第２部

テレワークにおけるセキュリティ対策のあり方

２０１７年 8月 ２５日

ＣＩＯパートナーズ株式会社
松井　亮宏
CIOパートナーズ株式会社
https://www.cio-partners.co.jp

第２部の講演内容

第１章　情報セキュリティ対策とは

第２章　セキュリティ原理主義にならないために

第３章　テレワークで活用できるIT技術とセキュリティ

はじめに…

- セキュリティ対策は非常に多岐に渡る論点があります。
- 従って、今回のセミナーは「テレワークにおけるセキュリティ対策」に焦点を絞って講演します。
- また、ポイントを出来るだけ分かり易く解説する為に、具体例を用いていますが、反面、皆様の会社の実態とは異なる例示も少なくない、と考えられます。
- こうした点をご理解いただきたく、予めお願い申し上げます。

情報セキュリティ対策とは

● 元奈良先端大学院大学　山口英教授(2016年5月9日逝去)

誰もが感じていると思うが、どんな組織でも情報セキュリティ対策の実施は**本当に難しい**。なぜこれほど難しいのか。答は簡単だ。情報セキュリティ対策では、かなり複雑な問題を合理的に解く必要があるからだ。

情報システムは、もはや組織の基盤である。しかし、基盤化してしまったが故に、情報セキュリティ対策では、考慮しなければならない事項が多く、事項同士が相互依存しており、**組織毎に考慮すべき事項の構成が変わり**、かつ、**事項の内容も変化しうるものである**ことを考慮しなければならない。この結果、それぞれの組織が、情報セキュリティの問題を主体的に理解し、その解決方法を考え出すプロセスを設計し、**常に変化に対応できるメカニズムを構築しなければならない**ことになる。しっかりした体制を作り、**経営層の巻き込みを行い、技術、財務、法令、運用、教育、組織統治に関わる面倒な作業**をこなしていかなければならない。

そのためにすべきことは

1．事実に真正面から向き合う勇気を持つこと

2．良いものを学び、良さを吟味する力を持つこと

3．創意工夫に溢れた対策を徹底して考えること

情報セキュリティ対策とは

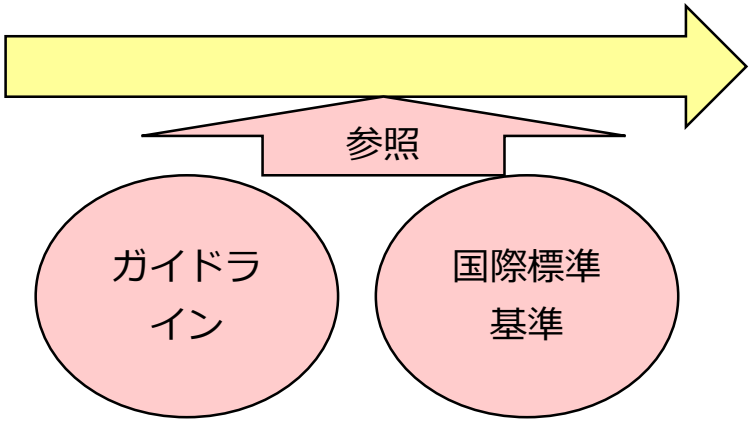
１．事実に真正面から向き合う勇気を持つこと

情報システムを取り巻く状況を的確に理解する	リスクアセスメントの実施
	情報資産の棚卸
	ユーザやアクセス権限などの把握
問題点を識別し解決策を検討する	問題を正しく認識すること
	問題点を責めるのではなく、 事前にトラブルが回避できたとして評価する

情報セキュリティ対策とは

2．良いものを学び、良さを吟味する力を持つこと

組織ごとの情報セキュリティ対策



オーダーメードの解決方法

内容を吟味し、組織に合う形で
取り込む
無条件に採用しない

3．創意工夫に溢れた対策を徹底して考えること

(そもそもの)
情報化の目的

VS

セキュリティ

- 生産性の向上・改善
- 業務で情報システムを活用
- 新しい事業・働き方の創造

情報化の目的
に合った対応

情報セキュリティ対策が「**目的**」で
はない！

● セキュリティ対策を施すためには，明確な目標を設定する必要がある。

目標は二つあり、

一つは、ITによる恩恵を最大化すること

もう一つが，リスクを最小化することである。

セキュリティ対策においては、これら二つは両立しなければいけないことでありかつ、これら二つは両立できることである

● セキュリティ対策で陥りやすい議論

データやシステムの現場での利用方法を知らないまま、どのデータやシステムをどの程度まで守るのかを明確にせずに、「どのようなセキュリティ対策を施せばよいのか」だけが議論される場合が多い

情報セキュリティ対策が
目的化すると

セキュリティ原理主義に陥いる！

- 過度な規制
- 変化に対する硬直化
- イノベーションへの妨げ

● セキュリティ対策において大事なこと

・セキュリティ対策に満点はない

セキュリティに対するリスクは、いくらお金を掛けて、人手を費やしても０にはできない
対策を検討し、実施した時点ではその時点での最適な対策を施したとしても、
IT技術の進化、組織・業務の変更、外部環境の変化、攻撃者の手口の巧妙化などですぐに陳腐化してしまう

・教科書的に正解の対策が企業にとっては必ずしも正解ではない

例：ランサムウェア(身代金要求攻撃)に感染したときの対応
　教科書的な正解：感染したパソコンを「すべて」調査し、復元を依頼する
　これを実施しようとすると・・・
　　調査・復元するためには1台10万円程度する。100台で1000万円程度かかる

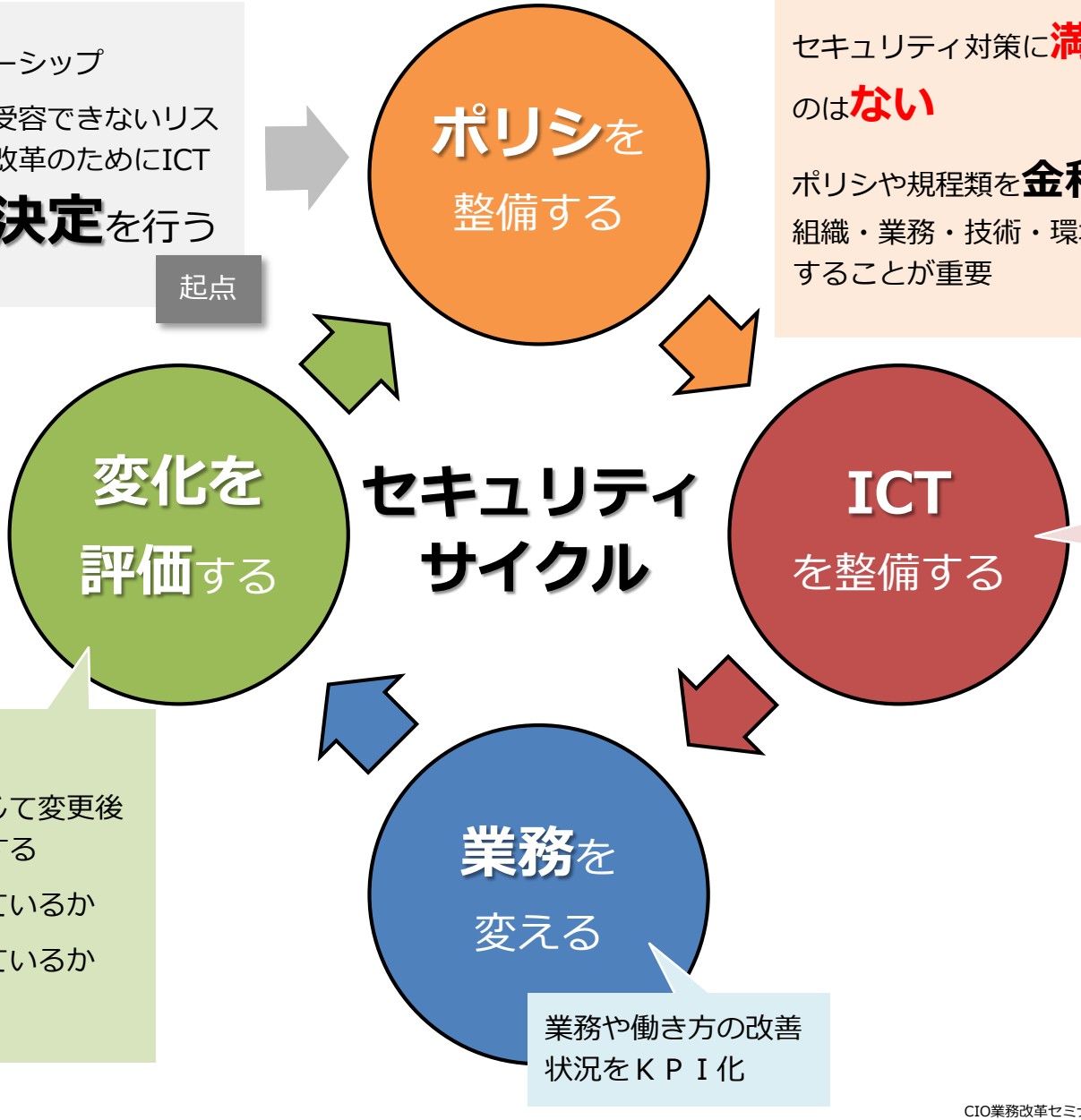
・ベストプラクティスはあくまで参考例であり自社の文化・社風・組織・システムにより対策はかわる

同じ業種・業態だからと言って同じ対策にはならない
例：メガバンクの3行のセキュリティ対策の方策は全く異なっている

経営トップのリーダーシップ

受容できるリスクと受容できないリスクを識別し、働き方改革のためにICTを導入する**意思決定**を行う

起点



セキュリティ対策に**満点の対策**というのは**ない**

ポリシや規程類を**金科玉条とせず**に、組織・業務・技術・環境の変化に柔軟に対応することが重要

クラウド
VDI
AI(人工知能)
など

監査や業務点検を通じて変更後の業務と規程を評価する

規程通りに業務されているか

業務に規程は適合しているか

業務や働き方の改善状況をＫＰＩ化

テレワークで利用できるIT技術

会社がサーバ上に用意した環境で作業を実施

シンクライアント(Thin Client)
VDI(Virtual Desktop Infrastructure)仮想デスクトップインフラストラクチャ)

パソコン

画面表示

表示・入力データの送受信

プログラム実行

データの保存

サーバ

作業は会社貸与/個人のパソコンで実施。データをサーバで共有

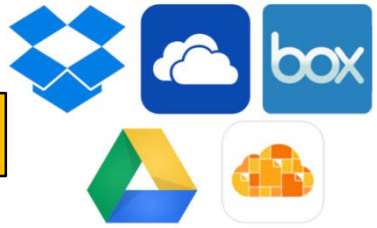
クライアントサーバ型(Client-Server)
クラウドサービス(Cloud) / ASP(Application Service Provider)

パソコン

プログラム実行

インターネット
VPN

データの保存



テレワークで活用するIT技術のセキュリティ対策

VDIにおけるセキュリティ対策

ウィルス対策

１．アンチウィルスストーム

何十台ものクライアントPCで一斉にスキャンが行われた場合、サーバのリソースを大量に消費してパフォーマンスが大きく低下する危険性があり、スキャンを行っていないPCも影響を被ることになる
パターンファイルの配信でも同様の問題があり、ネットワーク負荷が一時的に増大する

２．インスタント・オン・ギャップ

VDI環境では、多数のPCが同じサーバ内に存在する。その中にパターンファイルが古いなどの脆弱なPCが紛れ込んでいれば、他の全てのPCを危険に晒すことになる

３．運用コスト

VDIの環境次第では、定期的にVDI用のマスターイメージのパターン更新を行わなければならず、管理者の負担が増えることになる。パターンファイルの更新で差分ではなくフルパターン更新となるとネットワークの負荷が増大する。

4. 未知の攻撃への対応

仮想環境に対する未知のリスクの情報を収集し、対応が必要となる。物理環境とは異なる対応が必要な場合も発生する。

テレワークで活用するIT技術のセキュリティ対策

クラウドにおけるセキュリティ対策

ネットワークとファイルの暗号化対策

1．クラウドの保管環境の安全性

ファイルが暗号化されていないと、不正アクセスや、操作ミス等でファイルが漏えいした場合に、中身を盗み見られる恐れがある

2．パソコンなどの端末とクラウドシステム間のネットワークの安全性

パソコンとクラウドシステム間のネットワークが暗号化されていなかったり、隠ぺいが実施されていないと、ネットワークの途中でIDやパスワードが盗み見られたり、重要な情報などが盗み取られたりする恐れがある

クラウド会社に預けている資産の保全

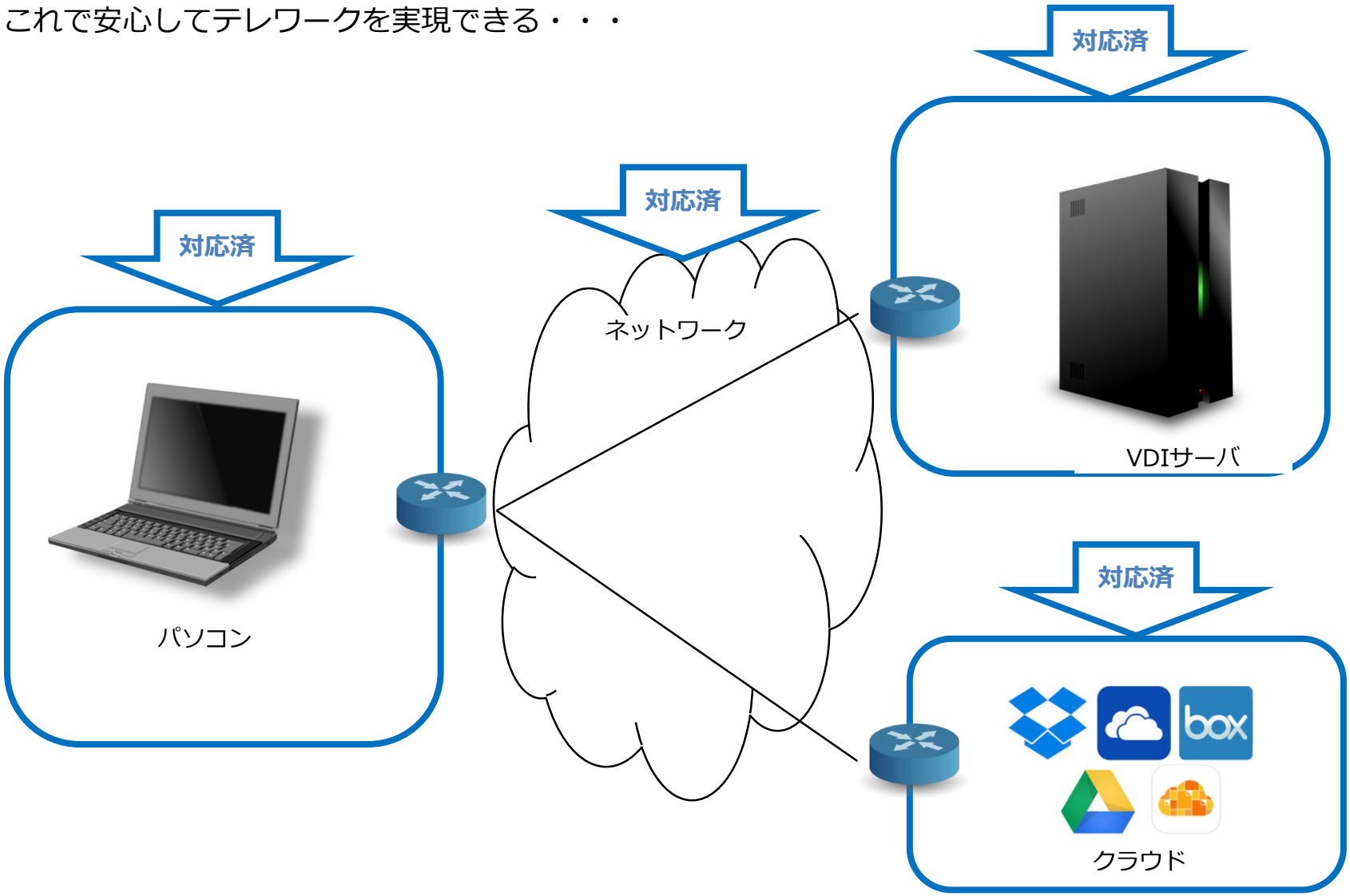
1．事業継続性の対策

データやシステムのバックアップが複数拠点に設置されていないと、一つのクラウドサービスの拠点に障害がある場合に事業が実施できない可能性がある

2．クラウド会社変更時やクラウドサービス終了時の資産保全

利用するクラウド会社を変更する場合や、クラウド会社が倒産等で事業が継続できない場合に、資産が適切に移行できなかったり、廃棄が実施されない恐れがある

パソコンとネットワーク、サーバ・データセンタのセキュリティ対策は適切に実施できた
これで安心してテレワークを実現できる・・・



忘れがちなルータのセキュリティ対策

管理者機能のパスワードがかかっていないorデフォルトのまま

脆弱性が発見されてもファームウェアが更新されていない

資産台帳に乗っていないルータの対策

- システム導入時にきちんと管理していないルータ
- 野良ルータ(WiFi)の対策
- テレワークの利用者側(自宅など)のルータのセキュリティ

ドイツテレコムで被害が発生
発生日時：2016年11月27日
影響：90万顧客
攻撃者：英国在住の29歳
(2017年2月に逮捕)

対策としては・・・

管理用パスワードを変更する

ファームウェアを適切に更新する

セキュリティのかかっていないLANやWifiを利用しない

利用者への教育・訓練

ルータを貸与する

企業側で遠隔管理・・・？

テレワークのみならず、IoTの推進においても課題となっている

セキュリティ対策は予防と対処

すべての事象に対して予防することは難しい(不可能！)
ITにおいても、重要なのは、問題が発生した時に迅速に対応し、被害をできるだけ低減できるようにすること！
そのためにすることは、発見と対処について体系化しておくこと

対処(異常の検知)におけるポイント

- 些細な異常(ヒヤリハット)やセキュリティ事故が発生した時の報告手順を明確にする
  - 異常が異常であるとわかるように、正常の状態の定義をしておく
- KPIとして、起こってしまったことを責めるのではなく、連絡してきたことに感謝する
  - セキュリティ事故の件数で評価するのではなく、セキュリティ事故があった時に規則に従って報告したかどうかの件数で評価する
- 災害に対する訓練や業務の点検に事故対応を含める
  - 日々の業務点検で、正担当者がいない場合でも他の担当者がマニュアルの場所を把握しているかどうか、組織として対応できるかを確認する
- ITシステム部門と業務部門が協力して対処にあたる
  - ITシステム部門と業務部門が日ごろから互いに何をしているかを知る事が重要

最終的には人の問題

ITシステム部門と業務部門の日ごろからのコミュニケーションが重要！

総括

セキュリティ対策は一朝一夕にできるものではありません。

何を守るのか、誰から守るのかによって、採用すべきセキュリティ戦略は異なります100点のセキュリティ対策は残念ながらありません。リスクを認識し、新しいIT技術の動向を常に把握しつつ、社内で発生したセキュリティ事故やヒヤリハットの事象を適切に集めて対応策を検討することが必要です。

また、業務とのバランスも重要です。セキュリティ「原理主義」「至上主義」に陥ってセキュリティ対策を押し付けてはいけません。システム部門と業務部門が敵対関係にならずに、協力してリスクに対応していくことが重要です。

そういう意味ではセキュリティ対策は組織力・人間力・コミュニケーション力・技術力で対応していく課題です。

情報セキュリティ対策とは(再掲)

誰もが感じていると思うが、どんな組織でも情報セキュリティ対策の実施は本当に難しい。なぜこれほど難しいのか。答は簡単だ。情報セキュリティ対策では、かなり複雑な問題を合理的に解く必要があるからだ。

情報システムは、もはや組織の基盤である。しかし、基盤化してしまったが故に、情報セキュリティ対策では、考慮しなければならない事項が多く、事項同士が相互依存しており、組織毎に考慮すべき事項の構成が変わり、かつ、事項の内容も変化しうるものであることを考慮しなければならない。この結果、それぞれの組織が、情報セキュリティの問題を主体的に理解し、その解決方法を考え出すプロセスを設計し、常に変化に対応できるメカニズムを構築しなければならないことになる。しっかりした体制を作り、経営層の巻き込みを行い、技術、財務、法令、運用、教育、組織統治に関わる面倒な作業をこなしていかなければならない。

最後に・・・

人城を頼らば城人を捨てる

- 織田信長 -

人は城、人は石垣、人は堀、情けは味方、仇は敵なり

- 武田信玄 -

ご清聴、ありがとうございました。

当資料に関する、お問い合わせやご質問等がございましたら
下記までご連絡ください。

Simple Consulting

ＣＩＯパートナーズ株式会社

〒550-0014
大阪市西区北堀江 1-19-8　四ツ橋ＫＭビル ７階

（担当：吉田）

TEL 06-6599-8661

✉ office@cio-partners.co.jp