資料２－１

NISC

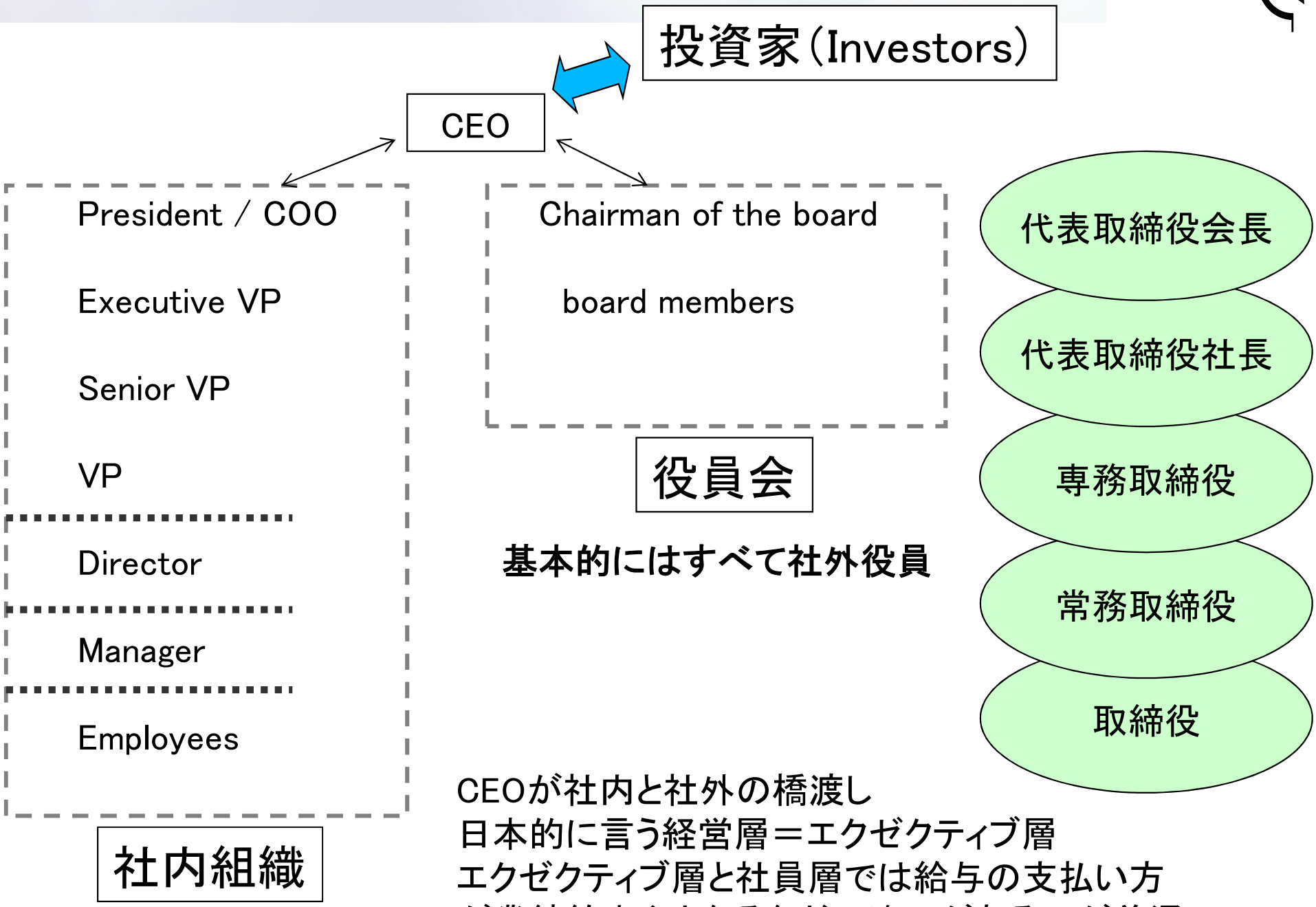
National center of Incident readiness and Strategy for Cybersecurity

欧米と日本における経営マインドの相違について

2016年6月1日

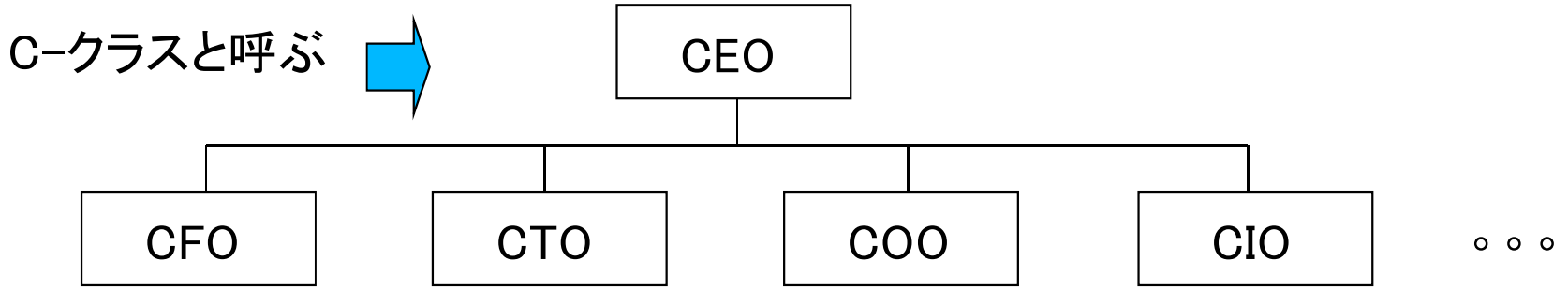
内閣サイバーセキュリティセンター（NISC）
情報セキュリティ指導専門官　八剱　洋一郎

エクゼクティブの名称



CEOが社内と社外の橋渡し
日本的に言う経営層＝エクゼクティブ層
エクゼクティブ層と社員層では給与の支払い方が業績給中心となるなどの違いがあるのが普通

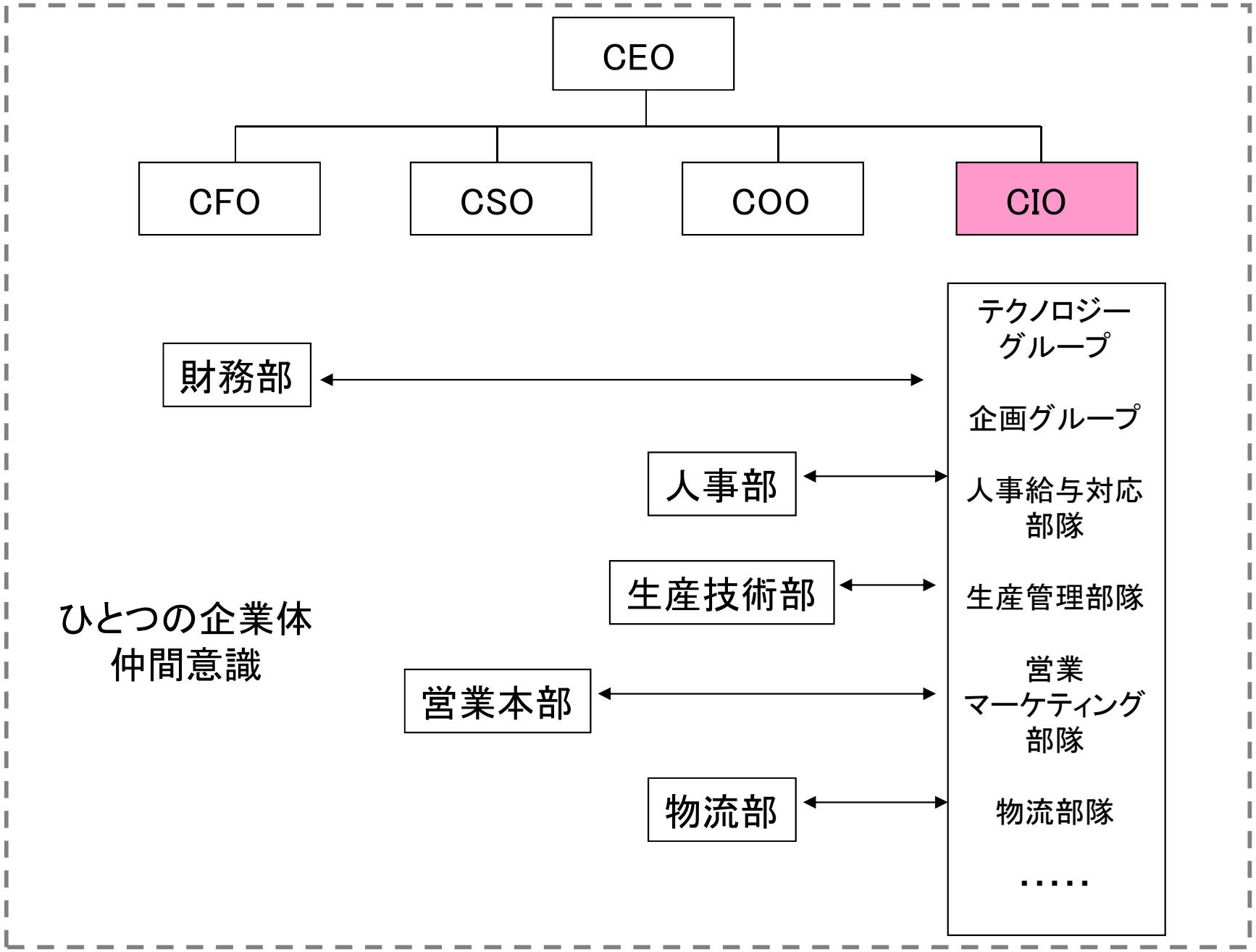
エクゼクティブの名称 その2



Chief Technology Officer
Chief Marketing Officer
Chief Sales Officer …

どれだけ、はっきりと職掌が公知されているかは微妙
CEO と CFOはかなり確立されている。。。
職掌が確立されているポジションのリスク

CIOという職種の難しさ　1



CIOという職種の難しさ　2：責任のグレーゾーン

伝統的に　電話＝総務部、データ通信＝情報システム部　という区分け

音声、データの統合プロジェクトから　どちらかに責任を集約　一般的には情報システム

モバイルの責任範囲も微妙

総務部系と情報システム系との連携の問題

人事系については完全に独立しているケースも多い

子会社のシステムにどこまで関与するかについても多様性あり

海外の分離もよくあるケース

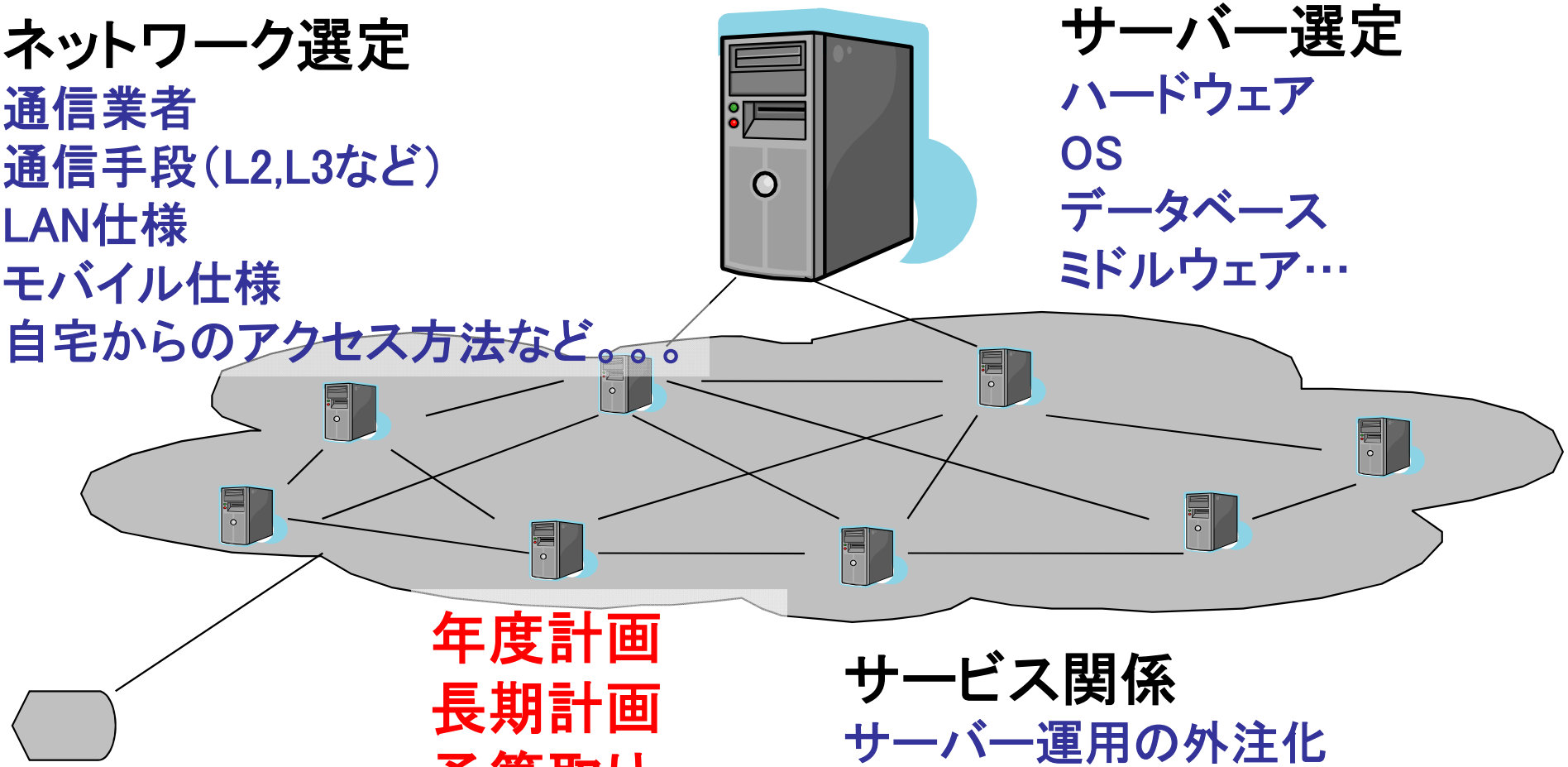
LANの取り扱い

製造、工場、物流センター、商品デザイン等に直結する情報システムの関与の度合い

CIOという職種の難しさ　3：わかりにくさ

ネットワーク選定
通信業者
通信手段（L2,L3など）
LAN仕様
モバイル仕様
自宅からのアクセス方法など。。。

サーバー選定
ハードウェア
OS
データベース
ミドルウェア…



年度計画
長期計画
予算取り、、、

PC(クライアント）選定
ハードウェア
OS
グループウェア…

サービス関係
サーバー運用の外注化
ヘルプデスクの外注化
ネットワーク監視
ハードウェアトラブル対応
ソフトウェアトラブル対応
アプリケーショントラブル対応

CIOという職種の難しさ　４：予算規模の大きさ

予算が大きい割りに何をしているのかわかりにくい

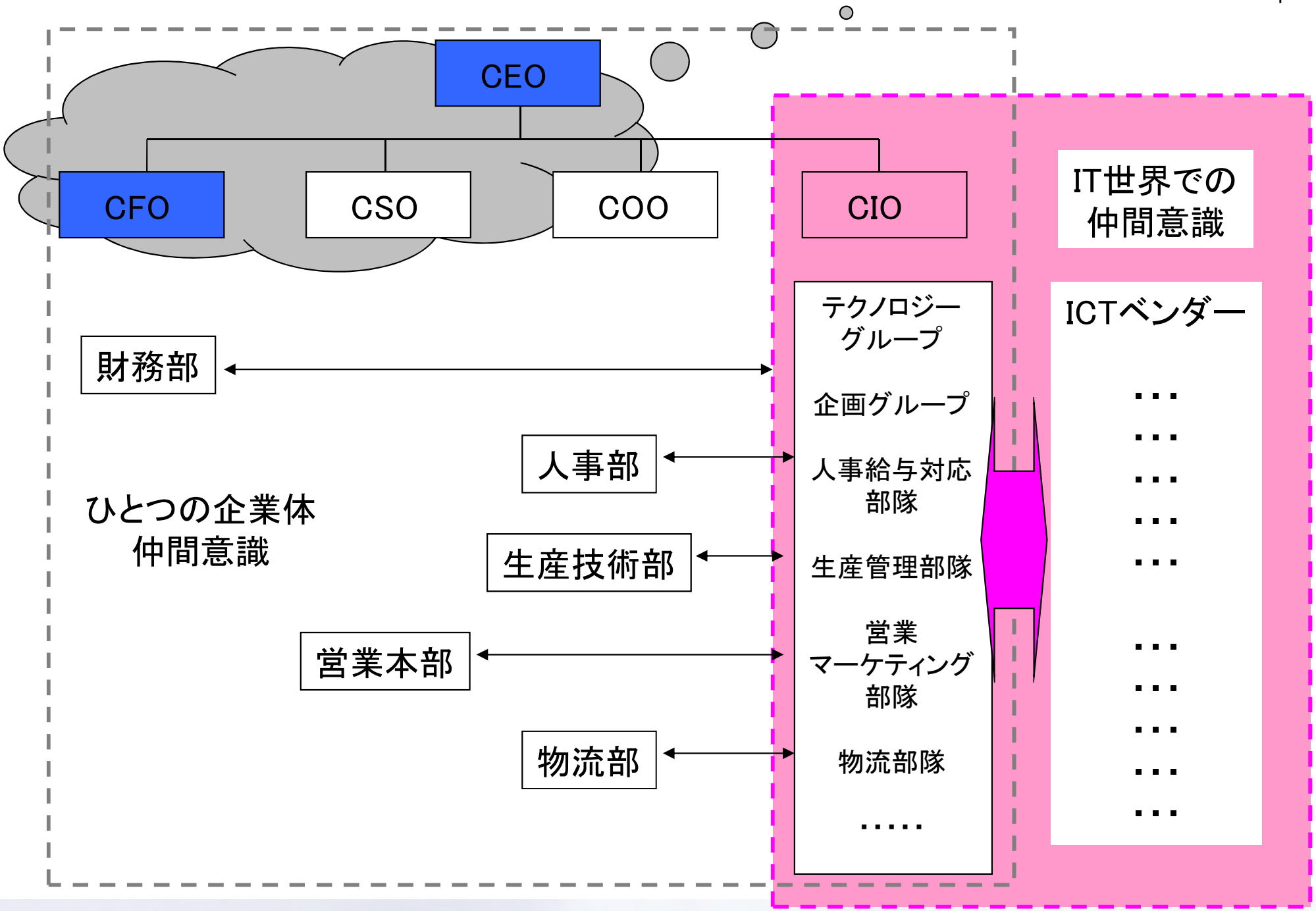
予算を増やした時の効果、減らした時の弊害もわかりにくい

高いから安全？

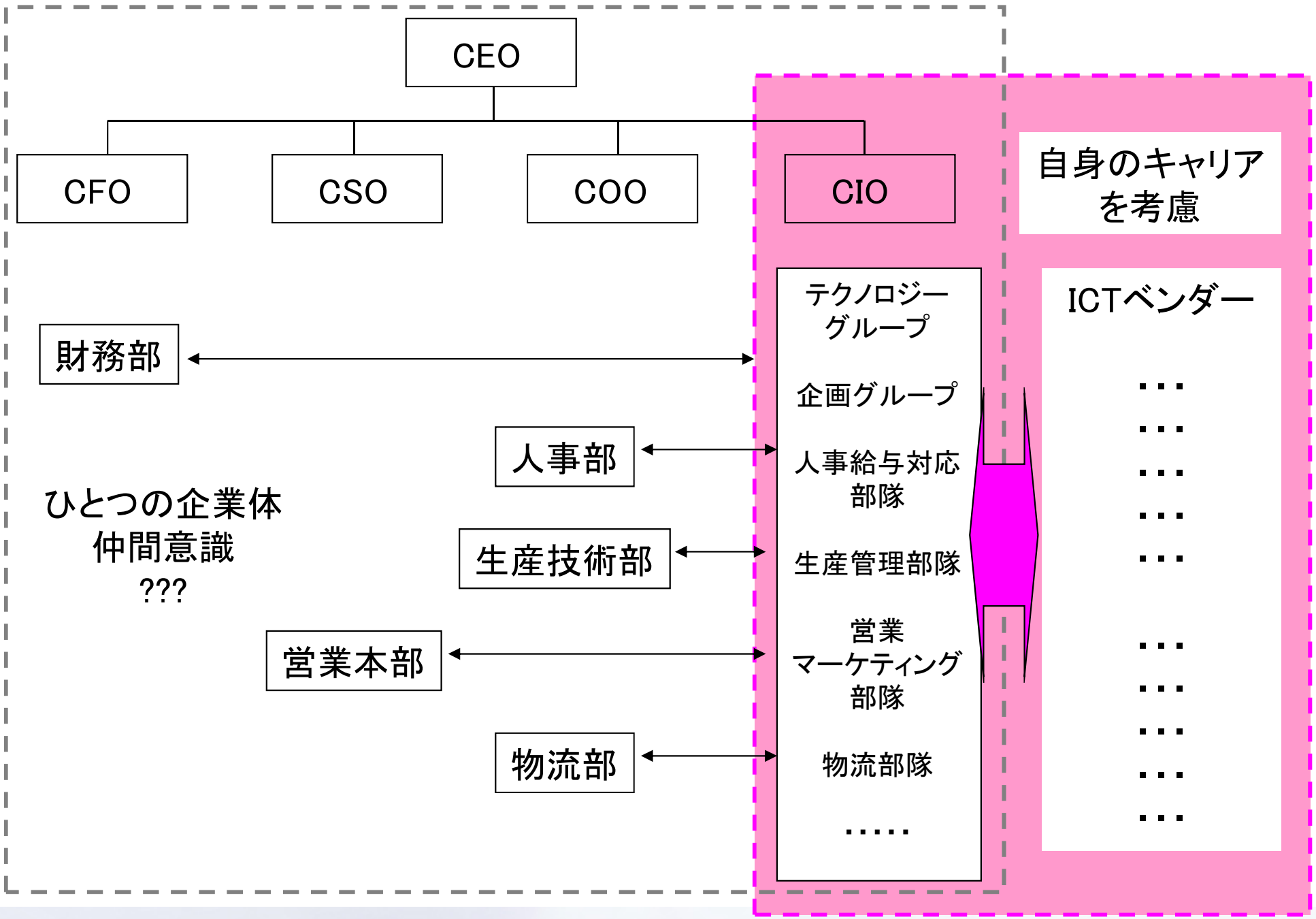
グローバルに通用しているものを使えば安心？

日本オリジナルのものは信用できない？

CIOという職種の難しさ　５



欧米のCIOも同様だが。。。



今回の取りまとめに向けて

日本企業固有の事情：
欧米では外部からCEOを招聘することも珍しくないが、その場合にはIT活用についての知見を持っていることが条件になることが多い。
日本では生え抜き人材が社長になることの方が多く、その場合、IT活用についての知見を有していない場合もありうる。
しかし、日本型社長は欧米型CEOに加えて、自社内事情や業界事情に精通しており、ITの知見を高められればそれなりのメリットが期待できる。
幸いにも日本の経営層もIT活用について理解しなければならないという自覚は十分に持っており何らかのきっかけでIT活用を戦略的に考える可能性は十分にある。

大きく広がるビジネスチャンス：
ネットパワーを活用し、B to Cの世界ではつい先日まで考えられなかったような急激なビジネス拡大ストーリーが続々と実現している。
一方でB to Bではネットワークを通じて急激なビジネス拡大を実現したケースはまだ少ない。
しかし、B to Bでの商取引を含めて、ネットワークを通じて、自動化していこうという流れは確実に進展しており、その結果、2015年9月のサイバーセキュリティ戦略で言う「連接融合情報社会」は確実に到来しつつある。

今回の取りまとめに向けて

高まるリスク:
今までの情報社会では、常に人間が関与していることを前提としていたため、トラブル回避、リスクマネジメントの考え方についても要所要所で人間の判断が入ることを前提としていた。
一方で今日ではIoTに代表される、機械同士の会話、通信等が実現している。この場合、機械同士のコミュニケーションの脆弱性を「踏み台」にして企業の枢要なノウハウにアクセスされるリスクが高まっている。
同様に、企業間取引において、セキュリティ防備の薄い会社から進入し、そこを「踏み台」にしてより上位の企業の枢要なデータにアクセスされてしまうリスクも顕在化しつつある。

経営者の責任:
最近東京証券取引所がとりまとめた「コーポレートガバナンス・コード」においても、その第三章において適切な情報開示と透明性の確保、そしてリスクやガバナンスに関わる情報の適切な開示が肝要であると明記されている。リスクと引き換えに大きなビジネスチャンスが期待される「連接融合情報社会」への取り組み状況は株主に対して開示すべき重要な項目のひとつと考えられる。
サイバーセキュリティに限らず、先進のIT活用は今後の企業経営に少なからず影響を与えることになるため、経営者は自身を含め、経営幹部層に対しての適切なトレーニングを考慮すべきである。