サイバーセキュリティ人材育成プログラム（骨子案）の全体概要

資料2

現状と課題

〇脅威は更に深刻化、これまでの人材育成の取組は一定の成果を得つつも専門性を高める取組等一層の充実が必要。

〇 ITの利活用により、新しい価値を創造するビジネスイ・ノベーションと一体となったサイバーセキュリティへの取組が必要。

→ビジネスにおけるそれぞれの役割の中で、サイバーセキュリティ全体を俯瞰でき、関連するサイバーセキュリティを実践できる人材の育成が必要。

〇ビジネスイノベーションを生み出せるサイバーセキュリティ人材の育成が必要。また、将来的な社会変化に対応するため、セキュリティに対する意識を若年層から高めることが必要。

今後の取組方針

【基本方針】　需要（雇用）と供給（教育）の好循環の形成

〇これまでの取組に加え、ITの利活用により新たな価値を創造するためのサイバーセキュリティ人材育成が必要。

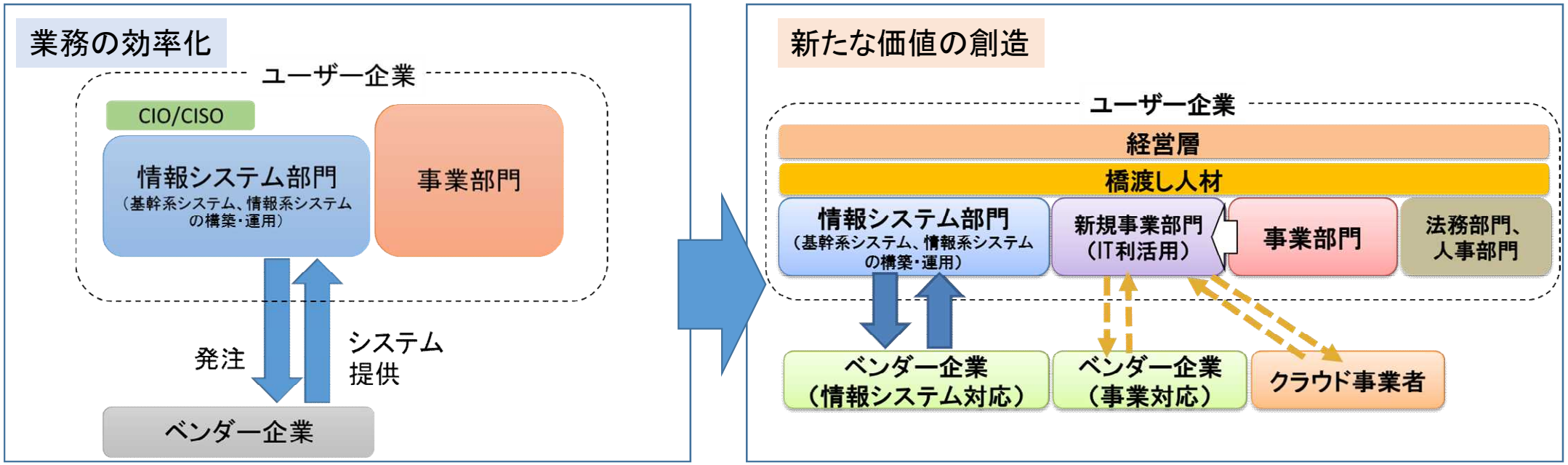
- 経営層：サイバーセキュリティを実務者層だけの問題ではなく経営問題として捉えるとともに、新たな価値の創造という「挑戦」に付随する。「責任」としてサイバーセキュリティに取り組むという意識改革を図る。
- 橋渡し人材層：経営層・実務者層のコーディネーターにとどまらず、ビジネス戦略と一体となってサイバーセキュリティの企画・立案を行い、実務者層を指揮できる橋渡し人材層の育成に取り組む。
- 実務者層：情報セキュリティ技術に関する知識・能力の向上だけでなく、チームとなってサイバーセキュリティを推進するための人材育成に取り組む。
- 高度人材：高度なセキュリティ技術の専門性を持ちつつ、ビジネスイノベーションが実現できる高度人材の育成に取り組む。
- 初等中等教育段階：児童生徒の情報活用能力（プログラミング的思考や情報セキュリティ、情報モラルを含む）を培う。

〇これまでの取組と新たな取組の質的向上を図るため、施策間連携の場をつくり、具体化（例：モデルとなるカリキュラムの策定）を図る。

まとめ（今後の検討）

産学官の取組状況や施策間連携の検討状況、サイバーセキュリティ人材をとりまく課題について、フォローアップを行い、必要に応じて本プログラムの見直しを検討。

ITの利活用に関する変化への対応



ITの利活用による業務効率化等を目的として、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。

【特徴】
・ユーザー企業のニーズ（要件）は、明確であり、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
・ベンダー企業は固定していることが多い

IoTやAI、ビッグデータなど、ITの利活用により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）への挑戦においては、事業部門がベンダー企業やクラウド事業者などからシステムを調達。

【特徴】
・ユーザー企業のニーズ（要件）は、事業の試行錯誤と連動
・システム構築の時間軸は短く、事業そのものに対する理解とスピード感が不可欠
・クラウド事業者など新たなベンダーが関与することがある

		これまでの取組	新たな取組
セキュリティへの意識		業務効率化のための情報システムのセキュリティ	IoT、AIなど、ITの利活用により新しい価値を創造するための「挑戦」に付随するセキュリティ
主な対象		ITベンダー、セキュリティベンダー、 ユーザー企業の情報システム部門	経営企画部門、情報システム部門、事業部門、製造部門、法務部門など企業内の幅広い組織
重視される能力		サイバーセキュリティのスペシャリストとしての深い知識と実践力を持つこと	経営、IT、事業、製造、法務などそれぞれの役割を担うエキスパートとして関連するサイバーセキュリティの知識を持ち、異なるエキスパートやスペシャリストとチームとなって業務ができること
人材の規模		現在の人材：26.5万人（不足数：8.2万人） ※対企業アンケート（情報セキュリティ人材）をベースに不足数を推計（2014年のIPA推計）	現在の人材：28.1万人（不足数：13.2万人）＋認識されていない人材 ※対企業アンケート（事業部門も対象）をベースに不足数を推計（2016年の経済産業省推計）
取組	経営層	経営層が経営戦略の一環として情報セキュリティ対策をとらえることが重要（実務者任せにしない） ・「サイバーセキュリティ経営ガイドライン」の策定や中小企業向けの普及啓発	「挑戦」とそれに付随する「責任」として、リスクの一項目としてのサイバーセキュリティに取り組むことが重要。 ・「企業経営のためのサイバーセキュリティの考え方」を踏まえたフォローアップ、普及啓発
	橋渡し人材層	実務者層のリーダー層が経営層との調整を含めたコーディネーター（橋渡し役）となることが重要	ビジネス戦略と一体となってサイバーセキュリティの企画・立案し、経営層に説明し、実務者層（技術者等）を指揮する人材が重要 ・橋渡し人材層向けのセミナー等の開催、情報処理安全確保支援士の活用、学び直しプログラムの活用
	実務者層	情報セキュリティ技術に関する知識・能力を高めることが重要 ・職業実践力育成プログラムを通じたセキュリティ技術人材の育成（例：東京電機大学CySec）、実践的サイバー防御演習（CYDER）、情報処理安全確保支援士の創設	チームとなって推進するための人材育成の取組が重要 ・社会人の学び直しプログラムの活用（enPiT、産業サイバーセキュリティセンター）、高等専門学校における情報科の学生にとどまらないセキュリティ教育、セキュリティマネジメント試験の活用
	高度人材	高度なセキュリティ技術の専門性を持つ人材育成が重要 ・大学学部生・院生の育成（enPiT）、高専や専修学校における教育、ホワイトハッカーの育成（セキュリティキャンプ）、サイバーコロッセオ	ビジネスイノベーションが実現できる高度なセキュリティ人材の育成が重要 ・若手セキュリティエンジニアの育成（NICT）

これまでの各取組は、
着実に進展し、一定の成果。
橋渡し人材層の取組等一層の充実を図る必要

これまでの取組と新たな取組の質的向上を図るため、以下の取組を推進する。

〇具体的な施策間連携の強化（検討例）
- ・モデルとなるカリキュラムの策定のためのワーキンググループの設置
- ・実践的演習における共同実施やカリキュラムの共有
- ・教育や演習の参加による資格試験の一部免除