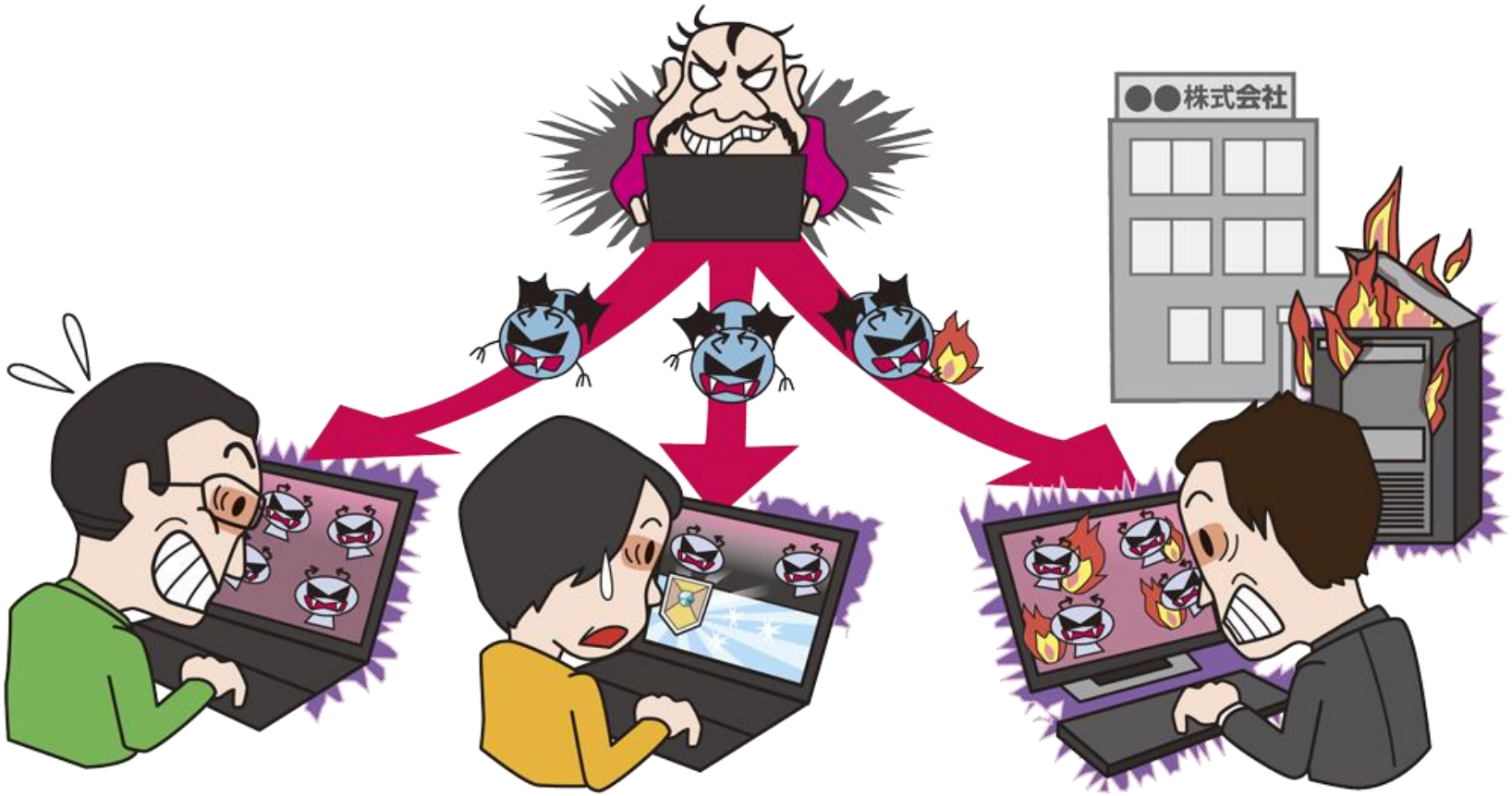
凡例：○ 対策効果あり、または部分的に効果あり
△ 踏み台(攻撃者)にならないための対策

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

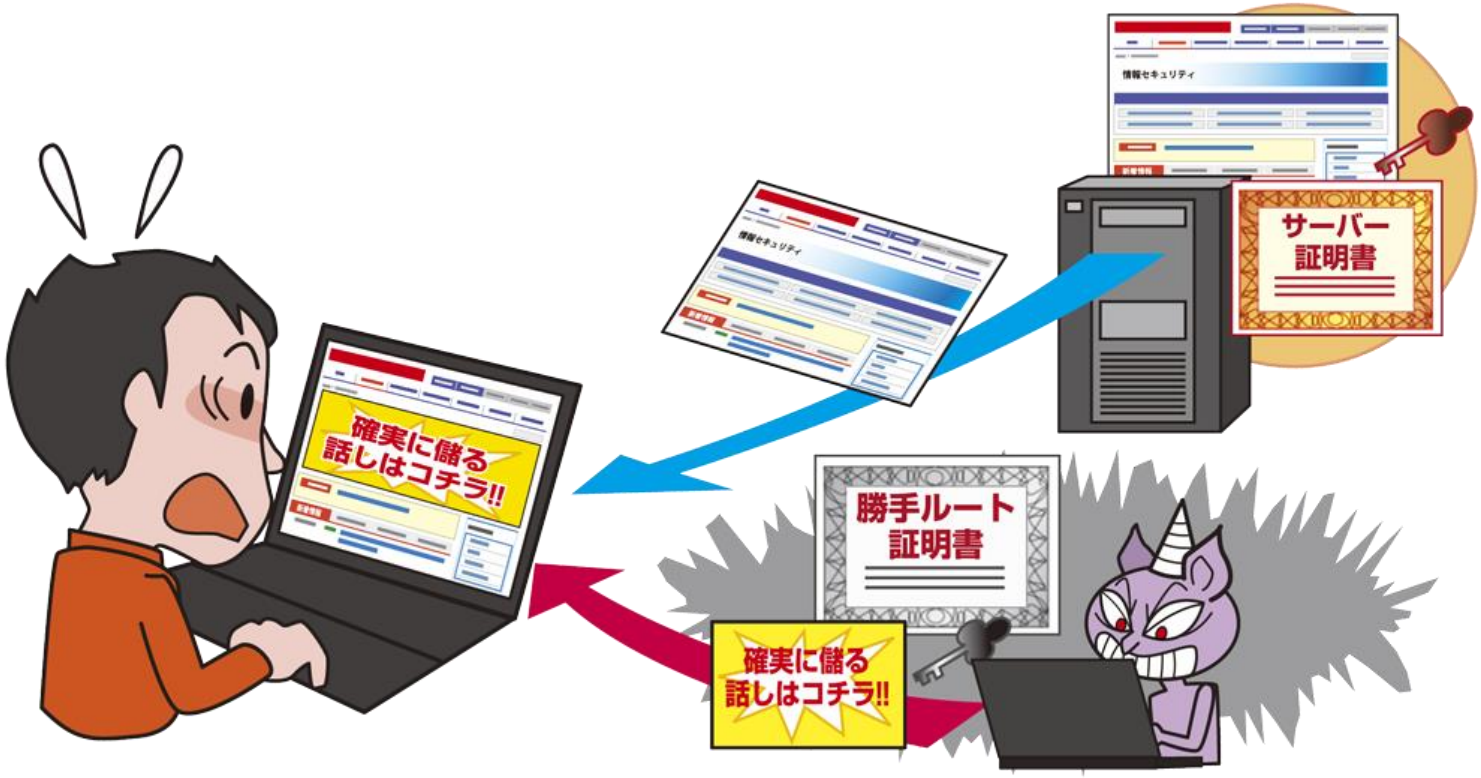
1．サポートの終了したソフトウェアを継続使用する危険性
～サーバーOSやブラウザも最新版の利用へ移行を～

- 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

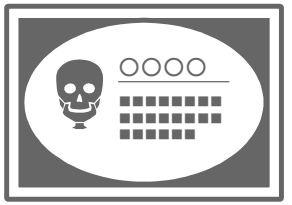
～ルート証明書の強制インストールに御用心～



- 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



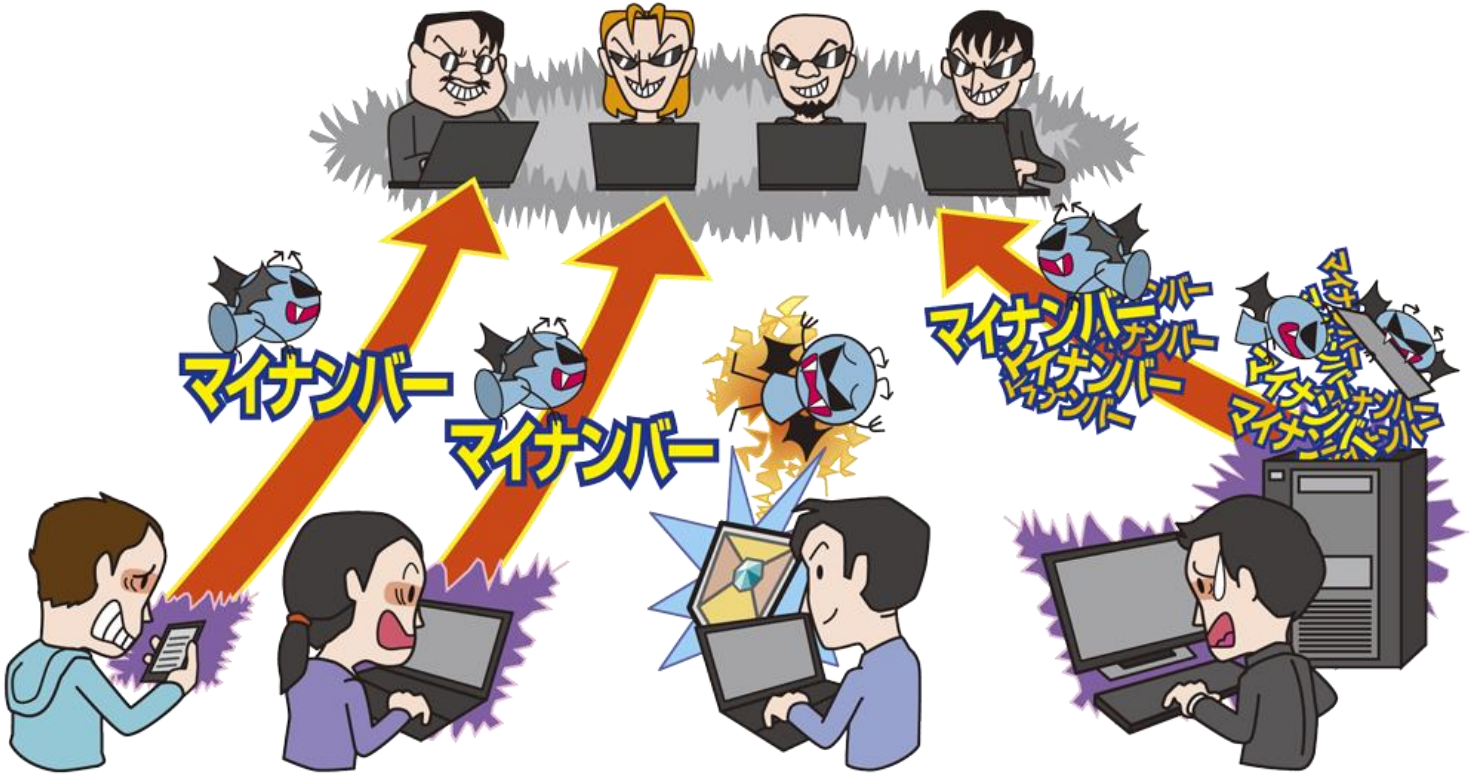
2. 証明書の導入・設定不備や検証不備に起因する脅威と対策
～ルート証明書の強制インストールに御用心～

- 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