KPMG

クラウド型コラボレーションツールの導入・運用に関するセキュリティ・費用試算

セキュリティポリシー見直しによる低コスト導入







Executive Summary

近年、Office 365やG Suiteといったクラウド型コラボレーションツールの導入により場所や時間に縛られない柔軟な働き方を推奨し、生産性を高め、労働時間を削減する働き方改革を推進する企業が出てきています。一方で、クラウド型コラボレーションツールの導入に伴う通信量の増加に合わせてネットワーク・機器を増強することで、コストが増大することを懸念する企業も見られます。

クラウド型コラボレーションツールには、各種セキュリティ機能を有しているツールもあり、既存のセキュリティポリシーを見直してこれらの機能を有効活用することで、導入・維持にかかるコストを抑えられる可能性があります。そこで、本ホワイトペーパーでは、「既存のセキュリティポリシーのままネットワーク・機器を増強したモデル」と「セキュリティポリシーを見直しツールのセキュリティ機能を有効活用したモデル」について、各種前提を設定し、セキュリティのレベルと導入・維持のコストを算出して比較しました。

今回設定した前提では、「既存セキュリティポリシーモデル」と「セキュリティポリシー見直しモデル」のセキュリティレベルは同等となり、導入・維持コストはセキュリティポリシー見直しモデルの方が約50%削減できることが判明しました。

現在のネットワーク構成等により各モデルのセキュリティレベルや導入・維持コストは異なりますが、クラウド型コラボレーションツールの導入を検討されている企業におかれては、既存のセキュリティポリシーを見直して、ツールのセキュリティ機能を最大限活用するという選択肢を検討されることをお勧めします。

Contents

1 クラウド型コラボレーションツール導入の効果と課題

クラウド型コラボレーションツール導入の効果

少子高齢化に伴う生産年齢人口の減少により、長時間労働の是正、女性・高齢者の活躍推進といった働き方改革が企業に求められています。企業によっては、日々の業務をオフィス以外の場所で行うことができるよう、「いつでも」「どこでも」業務を遂行できる環境の整備を進めています。特に、自由なコミュニケーション、手軽な情報共有を推し進めることができるOffice 365やG Suiteといった「クラウド型コラボレーションツール」が注目を集めています。

クラウド型コラボレーションツールを利用することで、社内だけでなく社外においても、スマートフォンやタブレット等の様々なデバイスを利用して業務を行うことができ、効率的な業務遂行が可能となります。例えば、外出先でスマートフォンを利用してメールを確認することで、オフィスに戻る必要がなくなる、テレビ会議ツールを活用することで、無駄な出張がなくなるなどの効果が生じます。

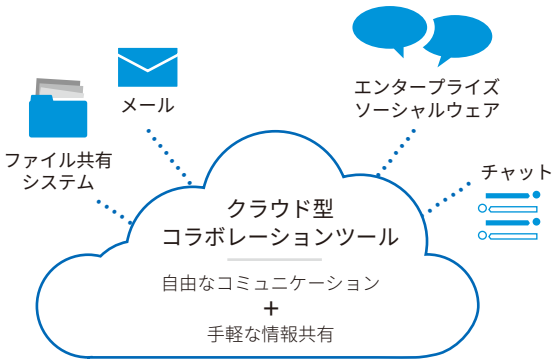
クラウド型コラボレーションツール導入の課題

クラウド型コラボレーションツールを導入すると、テレビ会議ツールの利用などにより、社外のクラウドサービスとのデータ通信量が増加することが一般的です。導入検討する場合は、インターネット通信のデータ量増を考慮して、ネットワーク構成の見直しを行う必要があります。

社外からのサイバー攻撃を防ぐため、ほとんどの企業ではネットワーク境界への対策を定めたセキュリティポリシーを整備しており、社内外の通信にはファイアウォールやプロキシを通すことなどを定めています。しかし、既存のセキュリティポリシーを維持したまま、データ通信量の増加に合わせてプロキシやファイアウォールといったネットワーク・機器を現状構成のまま増強してしまうと、セキュリティは維持できますが大幅なコスト増となることが想定されます。

クラウド型コラボレーションツールには、各種セキュリティ機能を有しているツールもあり、導入の際に、既存のセキュリティポリシーを見直してこれらの機能を有効活用すれば、コストを抑えられる可能性があります。

1 クラウド型コラボレーションツール概要



2 「いつでもどこでも」働ける環境

場所を選ばない
日常業務を外出先や自宅などでおこなう

移動時間を活用
出張の際の移動時間も携帯やタブレットを活用

オンラインでのコミュニケーション
取引先や社内の会議はオンライン会議にするなど

2 ツールのセキュリティ機能を有効活用することで得られる効果の検証 （Office 365に基づく試算）

セキュリティおよびコストを比較検討した2つのモデル

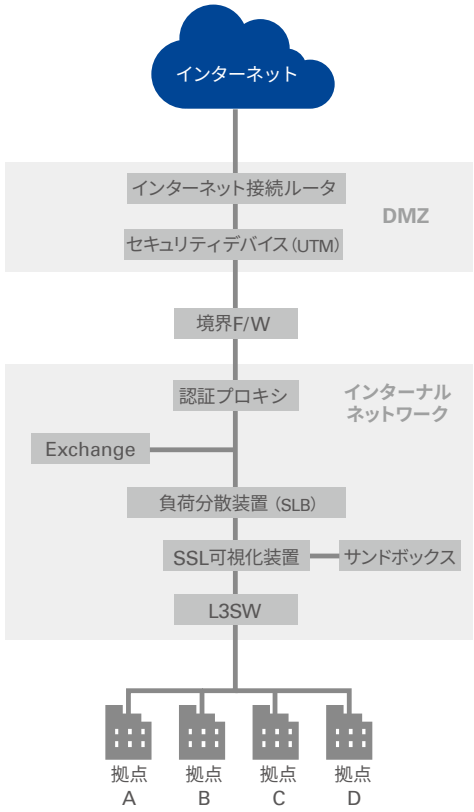
クラウド型コラボレーションツールのセキュリティ機能を有効活用することで、どの程度の効果が得られるのか、「既存のセキュリティポリシーのままネットワーク・機器を増強したモデル」と「セキュリティポリシーを見直しツールのセキュリティ機能を有効活用したモデル」について、セキュリティのレベルと導入・維持のコストを算出して比較しました。

なお、比較にあたっての前提条件、導入前のネットワーク構成は下記としました。

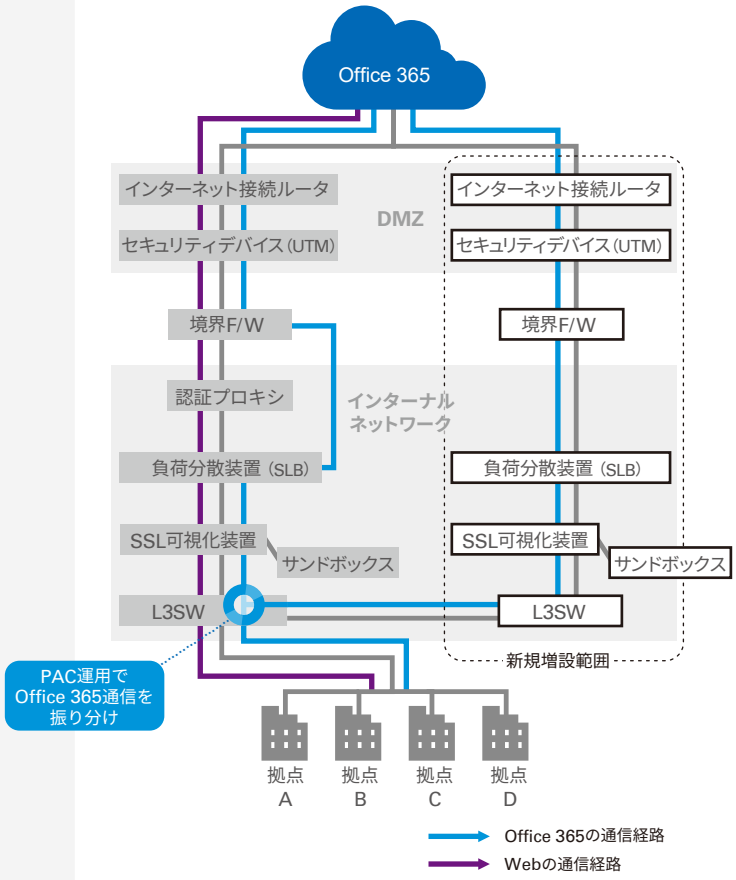
比較にあたっての前提条件

クラウド型コラボレーションツール	Office 365 Outlook、OneDrive、Teams、Forms、SharePoint 等の利用を想定
想定利用ユーザ数	3 万人
想定拠点数	4 拠点
想定通信データ量	1Gbpsから2Gbpsに増加

Before 導入前のネットワーク構成



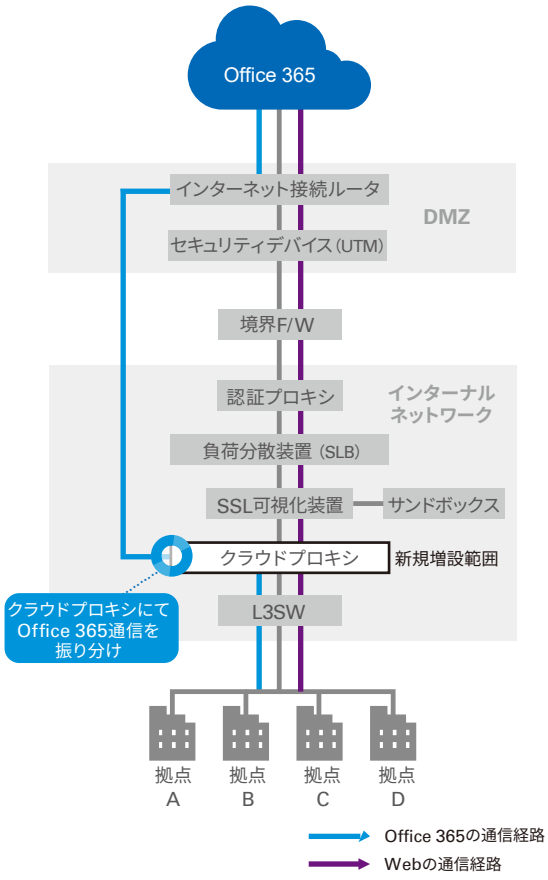
model 1 既存のセキュリティポリシーのまま ネットワーク・機器を増強したモデル



既存のセキュリティポリシーを変更しないため、通信データ量の倍増に合わせて、既存のネットワークと同様の機器を1セット追加する想定としました。Web通信については、全拠点共通で既存ネットワークを経由することとし、Office 365通信については、2拠点は既存ネットワークを経由し、残りの2拠点は新たに設置したネットワークを経由することとしました。

本モデルを実現するために、エンドユーザが利用するPCのPACファイルでOffice365通信を振り分ける必要があります。そのため、クラウド側のネットワーク環境の変更がある度にPACファイルの設定を変更するという手動の運用を必要とするため、運用負荷が非常に高いモデルとなりました。

model 2 セキュリティポリシーを見直しツールの セキュリティ機能を有効活用したモデル



ウィルスチェックやスパムチェック等のメールセキュリティ対策については、Office 365の機能を用いて実現することとし、既存ネットワークにクラウドプロキシを設置することでUTM、境界F/W等の既存のセキュリティ対策をバイパスする想定としました。また、クラウドプロキシがOffice 365通信とその他の通信を振り分けることとしました。

本モデルでは、クラウドプロキシが自動で生成する設定ファイルに基づき通信の振り分けを行うことで、「既存セキュリティポリシーモデル」とは異なって自動の運用となるため、運用負荷はほとんど増えません。

3 両モデルにおけるセキュリティレベルの比較

KPMGが策定した「KPMGサイバーセキュリティ対策態勢アセスメントフレームワーク」に基づき、両モデルのセキュリティレベルを分析しました。当該フレームワークは、KPMGが持つ知見・経験をもとにして、NIST[1]、NISC[2]が発行したセキュリティアセスメントガイドラインの要素を盛り込んでサイバー攻撃のステップ毎に策定したものです。当該フレームワークを採用することにより、図3に示す近年のサイバー攻撃の動向を考慮することができます。

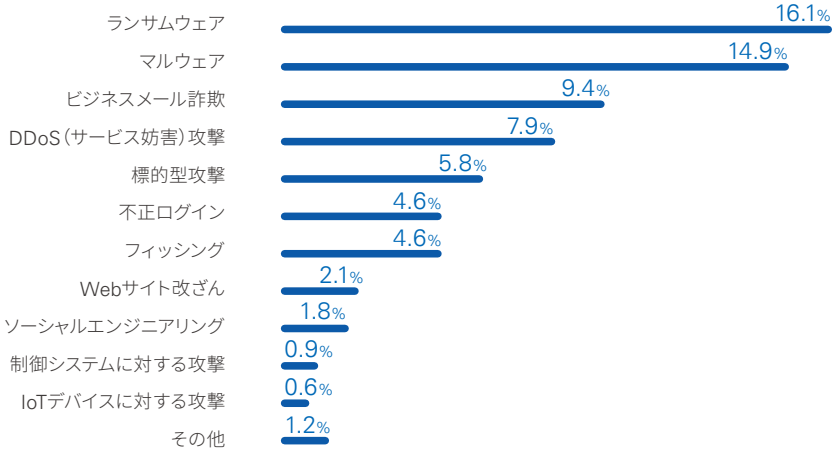
1 米国国立標準技術研究所（NIST）「Cybersecurity Framework」 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

2 内閣サイバーセキュリティセンター（NISC）「高度サイバー攻撃対処のためのリスク評価等のガイドライン」 https://www.nisc.go.jp/active/general/risk.html

3 サイバー攻撃の7つのステップ

step 1 偵察＆武装	ウェブ、SNSや公開情報を基に標的組織の情報を探る。 侵入プロセスを開発し、マルウェアをカスタマイズする。
step 2 侵 入	マルウェアや、悪意のサイトのURLをリンクしてメール。 悪意のサイト経由で攻撃コードを実行し、マルウェアをダウンロードさせる。
step 3 誘 導	標的型メールや正規のサイトを改ざんし、悪意のサイトに誘導する。
step 4 潜 伏	マルウェアをインストールし、端末の権限を掌握する。
step 5 指 令	リモートの指令サーバから、攻撃のための指示（コマンド）を 受け取るためのバックドアを開設する。
step 6 探 索	他の端末に感染を拡大させ、標的組織のネットワーク内で機密情報を探索する。
step 7 達 成	発見した機密情報を外部へアップロードし、攻撃の形跡を消去する。

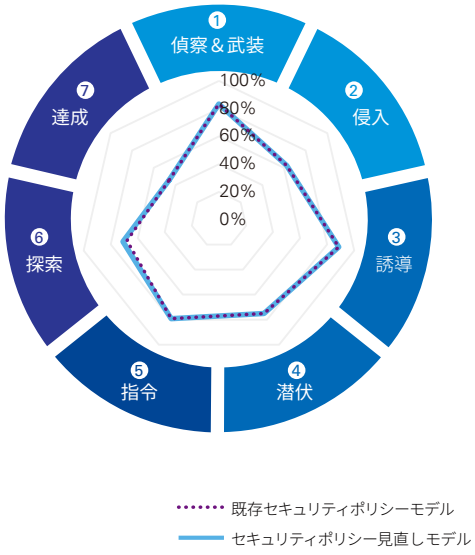
4 近年のサイバー攻撃の動向



Source：KPMG,「サイバーセキュリティサーベイ2018」

両モデルを「KPMGサイバーセキュリティ対策態勢アセスメントフレームワーク」に当てはめ7つのステップごとに点数付けを行い、比較しました。その結果、Office 365のセキュリティ機能を最大限に活用することで、一部の機器がなくともセキュリティレベルの維持が可能であり、「既存セキュリティポリシーモデル」と「セキュリティポリシー見直しモデル」のセキュリティレベルは同等で差異が無いことが分かりました。Office 365の機能として、DHA攻撃対策、脆弱性スキャン、マルウェア対策等があり、これらの有効活用により一部の機器類がなくともセキュリティレベルを維持することが可能です。

5 セキュリティアセスメント結果



4 両モデルにおける導入・維持コストの比較

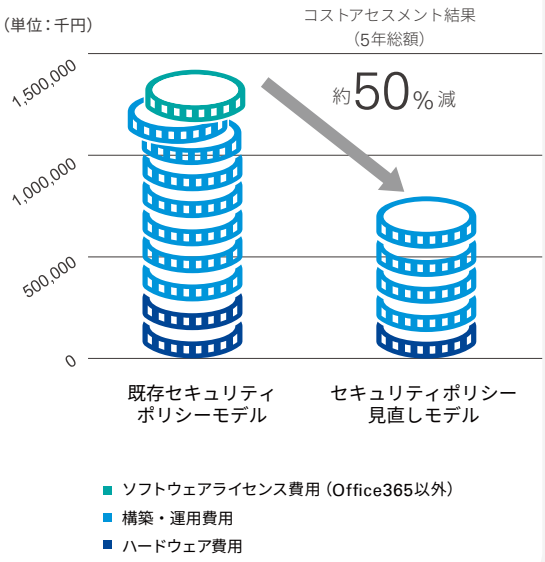
両モデルの導入・維持コストについて、図6の各項目の5年間のコストを算出した結果は図７のとおりです。なお、両モデルに必要なOffice 365のライセンス費用は同額であるため、当該コストは除外しました。

前提条件に従い、両モデルの導入・維持コスト（5年総額）を算出した結果、「セキュリティポリシー見直しモデル」は「既存セキュリティポリシーモデル」よりも、ハードウェア、構築・運用、ソフトウェアライセンスの全ての項目についてコストが下回り、およそ半額で導入・維持できることが分かりました。

6 コストアセスメントの検討

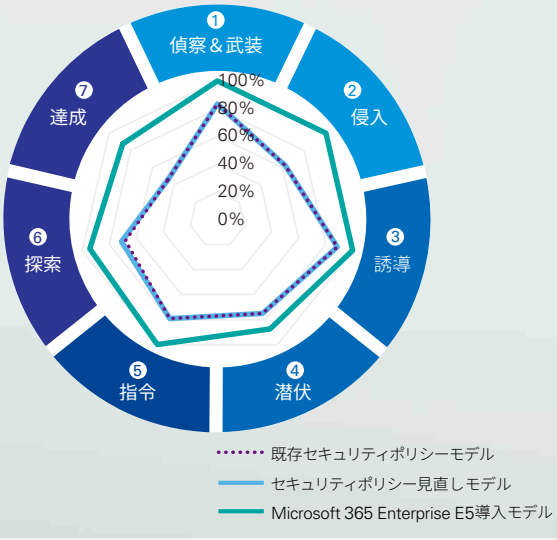
大分類	中分類	備考
ハードウェア	初期費	ネットワーク機器の初期費（F/W、プロキシ等）
	保守費	ネットワーク機器の保守費（5年総額）
構築・運用	初期費	ネットワーク機器の設置等のSI費、運用体制の構築費
	保守費	システム維持・運用費（5年総額）
ソフトウェアライセンス		クラウド型コラボレーションツールやセキュリティツールのライセンス費（5年総額）

7 両モデルのコスト比較結果



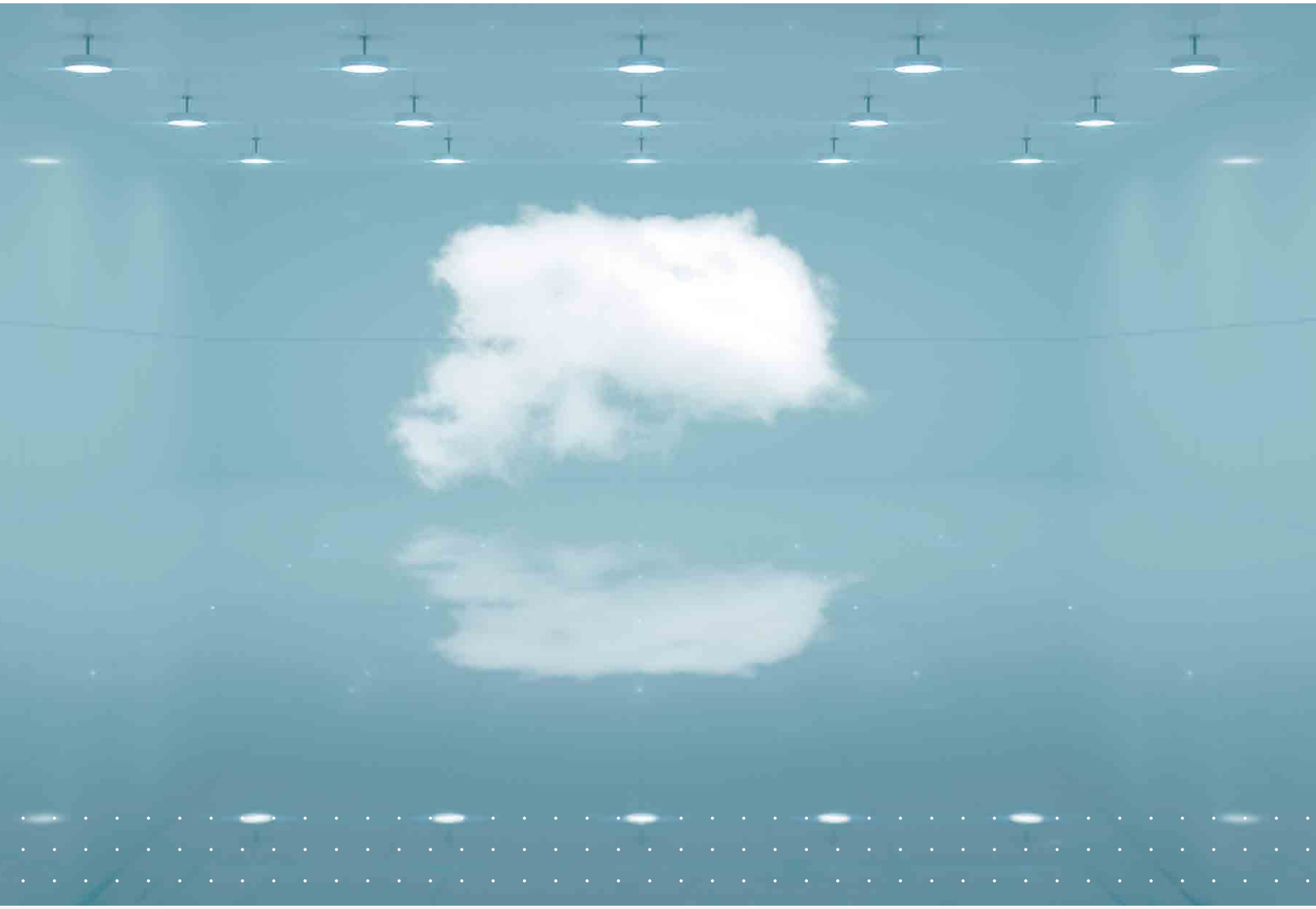
【参考】Microsoft 365導入による更なるセキュリティ向上

参考として、「セキュリティポリシー見直しモデル」において、Microsoft 365 Enterprise E5を導入した場合のセキュリティレベルを分析しました。
「Office 365 Threat Intelligence」「Windows Defender Advanced Threat Protection (ATP)」「Azure Information Protection」等の活用により、大幅なセキュリティレベルの向上を見込めることが判明しました。



8 **セキュリティアセスメント結果**
(Microsoft 365 Enterprise E5導入後)

5 KPMGによる クラウド型コラボレーションツール導入支援



クラウド型コラボレーションツールを働き方改革に役立てようとする企業が増えつつありますが、2章で比較したモデルのように、導入の仕方によって導入・維持コストは大きく変わります。2章で例示したセキュリティポリシー見直しモデルだけでなく、特定のクラウドサービスの通信をデータセンター経由とせず、拠点から直接インターネット環境へ通信させるローカルブレイクアウトのモデルなどもあり、ツール導入にあたっては、現在のネットワーク構成等に基づき柔軟に比較検討を行うことが必要です。

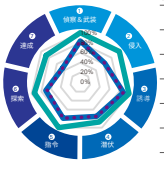
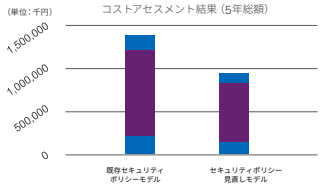
KPMGでは、ネットワーク・セキュリティにかかる豊富なナレッジ、多数の支援実績に基づき、セキュリティレベルを高く維持した上での、コスト効果の高いクラウド型コラボレーションツールの導入を支援します。

既存の環境やセキュリティポリシーを見直し、豊富な実績に基づいた最適な導入モデルを選定することで、導入・維持コストを大幅に削減できる可能性があります。クラウド型コラボレーションツールの導入にあたっては、貴社に最適な導入モデルを分析・評価する「クイックアセスメント」の実施をお勧めします。

9 KPMGが提供する クラウド型コラボレーションツール導入支援サービス

	Phase1 クイックアセスメント	Phase2 あるべき姿のデザイン	Phase3 ロードマップ策定	Phase4 導入支援
目的	既存環境を整理し、クラウド型コラボレーションツール導入の可否・コスト削減効果を分析	セキュリティ面・コスト面から貴社に合ったあるべき姿をデザイン	中長期的な目標と、短期的な目標を達成するための具体的な計画を策定	プロジェクトを円滑かつ確実に実行するための支援を実施
作業内容	社内の現行システムに関するセキュリティ対策を整理して可視化し、コスト・セキュリティの観点で評価	インフラ構成、運用体制の理想像を描き、それらを実現するための施策とその効果を提案し、実行有無の意思決定を促す	各種施策の優先度を設定し、実行する順序、期間、体制を検討	各施策に係るプロジェクト全体のスケジュールやステークホルダーの管理・調達を支援

10 クイックアセスメントの概要

アセスメント観点	アセスメント概要	アウトプットイメージ
セキュリティ	以下の観点でセキュリティレベルを評価 ■ 最新のサイバー攻撃への対応 ■ 未知の攻撃への予測的対応 ■ 既存のセキュリティ対策ツールが担保するセキュリティ ■ 新たなセキュリティ対策ツールが担保するセキュリティ	
コスト	以下の観点でコストを比較 ■ 既存のセキュリティ対策ツールを利用し続けた場合に今後発生する運用コスト ■ 新たなセキュリティ対策ツールを新規に導入し、全社展開した際に発生する初期コスト+運用コスト	

アセスメント領域	既存のセキュリティ	新たなセキュリティ
偵察＆武装	High	High
侵入	Middle	High
誘導	High	High
潜伏	High	High
指令	High	High
探索	Middle	High
達成	Low	High

Contact us

KPMGコンサルティング株式会社

T:03-3548-5111
E:kc@jp.kpmg.com

kpmg.com/jp/kc