



National center of Incident readiness and  
Strategy for Cybersecurity

資料5

# 次期人材育成プログラム について

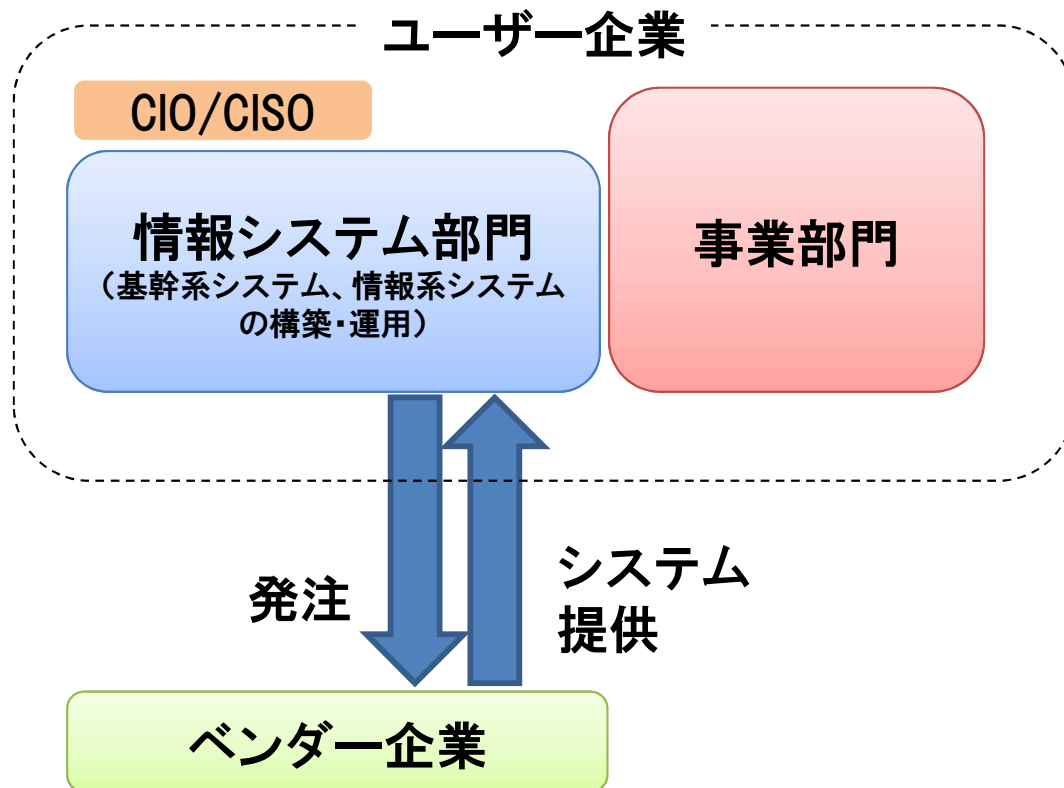
平成28年12月7日

サイバーセキュリティ戦略本部 普及啓発・人材育成専門調査会  
内閣サイバーセキュリティセンター (NISC)

# 1. ITの利活用に関する近年の変化～従来型～

## ① 従来型のユーザー企業におけるITの利活用

- 業務効率化によるコスト削減等を目的に、情報システム部門がベンダー企業から基幹系システム（生産・販売、会計、人事、給与、資産の管理等に関する企業内のシステム）や情報系システム（メールや文書作成、スケジュール管理等に関するシステム）を調達。
- 情報システム部門はベンダー企業と連携して、調達したシステムのサイバーセキュリティを見ていけばよかった。



### 【特徴】

←ユーザーのニーズ（要件）は、明確で、個々の事業に左右されにくい。

←システム構築の時間軸は、数年単位

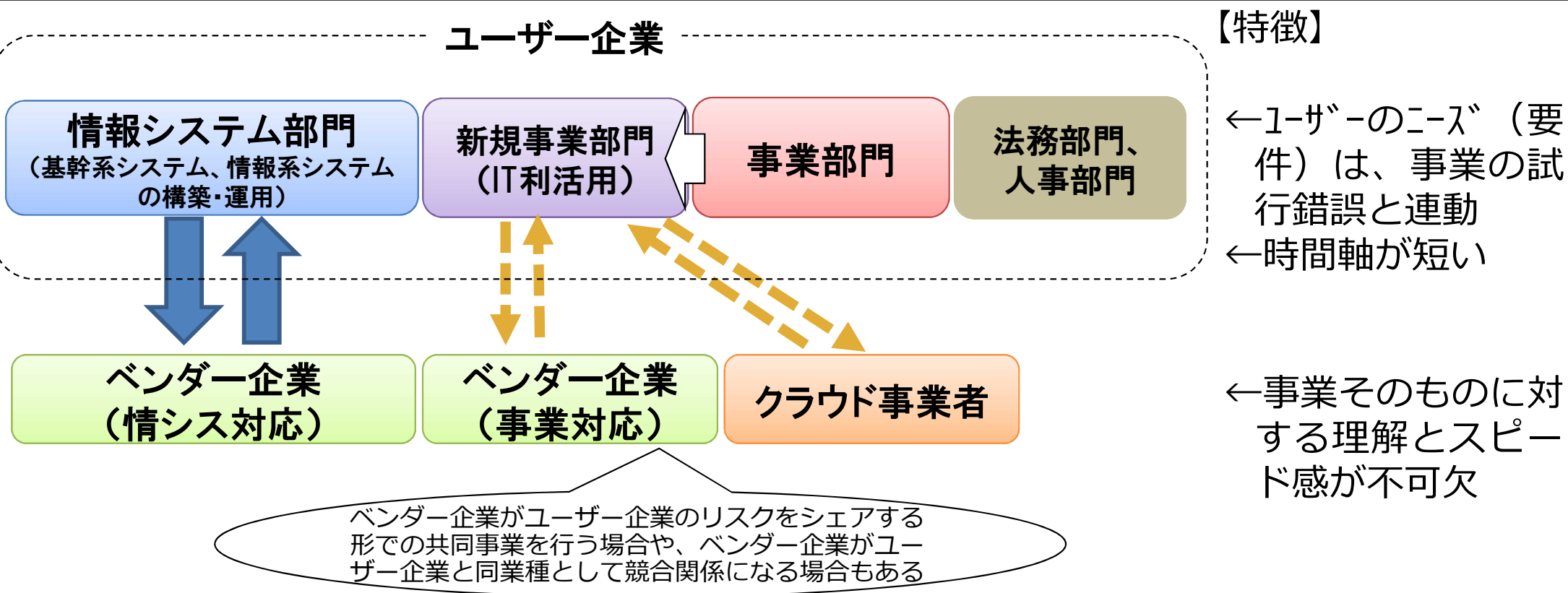
←固定したベンダーを相手に仕事

## 2. ITの利活用に関する近年の変化～近年の動向～

### ② 「挑戦」するユーザー企業のIT利活用に関する近年の動向

- IoTやAI、ビッグデータなど、ITを利活用して新しい価値を創造するような新規事業（ビジネス・イノベーション）を立ち上げる場合、従来型の情報システム部門が進めてきたようなシステムの構築・運用とは、要件や時間軸が異なる。
- サイバーセキュリティの不備などによる訴訟リスク対処の観点から法務部門などの関与も必要。

➡ **新規事業への「挑戦」と一体となった「責任」としてのサイバーセキュリティが必要ではないか。企業内におけるサイバーセキュリティの関係者の広がりや踏まえた対応が必要ではないか。**





### 3. 企業の「挑戦」と「責任」を実現するための人材育成とは？（論点）NISC

#### 1. 経営層のリーダーシップ

（論点例）企業の「挑戦」と「責任」について判断する、すなわち、企業全体にわたってサイバーセキュリティを基礎としつつビジネスを推進するためには、経営層のリーダーシップが不可欠ではないか。

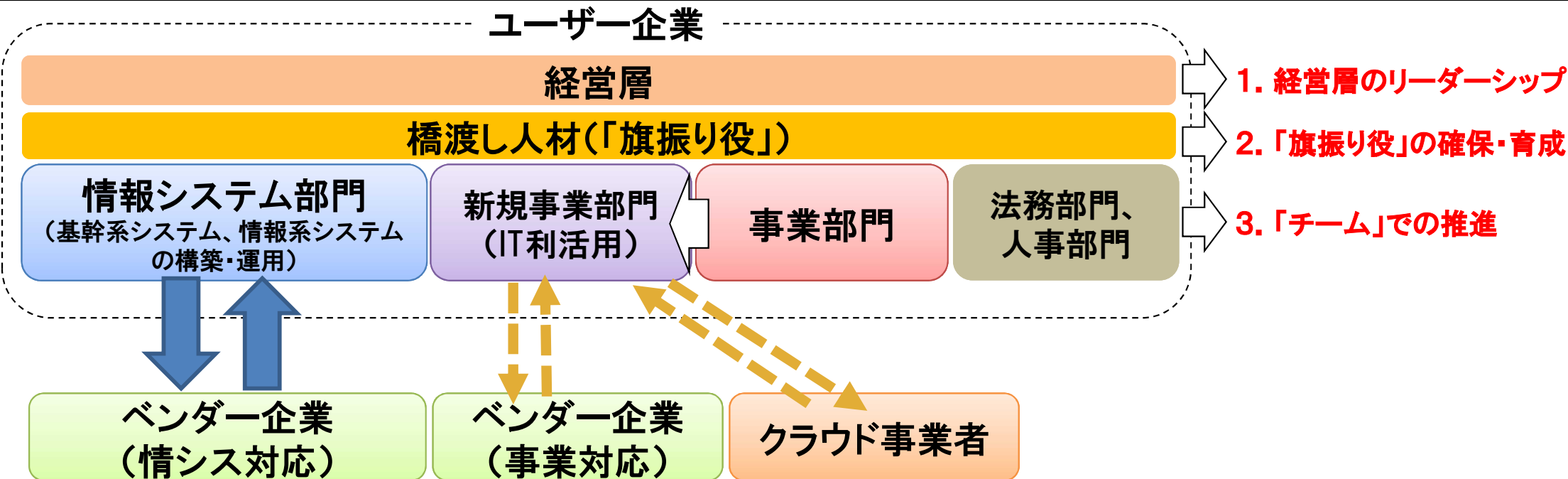
#### 2. 「旗振り役」の確保・育成

（論点例）経営者の方針を受けて、実態を踏まえた、企業内全体のサイバーセキュリティの企画・総合調整や実務者の人材育成を行うためには、橋渡し人材（「旗振り役」）の確保・育成が重要ではないか。

#### 3. 様々な役割や能力を持った人材による「チーム」での推進

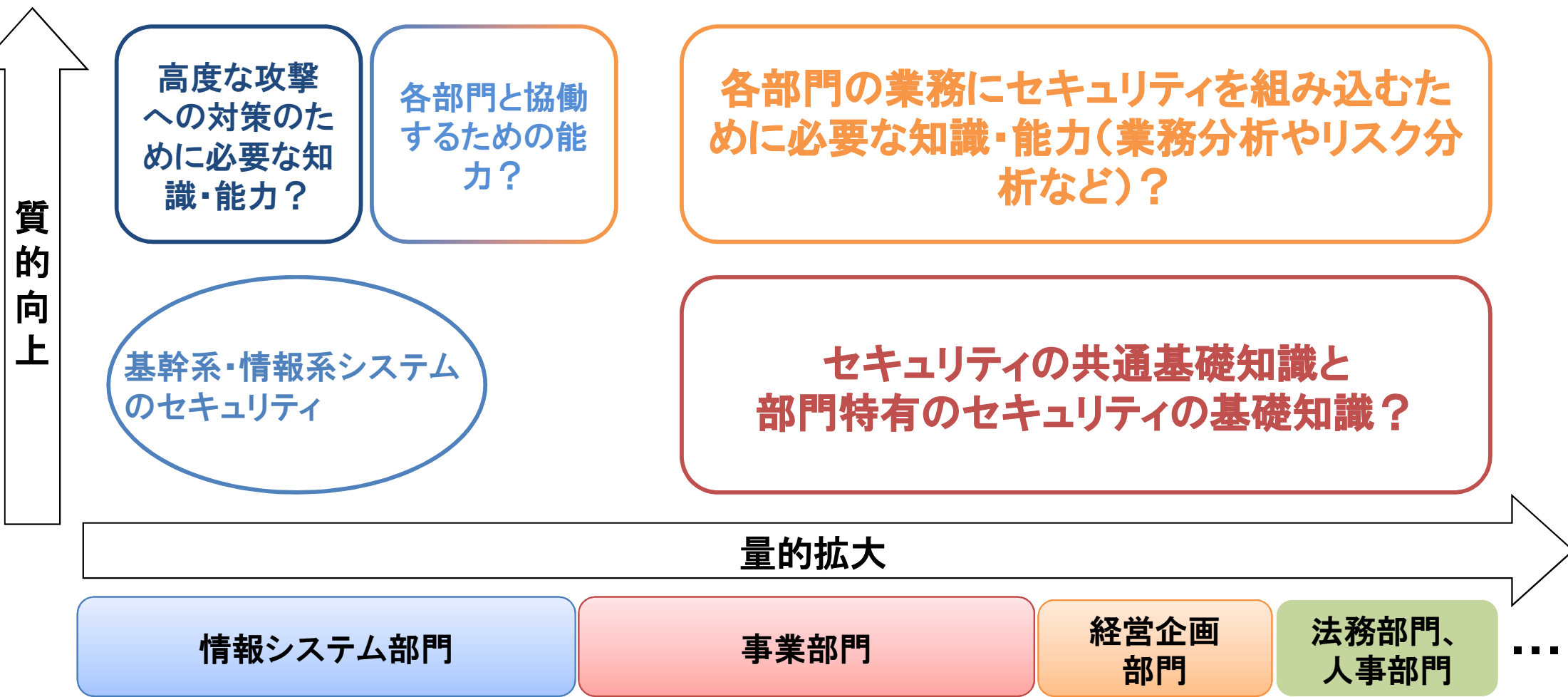
（論点例）

- ・セキュリティをよく知っているセキュリティの専門人材だけでなく、社会人の学び直しなどを通じ、〇〇（経営、製造、家電、・・・）を知っているセキュリティ人材の育成が必要ではないか。
- ・情報システム部門と事業部門との異動など、セキュリティ人材のキャリアパスの流動性を高めるべきではないか。（例えば、セキュリティをよく知っている人材であっても、事業を知ることなど、創意ある人材育成の仕組みが必要ではないか。）
- ・こうした人材育成は、事業のイノベーションを生むセキュリティ人材になるか。そのために必要なカリキュラムは何か。



# 4. 企業が必要とするセキュリティ人材像への対応とは？

- 「セキュリティに強い人材」のみならず「セキュリティにも強い人材」の育成をどのように進めるか？
- 企業が「挑戦」するためにITを利活用していく中で、情報システム部門だけでなく、事業・経営・法務・人事等の部門がセキュリティ対策の議論が出来るよう、基礎知識を身に着けるべきではないか？
- その上で、各部門の業務にセキュリティを組み込むために必要な知識・能力とは何か？（情報システム部門、事業・経営・法務・人事等の部門でそれぞれ求められる知識・能力は何か？）
- 各部門の人材育成に、こうした知識・能力を育成するためのコンテンツを組み込んでいくべきではないか？



## 5. セキュリティ技術のイノベーション、個人が常につながることを踏まえた対応について

### ①セキュリティ技術のイノベーション

- 画期的なセキュリティ技術は、これまでの情報セキュリティエンジニアが提供してきた価値に対する評価を変える可能性があるのではないか。
- 将来の進化（セキュリティ技術のイノベーション）に柔軟に対応できるよう、ジョブチェンジによるキャリアパスを視野に入れた基礎力の高いハイブリッド型人材の育成が必要ではないか。
- セキュリティ技術のイノベーションを生み出すため、セキュリティを学問領域として体系化し、大学等における教育カリキュラムを確立すべきではないか。

#### 【セキュリティ技術のイノベーションの例】

##### （AIを活用したセキュリティ技術）

- ・データマイニング、機械学習などにより、非構造化データや自然言語を含めた脅威情報を理解し、潜在的な脅威を特定。

#### 【社会において必要な能力に関する提言の例】

- ① 21世紀型能力（国立教育政策研究所）（2013）
  - ・基礎力（言語・数量・情報のスキル）
  - ・思考力（問題解決力、論理的思考力等）
  - ・実践力（自律的活動力、人間関係形成力等）
- ② 社会人基礎力（経済産業省）（2013）
  - ・前に踏み出す力、考え抜く力、チームで働く力

### ②個人がネットワークに常につながる時代

- より若年の段階から、ますます個人がネットワークに常につながる時代になると、基礎的な知識や技能を伴うセキュリティマインドを若年層から持つことが必要ではないか。
- そのためには、高等教育以降の人材育成に加えて、裾野が広い初等中等段階の積極的なセキュリティ教育が有効ではないか。

#### 【スマートフォン所有・利用率】

小学生：2.1%（平成24年度） → 23.7%（平成27年度）  
中学生：13.0%（平成24年度） → 45.8%（平成27年度）

#### 【インターネットの平均利用時間】

小学生：84.8分/日  
中学生：127.3分/日

（青少年のインターネット利用環境実態調査（平成27年度～平成21年度 内閣府））

# 6. 社会・経済の変化を見据えた人材育成の方向性 (イメージ) NISC



社会・経済  
の変化

生産年齢人口の急減

価値観・ライフスタイルの多様化

グローバル化・多極化

消費行動の変化 (コト (体験) の重視)

業態・職業の在り方の変化

ハードや通信の低コスト化

オープンイノベーション重視

ITの進化

人材面の課題

方向性

## (1) ITの利活用の広がり

IoTの普及、ビッグデータ・AIの活用、オープンイノベーションの広がりなど、ITの利活用は、サイバー空間が物理空間ともつながり、大きく広がっていくのではないか。

ITを利活用した積極的な「挑戦」とそれに付随する「責任」としてサイバーセキュリティに取り組むことが必要ではないか。

さまざまな分野 (各業種の事業、安全、法務など) にセキュリティの範囲が広がっており、分野の壁にとらわれないことが必要ではないか。

- ・ 経営層の意識改革が必要ではないか？
- ・ 「旗振り役」が必要ではないか？
- ・ 様々な役割や能力を持った人材が「チーム」となって推進する必要ではないか？

## (2) セキュリティ技術のイノベーション

AIの活用など、画期的なセキュリティ技術が登場する可能性があるのではないか。

情報セキュリティエンジニアの需要を変える可能性があるのではないか。

セキュリティ技術のイノベーションを生み出すとともに、こうしたイノベーションに柔軟に対応していくことが必要ではないか。

企業間を含めたジョブチェンジによるキャリアパスも視野に入れた「基礎力」の高いハイブリッド型人材の育成を推進すべきではないか？カリキュラムを確立すべきではないか？

## (3) 個人が常につながる時代

より若年の段階から、ますます個人がネットワークに常につながるようになっていくのではないか。

技術だけに依存したセキュリティには限界があるのではないか。基礎的な知識や技能を伴うセキュリティマインドを若年層から持つことが必要ではないか。

高等教育以降の人材育成に加えて、裾野が広い初等中等段階の積極的なセキュリティ教育が有効ではないか？

# 7. 今後の検討スケジュール（イメージ）

<今回>

平成28年12月

平成29年1月

3月

普及啓発・人材  
育成専門調査会  
(第4回)

普及啓発・人材  
育成専門調査会  
(第5回)

普及啓発・人材  
育成専門調査会  
(第6回)

サイバーセ  
キュリティ  
戦略本部

普及啓発・人材  
育成専門調査会  
(第7回)

〔現状認識、課題及び  
必要な取組の提示〕

〔骨子案の提示〕

〔プログラム案  
の提示〕

〔プログラムの  
決定〕

プログラム  
作成スケ  
ジュール

骨子案の作成

プログラム案の作成

意見募集

具体的な  
作業内容

関係府省庁・企業・教育機関等からヒ  
アリング等

※普及・啓発  
プログラム

〔サイバーセキュリティ月間  
(2/1-3/18)の説明〕

〔骨子案の提示〕

〔プログラム案  
の提示〕