学校と企業における セキュリティ対策と 情報リテラシー

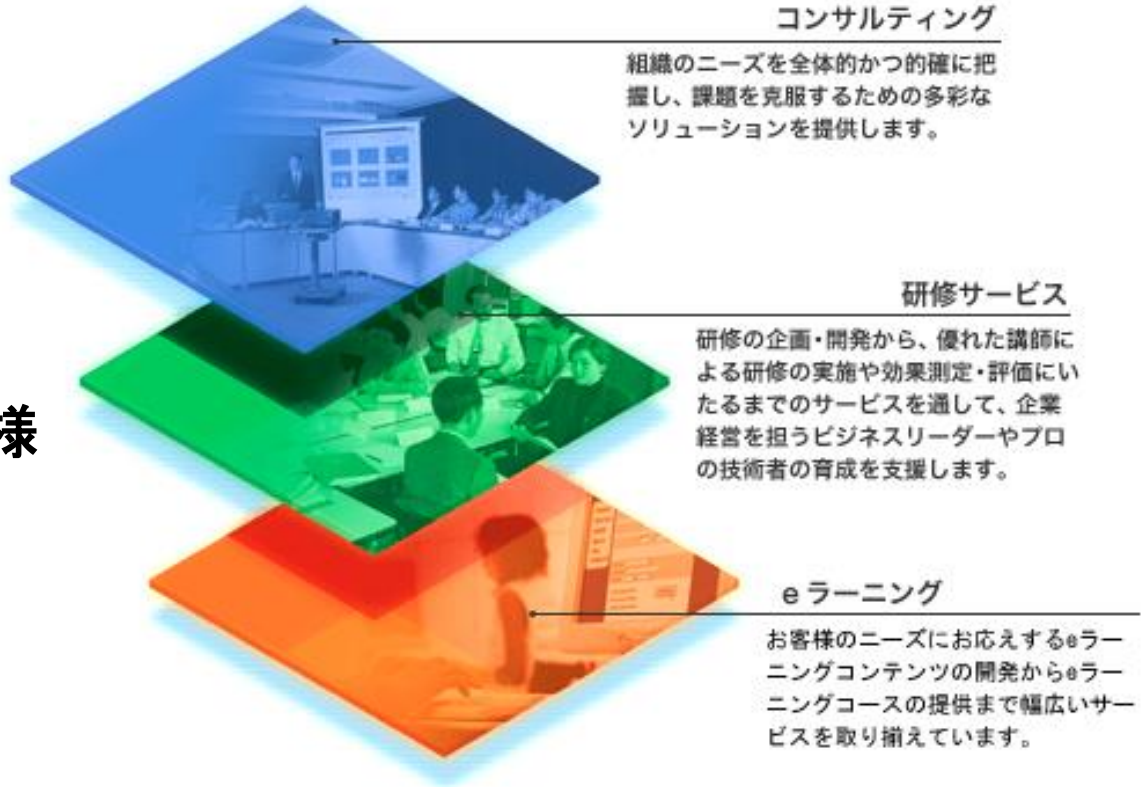
NECマネジメントパートナー
人材開発サービス事業部
山崎明子

自己紹介

- 学歴
  - 東京学芸大学 A類 学校教育課 心理学専修
- 職歴
  - NEC　人材開発部 ソフトウェア教育部
  - NEC　C&Cシステム教育部
  - NEC　Eラーニング事業部
  - NECラーニング　テクノロジー研修事業
  - NECマネジメントパートナー 人材開発サービス事業部
- その他
  - Microsoft MVP for Visual Basic 2003～2011
  - 佐賀県　先進的ICT利活用教育推進チーム　顧問団　外部アドバイザー 2014

NECマネジメントパートナー
人材開発サービス事業部

- 主なサービス
  - コンサルティング
  - 研修サービス
  - Eラーニング
- 対象
  - 企業・官公庁のお客様
  - NECグループ
- 主な研修内容
  - 新人研修
  - 技術者研修
  - 階層別研修
  - :



情報セキュリティ対策
学校と企業で何が違う？

- 基本は同じ
  - 考え方
  - 体制
- 違うことは？
  - 事例
  - 場面
  - 対象

- 企業の例が参考になる！

企業の情報セキュイリティ対策

- **体制＋研修**

体制

- 情報システムの管理体制
- 運用の管理体制
- 定期的なチェック体制
- 事故発生時の連絡体制

研修

- 繰り返し研修
- トレンド紹介
- 事故事例紹介
  による注意喚起

企業の一般的なセキュリティ体制

会社（戦略本部）	ポリシーの策定
推進会議	推進計画、施策検討
職場の推進者	情報セキュリティ管理・推進
全社員	するべきこと、してはいけないことを踏まえて行動

企業が求める情報リテラシー研修

- マインドの醸成が中心
  - 当事者意識
    - 社会的な影響
    - 自分への影響
- 「知っている」から「できる」へ
  - 「知っている」だけではセキュリティ対策にならない
  - 「できる」、「常にやっている！」が重要

最初に新入社員が学ぶこと

- 基本：セキュリティ入門
  - 1.情報セキュリティの重要性
  - 2.不正アクセス概要
  - 3.デスクトップセキュリティ
  - 4.コンピュータウイルス対策
  - 5.暗号技術によるセキュリティ対策
  - 6.企業倫理とセキュリティポリシー
- ＋最新の情報リテラシー
  - コンプライアンス
  - 情報セキュリティ
  - 個人情報保護

私が最近受講したセキュリティ関連の社内必須研修

研修名	形態	頻度	対象
コンプライアンス研修	Web	年1回	全員
個人情報保護と情報セキュリティ	Web	年1回	全員
情報セキュリティ教育	集合型	年1回	特定メンバ
セキュリティマネジメント研修	Web	年1回	特定部門
標的型攻撃メール疑似体験教育	Web	不定期	全員
情報セキュリティについて考える	ビデオ＆懇談会	不定期	全員

企業の研修体系


新入社員・中途社員研修
基本的なセキュリティ
コンプライアンス
情報セキュリティ
コンプライアンス
個人情報保護
情報セキュリティ
繰り返し
繰り返し・・・
変化する攻撃への最新の対応

セキュリティの3要素


この3要素を損なう脅威からの保護
機密性
Confidentiality
完全性
Integrity
可用性
Availability

何を守るのか？

- 定義(JIS Q 27002)
  - 「情報及びその情報を取り扱うプロセス、システム、ネットワーク」
  - 具体的には
    - データ
    - ソフトウェアやサービス
    - ハードウェア

どう狙われるのか?

直接攻撃

受動攻撃

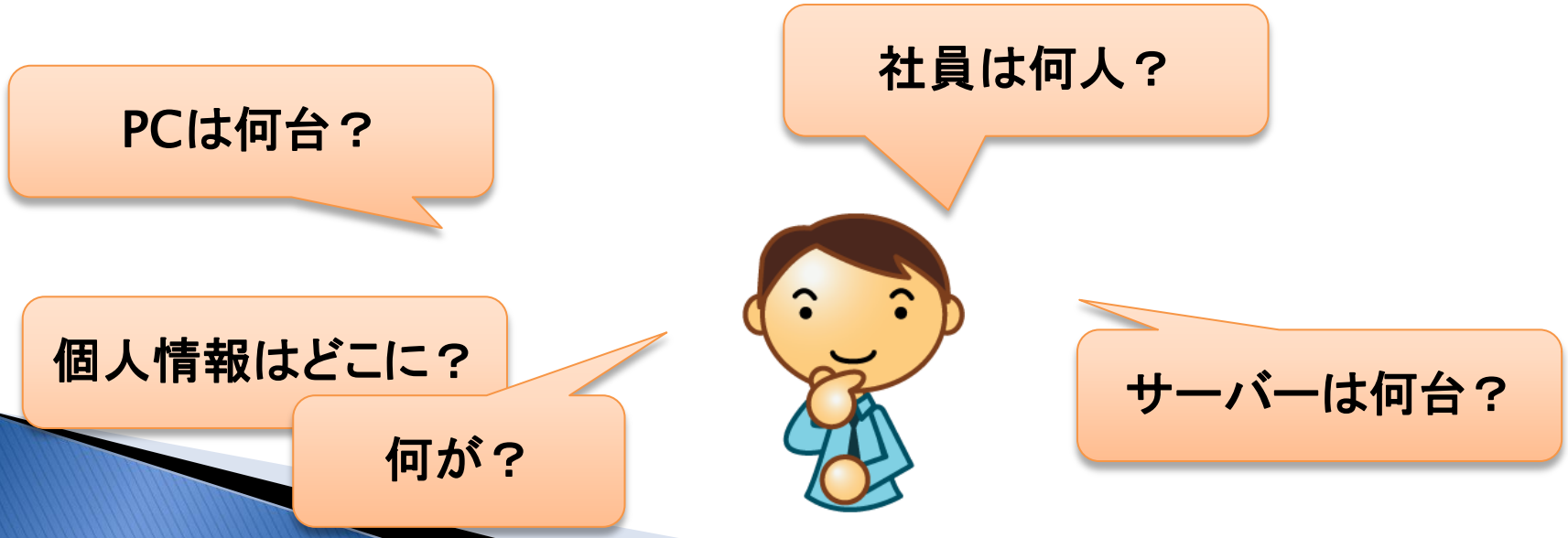
ソーシャル・エンジニアリング

被害はどのようにして発生するのか?

脅威 / 脆弱性 / 被害

どのように守るか？

- 見える化と多層防御
  - セキュリティは数えることから
    - 数えられるもの・・・管理できる
    - 数えられないもの・・・管理できない



多層防御の例　～

ゲートウェイ（入口）の対策	検知するシステム
	サーバーによる防御対策
PC・タブレット（端末）の対策	PCなどの脆弱性対策
	対策のマニュアル化
	暗号化
人的対策	啓発活動・セキュリティ研修

学校の現場では・・・

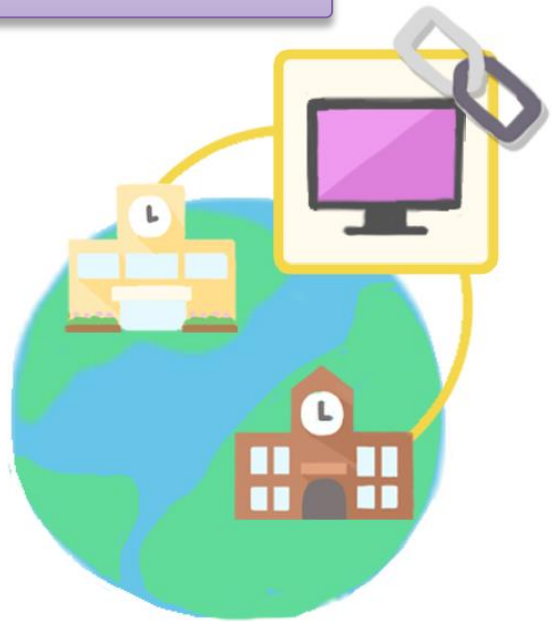
同じ？

違う？

これからの授業

学び方の改革/教える役割の変化

今までの枠を超えてセキュリティを
検討する必要性



セキュリティ体制の例　～学校編～

国・県・市区町村	必要な対策の検討 ポリシーの策定
推進者	ポリシーの徹底 先生方への日常的な指導
先生全員	児童生徒への指導 先生としての適切な行動
児童・生徒（保護者）	指導に基づいた行動

何を守るのか？

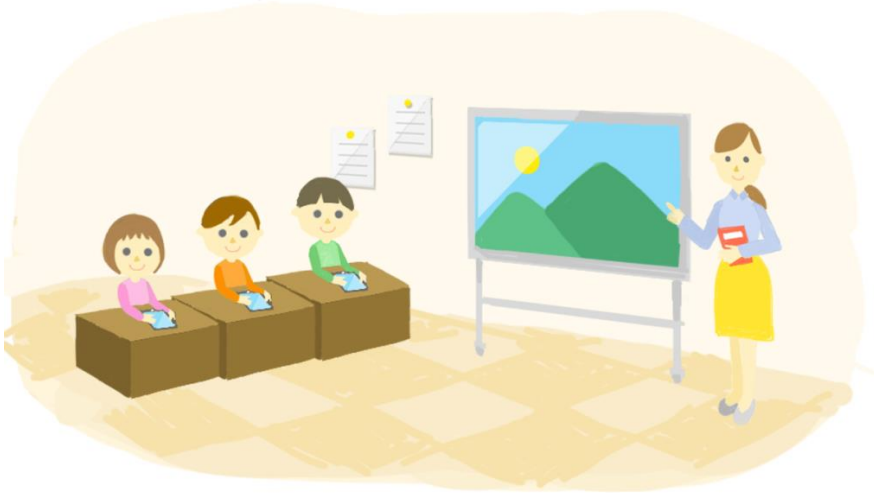
- 学校現場では・・
  - 友達を傷つけるような使い方はしていないか？
  - 学業を逸脱した使い方はしていないか？
  - コンプライアンス違反はないか？

どう狙われるのか?

直接攻撃

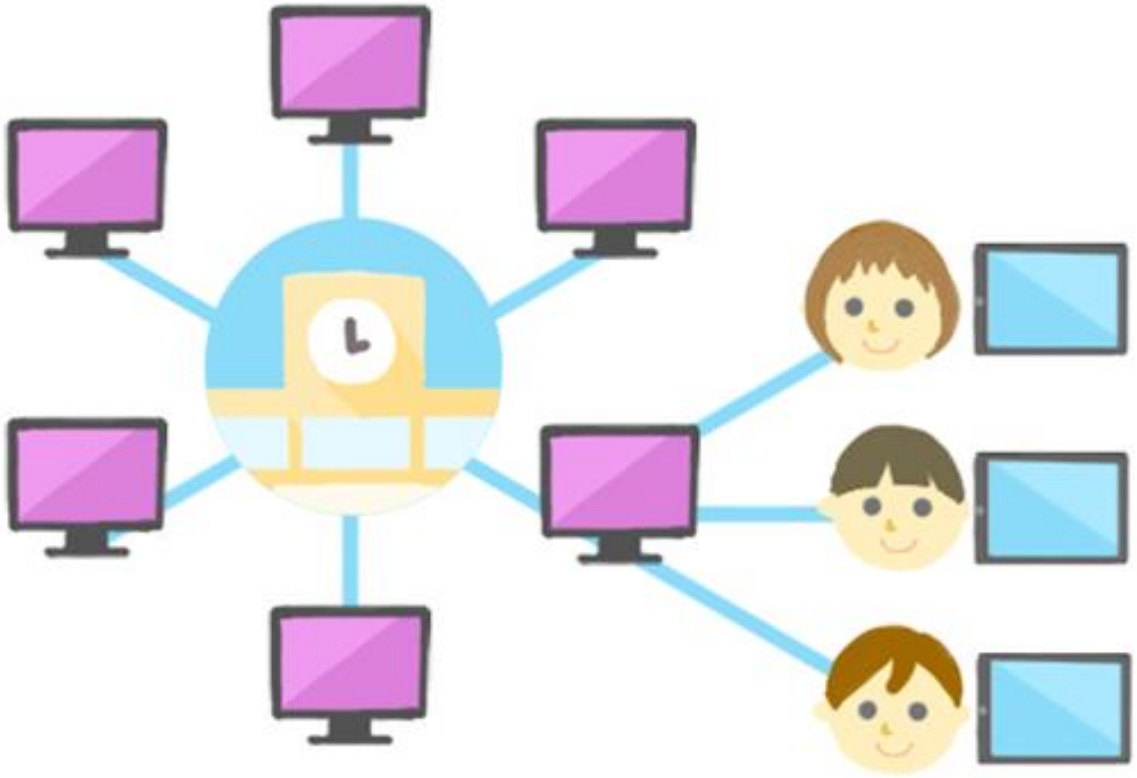
受動攻撃

ソーシャル・エンジニアリング



被害はどのようにして発生するのか?

脅威 / 脆弱性 / 被害



どの情報にどのような脅威があるのか？

どのように守るか？

- 見える化と多層防御
  - セキュリティは数えることから
    - 数えられるもの・・・管理できる
    - 数えられないもの・・・管理できない

先生、児童・生徒は何人？

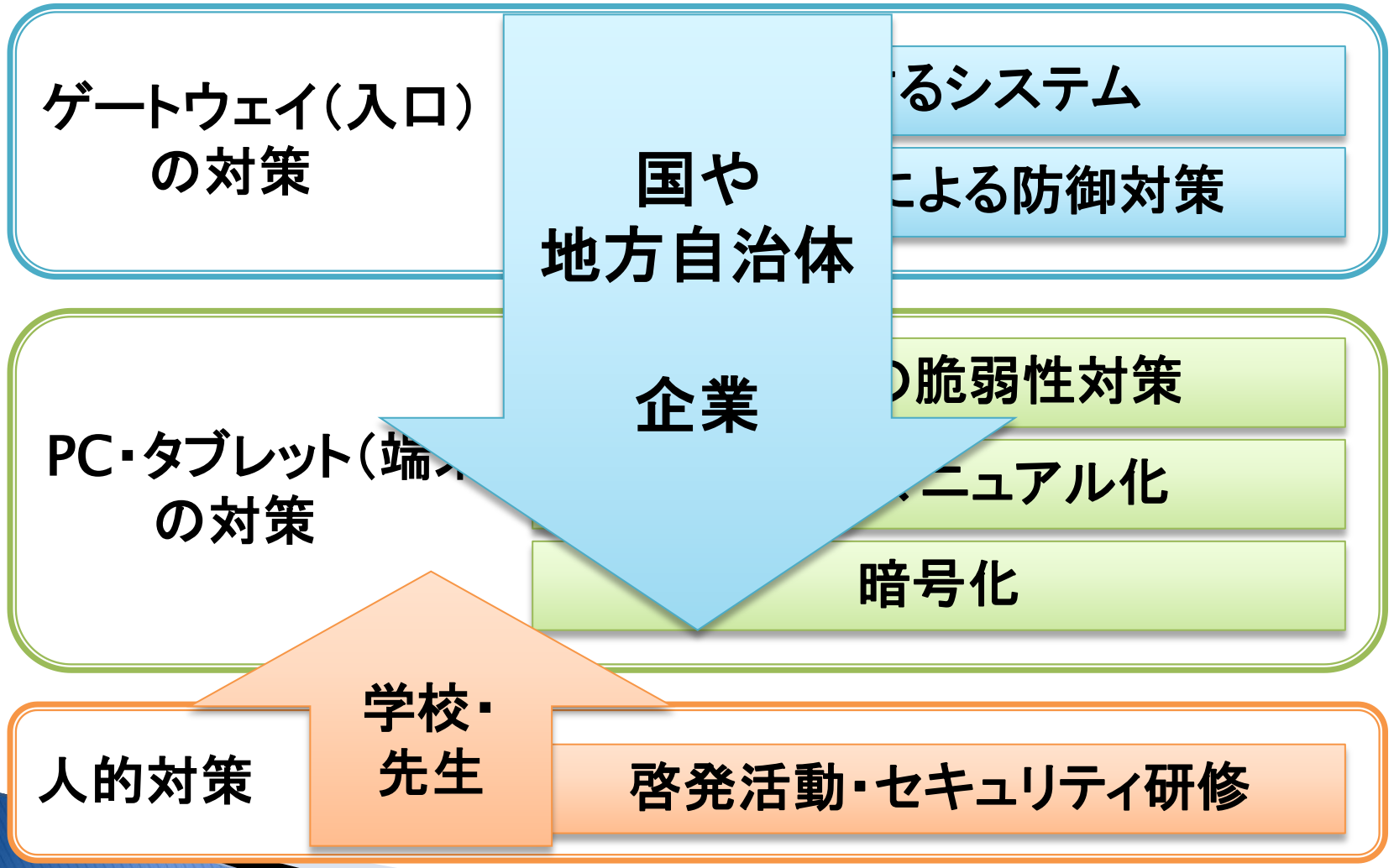
タブレットは何台？

個人情報はどこに？

何が？

どことどこ？
（理科室と図書室・・・）

多層防御の例


ゲートウェイ（入口）
の対策
るシステム
による防御対策
国や
地方自治体
企業
PC・タブレット（端
の対策
の脆弱性対策
ニュアル化
暗号化
学校・
先生
人的対策
啓発活動・セキュリティ研修

リスク管理のレベル

容認

対策なし

軽減

セキュリティソフト

転移

クラウドサービス

回避

不要ソフト利用禁止

情報リテラシーの研修体系

まとめ　情報セキュリティ管理のために

ルールづくり、基準づくり

管理体制づくり

運用体制づくり

人づくり(推進者、先生、児童・生徒)

まとめ　人づくりのために

情報リテラシー研修が重要

・情報セキュリティは何かについて知る
・学校でのリスクの可能性を知る

それぞれの役割に応じた適切な行動

・国・地方自治体、企業が何をしているのか
・自分が何をすべきか
・児童・生徒に何を伝えるべきか

最後までご清聴いただきまして
ありがとうございました