もしも社長が
セキュリティ対策を
聞いてきたら

日本マイクロソフト株式会社
マイクロソフトテクノロジーセンター
セキュリティアーキテクト
筑波大学非常勤講師
公認情報セキュリティ監査人
CISSP
蔵本 雄一

Microsoft

蔵本 プロフィール

【これまでの活動内容】
ウイルス対策ソフトの開発、侵入テスト、セキュリティ監査、
Windows 等の製品担当、セミナー講師等

【保持資格等】
筑波大学非常勤講師、公認情報セキュリティ監査人
CISSP、日本CISO協会主任研究員

【著書】
もしも社長がセキュリティ対策を聞いてきたら (日経BP社)
全国の書店で発売中

【Hackademy (セキュリティ教育)】
Hackademy で検索
https://www.udemy.com/hack-defence-basic/

現在の問題点

現在の問題点

経営層と IT エンジニアの会話/認識のプロトコルが合わない

プロトコルを合わせるためのお互いの歩み寄りが重要
特に IT エンジニア側からのアプローチが重要

タクシー乗車時の例

「○○通りを右折して△△交差点でよいでしょうか。」

道に明るい場合は正確に伝わるが、そうでない場合は
ランドマーク等、分かりやすい目印等で伝える必要がある。

よくある勘違い

「プロトコルを合わせる」事が重要

簡単な言葉を使えば良いというものではない。
経営やマーケティング等ビジネスインパクトを
意識したコミュニケーションが重要

経営層がすべき事

経営層が最低限すべきこと

IT / セキュリティ等用語の理解

PEST 分析等を利用した、IT の戦略的な活用

組織構成

リスクの認識

IT エンジニアがすべき事

IT エンジニアが特に注力すべきこと

ビジネスインパクトへの変換

リスクやITの見える化

ビジネスインパクトへの変換

～経営層への説明～

経営層への説明 (NGパターン)

この対策をしないとウイルスに感染してしまいます。
この対策をしないとハッキングされていまいます。

ビジネスへの影響が分からないため、
このままでは投資の意思決定材料としては活用不可

経営層への説明 (OK パターン)

この対策に投資しないと情報漏洩が発生する恐れがあります。
過去、4億円の損失になった企業が存在します。

投資の判断材料として活用可能

BATNA の観点から見た多層防御

※ BATNA = Best Alternative to a Negotiated Agreement

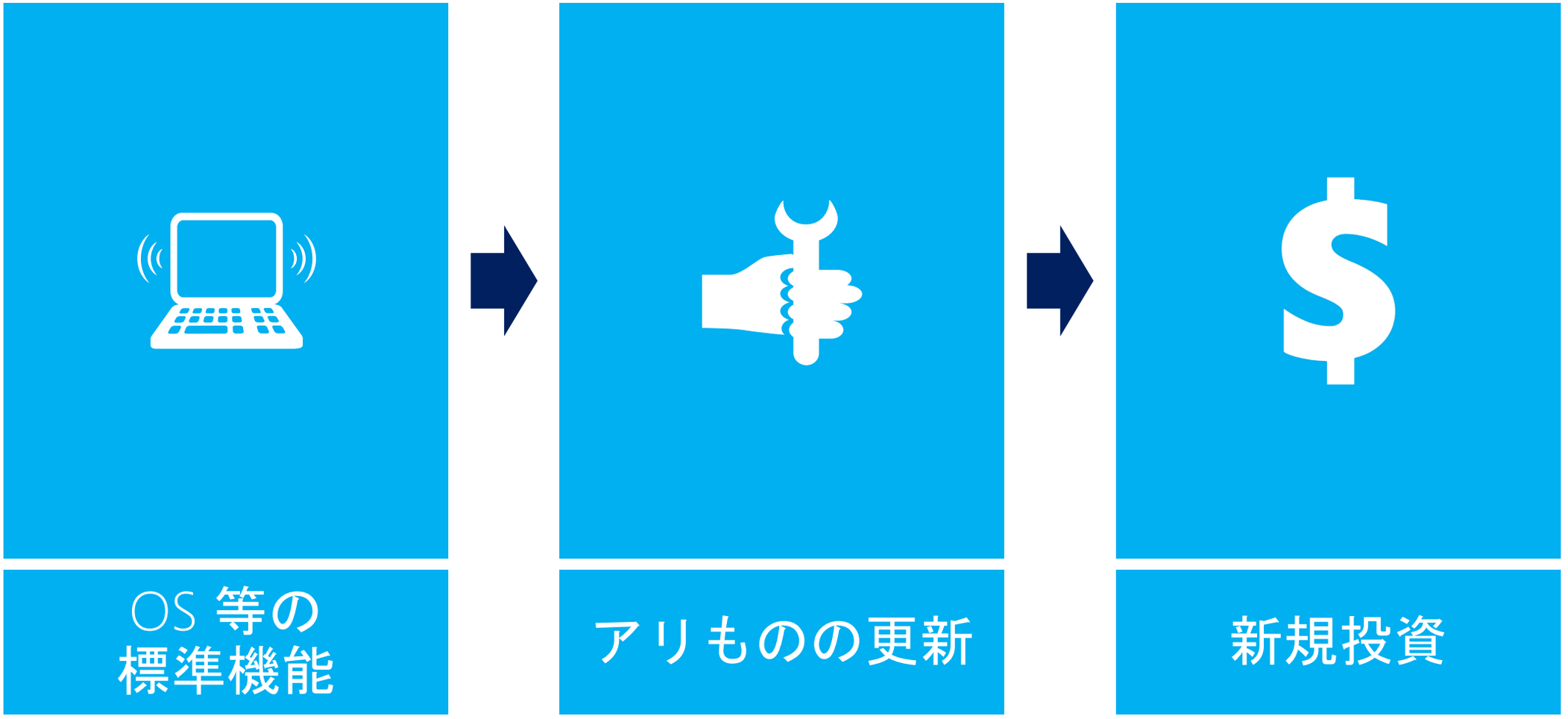
多層で防御しているから安全です。

多層で防御しているため、仮に防御 1 が破られたとしても
防御 2 が、防御 2 が破られたとしても防御 3 があるため安全です。

NIST SP 800 -61

準備	やられないようにする	防御力向上
検知・分析	やられている事を すぐに検知する	検知分析
根絶・復旧・ 封じ込め	やられても被害を 小さくする	被害軽減
事件発生後の 対応	やられた後でも、 情報を保護する	事後対応

投資の必要性



ドラッカー 4 つのコスト

生産的コスト：
利益や売り上げなどの直接的な経済価値を生み出し、
経済活動に貢献するコスト (生産、販売、営業など)

補助的コスト：
直接的な経済価値を生み出すわけではないが、
企業運用上不可欠と判断されるコスト (人事や経理など)

監視的コスト：
顧客や自社にとって悪いことが起こらないようにするコスト
(取引先の信用調査、警備員など)

浪費的コスト：
顧客や自社にとって全く貢献しないコスト (休眠在庫など)

ドラッカー 4 つのリスク

負うべきリスク：
事業の本質に付随するリスク

負えるリスク：
選択肢の可能性としてリスクテイク可能なリスク

負えないリスク：
チャレンジして失敗すると、経営に対して大きなダメージとなり、
事業そのものに影響が出てしまう恐れのあるリスク

リスクを負わないリスク：
負うべきリスクを負わなかった際に発生するリスク

ビジネスインパクトへの変換

～思考のパターン～

思考のパターン

危険だから禁止

どうすれば安全に利用できるのか？を提案

思考のパターン例１

危険だから車への乗車は禁止

シートベルトとエアバッグを装備することで安全に走行可能

思考のパターン例 2

ふぐは危険だから食べない

毒を取り除いて食べる

IT や リスクの見える化

～IT の見える化～

効果の見える化

システム名	機能	直接効果	間接効果	金額的効果
IT基板	テレワーク	社外から社内ネットワーク接続可能	在宅勤務、外出先からのテレワーク	
Web会議システム	映像と音声のネットワーク共有	遠隔地のユーザー同士によるリアルタイムな情報共有	遠隔地との打ち合わせ	毎月100万円の出張費用を削減
盗難紛失対策	HDD の暗号化	第三者から HDD の読み取り防止	安全なテレワーク	

DAGMAR 理論の応用 (それぞれの達成度を測定)

未知：まだ知られていない状態
認知：存在を認知
理解：スペックや性能を理解
確信：良いモノだと確信
行動：購買へ至る

未知：ルールがまだ知られていない状態
認知：ルールの存在を認知
理解：ルールの内容を理解
確信：ルールの重要性や自身の戒めとして有効であることを確信
行動：ルールを順守

コンジョイント分析の応用

対策	ソリューション	特長
ウイルス対策	A社製品	検出率：X機関のテストでは検出率98% IT基板統合：統合不可 管理工数：0.5人月→1人月に増加 ライセンス費用：1年2000円/1ユーザー
	B社製品	検出率：X機関のテストでは検出率92% IT基板統合：統合可能 管理工数：0.5人月→0.2人月に減少 ライセンス費用：1年600円/1ユーザー
出口対策	A社製品	提供形態：アプライアンス レポート：専用管理ツールによるレポート閲覧が可能 ライセンス費用：専用ハードウェア100万円 使用ライセンス 600円/1ユーザー 認証ユーザー：現在利用中のユーザーIDとの連携が可能
	導入済プロキシの利用	提供形態：既に導入済のプロキシサーバーの設定を変更 レポート：別途開発の必要あり ライセンス費用：追加費用不要 認証ユーザー：認証するユーザーIDは別途作成する必要あり

ペイオフマトリクスの応用

ＱＷ：遂行が容易だが、得られる効果も少ない領域
ＴＷ：遂行が困難なうえに得られる効果が少なく、
「時間のムダ」と呼ばれる領域
ＢＯ：遂行が容易でかつ得られる効果も大きいため、
優先して取り組むべき領域
ＳＥ：遂行が困難だが、得られる効果が大きいため無視はできない領域

購買プロセスの 5 段階モデル

問題意識	情報探索	代替製品の評価	購買決定	購買後の行動
ニーズを引き起こす	ニーズを満たす製品（方法）を調査する	ニーズを満たす製品（方法）を比較する	他人の評価などを参考に購入を決める	自身の判断が正しいかどうかを検証する
リスクを明確にする	リスクの対応策を調査する	列挙した対応策を検討する	他社の評価や事例等を参考に購入を決める	リスクを解決できているかどうかを継続してモニタリングする

IT や リスクの見える化
～リスクの見える化～

FMEA (故障モードと影響解析)

構成要素へ分解（ワークシートを作成）
リスク優先度を算出

FMEA (故障モードと影響解析)

FMEA (故障モードと影響解析)

リスク優先度 = 発生頻度 x 影響度 x 防御困難度

各パラメーターの定義例

点数	発生頻度	影響度	防御困難度
4	年に複数回以上	基幹業務停止や機密情報の漏洩など。 被害は致命的	防御不可能
3	年に1回程度	大多数の端末利用不可、 重要度の高い情報流出 など。被害は甚大	防御は難しい
2	過去に発生事例はないが、 将来発生する可能性がある	少数の端末利用不可、 重要度の低い情報流出 など。被害は軽微	容易に防御できる
1	過去に発生事例はなく、 将来発生する可能性もない	影響はない	確実に防御できる

セキュリティ対策の最大公約数を考える

セキュリティ対策の最大公約数を考える

PEST 分析 (外部環境要因分析)

Political (政治的要因)	Economy (経済的要因)	Society (社会的要因)	Technology (技術的要因)
			
マイナンバー 対策		ワークスタイル変革 サイバー攻撃対策	

PEST 分析 (ワークスタイル変革)

Political (政治的要因)	Economy (経済的要因)	Society (社会的要因)	Technology (技術的要因)
			
マイナンバー対策		ワークスタイル変革	
		サイバー攻撃対策	

これまでのセキュリティ

境界領域 (インターネットとイントラネットの境目)
で防御

社外にデータや端末が
出ないように保護

デバイス

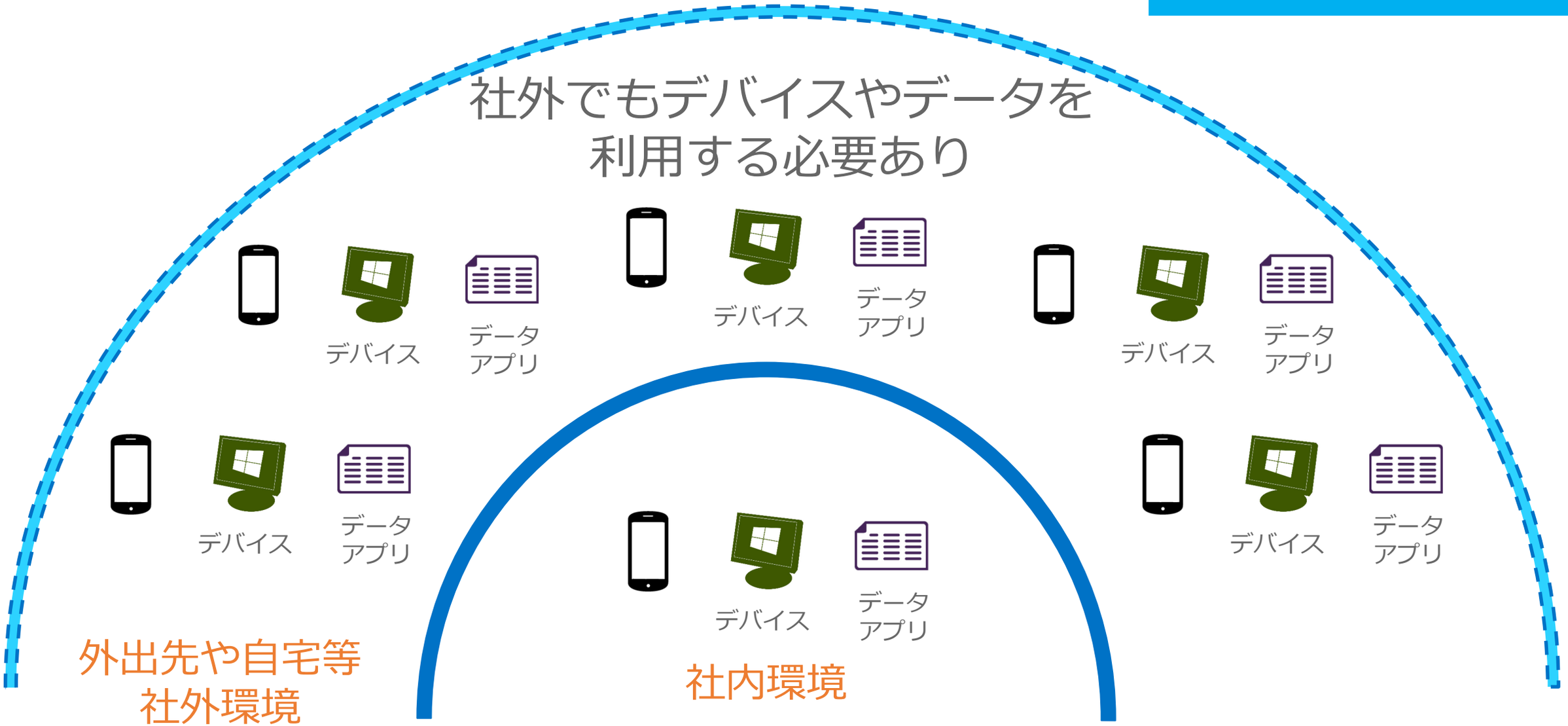
データ
アプリ

社内環境

外出先や自宅等
社外環境

これからのセキュリティ

境界領域の防御がないため、
クライアントやデータ自身の
セキュリティ対策が必須



PEST 分析 (サイバー攻撃)

Political (政治的要因)	Economy (経済的要因)	Society (社会的要因)	Technology (技術的要因)
			
マイナンバー 対策		ワークスタイル変革	
		サイバー攻撃対策	

サイバー攻撃の流れ
～将を射んとする者はまず馬を射よ～

ワークスタイル変革と同様に
クライアントやデータ自身の
セキュリティ対策が必須

メール

悪意あるメール
から保護

クライアント
（馬）

狙われる
クライアントを保護

サーバー上の機密
ファイル
(将)

ファイルへの
不正アクセスから
保護

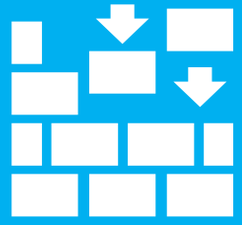
PEST 分析 (マイナンバー)

Political (政治的要因)	Economy (経済的要因)	Society (社会的要因)	Technology (技術的要因)
			
マイナンバー 対策		ワークスタイル変革 サイバー攻撃対策	

マイナンバー (法的な対応)

組織的
安全管理措置

人的
安全管理措置



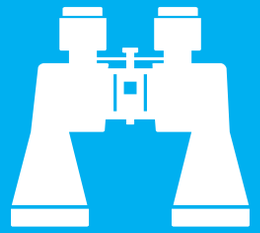
物理的
安全管理措置

技術的
安全管理措置

技術的安全管理措置

ワークスタイル変革と同様に
クライアントやデータ自身の
セキュリティ対策が必須

アクセス制御



アクセス者の
識別と認識

外部からの不正
アクセス等の防止

情報漏えい等の
防止

まとめ

現在の問題点

経営層と IT エンジニアの会話/認識のプロトコルが合わない

プロトコルを合わせるためのお互いの歩み寄りが重要
特に IT エンジニア側からのアプローチが重要

経営層が最低限すべきこと

IT / セキュリティ等用語の理解

PEST 分析等を利用した、IT の戦略的な活用

組織構成

リスクの認識

IT エンジニアが特に注力すべきこと

ビジネスインパクトへの変換

リスクやITの見える化

Microsoft