SB Technology

導入事例

株式会社NHKテクノロジーズ

導入サービス
- Microsoft 365 導入・運用支援サービス
- MSS for Microsoft 365
- MSS for EDR

プロフィール

所在地	東京都渋谷区神山町4-14 第三共同ビル
設立	1969年7月23日
従業員数	約2,000名
事業概要	・放送番組等の制作から送出、送信、配信、受信に係わる技術業務 ・番組制作設備や放送設備、共同受信施設等の設備整備および保守 ・コンピュータや情報通信、情報セキュリティに係わるシステム・ソフトウェア開発、サービス提供 等
URL	https://www.nhk-tech.co.jp/

株式会社NHKテクノロジーズ
取締役
ファシリティ技術本部
情報システムセンター長
長村 中 氏

株式会社NHKテクノロジーズ
経営企画室
IT企画部
穂積 律宇 氏

「Microsoft 365 E5・MSS 導入により、複雑化するサイバー攻撃から自社を守るゼロトラストとインシデントレスポンス強化を実現しました」

導入のポイント

- 巧妙化するサイバー攻撃を多層的に防御し『ゼロトラスト』を実現
- セキュリティ人材不足を解消、ユーザー対応に注力できる体制を実現
- セキュリティと働きやすさを両立できる環境を構築

NHKテクノロジーズは、2019年4月、NHKアイテックと NHKメディアテクノロジーの統合により放送・メディアの総合技術会社として発足した。同社は、番組制作、放送設備や情報システムの開発整備、その保守運用に至るまで、放送に関わる技術業務の全領域を担っている。

今回社内の情報システムを統括する IT企画部では、事業継続の観点からサイバー攻撃対策を進化させるため、Microsoft 365 E5 およびセキュリティの監視サービスであるマネージドセキュリティサービス（以下、MSS）を SBT の支援を受け、導入した。

Office 365 脅威可視化アセスメントによりリスクを可視化

2015年にサイバーセキュリティ基本法が施行され、サイバーセキュリティへの脅威に対し、国、地方公共団体、重要社会基盤事業者およびサイバー関連事業者が連携し対応する方針が示された。内閣サイバーセキュリティセンター（NISC）が定める、重要インフラグループに定められた14分野のうち「情報通信」に、親会社である NHK の「放送事業者」が該当しており、NHKテクノロジーズにおいてはセキュリティ強化への積極的な対応が不可欠となっていた。

同社は、これまでウイルス対策・メールのセキュリティ対策・UTM の設置などさまざまなセキュリティ対策を施してきたが、社外で業務にあたる社員も多いため、社内利用に限定しないさらなるセキュリティ強化が必要だと考えていた。加えて、2020年に東京で開催される国際的なスポーツイベントにより、サイバー攻撃が増し、セキュリティのリスクが高まるという懸念も抱いていた。それは過去にロンドンや北京においてセキュリティ事案が多く発生していたという前例があるためであった。

こうした背景から、同社は、マイクロソフト社が実施する「脅威可視化アセスメント」により、自社がどのようなサイバー攻撃を受けているのか、現状の対策がどのレベルにあるのかを可視化することにした。自社の Office 365 テナントを利用し、1か月間のアセスメントを実施したが、処理の遅延などユーザー影響もなく、社員でアセスメントの実施に気づいているものはいなかったのではないかと言う。

「アセスメントの結果を見て驚きました。亜種も含めどのようなマルウェアの攻撃を受けたのか、ID の不正利用などどういった侵害があったのかが正確に可視化されたのです。サイバー攻撃が複雑化・巧妙化していることは話に聞いて認識していましたが、この結果を受け、早急に次世代のセキュリティ対策を打つ必要があると感じました」（穂積氏）

こうして複雑化・巧妙化するサイバー攻撃に対し、社内外のセキュリティを包括的に担保できるセキュリティ対策を施す決断をした。

ゼロトラストを最も迅速に実現できる Microsoft 365 E5 の導入を決定

次世代のセキュリティ対策を検討するにあたり、『ゼロトラスト』というセキュリティモデルを採用し、その概念を具体化できるサービスの選定を開始した。

『ゼロトラスト』とは、「全てを信じない」という前提で設計されるネットワーク構成である。これまで“社内は安全”であるという前提に立ち、社内と社外の境界を守ってきた。しかし、働き方の変化もあり、社外からの接続が増え、またさまざまなデバイスから社内に接続されるようになり、境界のセキュリティ対策だけでは意味をなさなくなってきた。そこで、ユーザー、通信、インターフェイス、ネットワークに対し、常に疑いを持って接することでセキュリティを担保するというものである。

複雑化・巧妙化するサイバー攻撃に対して、自社の課題を3つ定義した。1点目は NHKグループにおける総合技術会社としてグループ全体を脅威から守ること。2点目は2020年に向けて高まるサイバー攻撃リスクへの対応。3点目として、脅威可視化アセスメントで発覚したサイバー攻撃への対応であった。

「ゼロトラストの実現に必要なサービスが全て含まれているのが Microsoft 365 E5 でした。さまざまな製品を組み合わせることで実現することもできましたが、管理・運用が別々になり煩雑です。Microsoft 365 E5 であれば必要なサービスが１つの製品内で完結していますので、連携がスムーズですし、トータルコストも抑えることができると判断し、採用を決めました」（穂積氏）

早期導入を考えていた同社では、これまで Office 365 を利用していたこともあり、Microsoft 365 E5 へのアップグレードであれば抵抗なく導入ができると考えた。さらに、クラウドサービスのため短期間での導入が可能である点、マイクロソフト社の圧倒的な脅威情報量から得られる脅威の検出率の高さも Microsoft 365 E5 採用の決め手になったという。

■ 対応すべき3つの課題

1. NHK グループにおける総合技術会社としてグループ全体を脅威から守る
2. 2020年に向けて高まるサイバー攻撃リスクへの対応
3. 脅威可視化アセスメントで発覚したサイバー攻撃を受けていた事実の解消

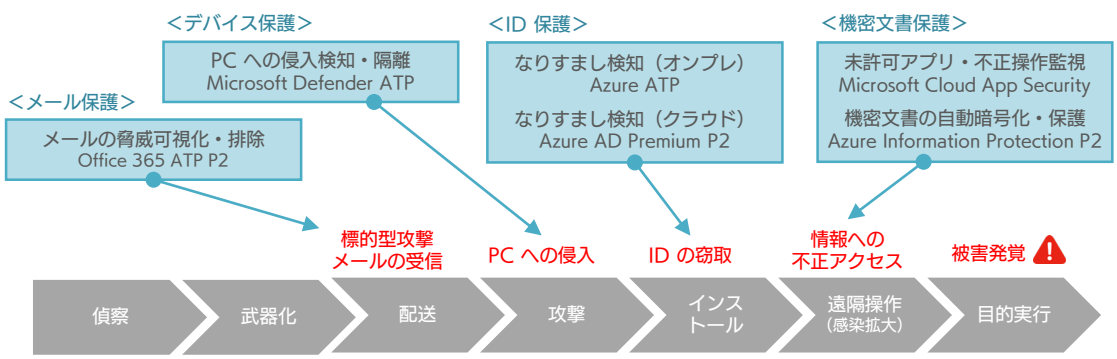
標的型攻撃のサイバーキルチェーンを包括的に防御・対処

近年のサイバー攻撃は段階を踏んで行われるようになっており、その段階を構造化したものを『サイバーキルチェーン』と呼んでいる。その『サイバーキルチェーン』を断ち切るために、攻撃の各段階に Microsoft 365 E5 の各サービスを活用し、多層的に防御・対処する。

メールの脅威可視化と排除には、フィルタリングサービスである『Office 365 ATP P2』を利用する。複雑化・巧妙化するサイバー攻撃により社内へ侵入してしまった場合には、PC への侵入検知と隔離にエンドポイントセキュリティの『Microsoft Defender ATP』で対処する。不正入手された ID とパスワードによってアクセスされた場合でも、『Azure AD Premium P2』と『Azure ATP』により、クラウド・オンプレミスの両方で、なりすましの検知と防止を行う。さらに、保存されている機密情報の公開範囲を把握し、分類し、保護する『Microsoft Cloud App Security』と機密文書を自動暗号化する『Azure Information Protection P2』によって、情報流出を防ぐ。

「当社にはニュース、スポーツ、音楽などの中継といった現場での仕事や、放送電波の中継所の設置や修繕作業、さらには災害時に無線局へ出向する緊急保守の仕事などがあります。どのような場合であっても、さまざまなワークスタイルとワークプレイスが Microsoft 365 E5 で保護できるようになることを期待しています」（穂積氏）

■ サイバーキルチェーンに対する Microsoft 365 E5 の対応イメージ



Microsoft 365 E5 からあがるアラートの処理に業務が圧迫

Microsoft 365 E5 の導入によりセキュリティの強化を実現した同社であったが、脅威が可視化されることにより、新たな課題が表面化した。

Microsoft 365 E5 からあがるアラート数が膨大で、調査・対応の時間が増大し、業務を圧迫する恐れがあるということである。アラートは重大なインシデントとなるものか、静観するものか、誤検知であるものかをすべて調査・判断していかなければならない。さらに、NHKテクノロジーズでは24時間365日働いている社員がいるため、常に監視を行い、夜間であってもアラート発生時には迅速に対処しなければならない。しかし、セキュリティを専門にするエンジニアが少数であったため、常に監視を続け、膨大なアラートを処理することは難しい状況にあった。

セキュリティの強化を実現し、検知分析、被害軽減、事後対応など、『インシデントレスポンスの強化』に取り組もうと考えていた同社は、アラートの対応に業務が圧迫されることを懸念し、監視・分析を自社だけで担うことは難しいと考えた。そこで監視を外部へ任せる決断をした。

■ Microsoft 365 E5 導入後の新たな3つの課題

- 誤検知も含めたアラート数が膨大になり、調査・判断・対応にかかる時間が増大
- 24時間365日の監視が必要であるが、対応できるリソースが不足
- 複雑化・巧妙化するサイバー攻撃に対応する、広い知見と経験を持つ優秀なセキュリティエンジニアが不在

インシデントレスポンス強化の実現に向け、SBT の監視サービスを採用

セキュリティの監視を外部へ任せることを決断した同社は、Microsoft 365 E5 の導入支援を行った SBT が提供するセキュリティ監視サービス、『MSS for Microsoft 365』および『MSS for EDR』の採用を決定、2019年9月から運用を開始した。

「NHKテクノロジーズは24時間365日働いている社員がいるため、夜間や休日であっても、平日の昼間帯同様に監視ができないといけませんでした。しかしながら自社では十分な人材を確保することができません。外部へ任せるにあたり、24時間365日の対応が可能であること、セキュリティに対する知見が十分であること、また、クラウドサービスの利用が増えているため、クラウド環境に対する知見が豊富であることも条件でした。SBT であれば当社への理解も深く、さらにクラウドサービスの導入実績が豊富なため、安心して任せられると感じました」（穂積氏）

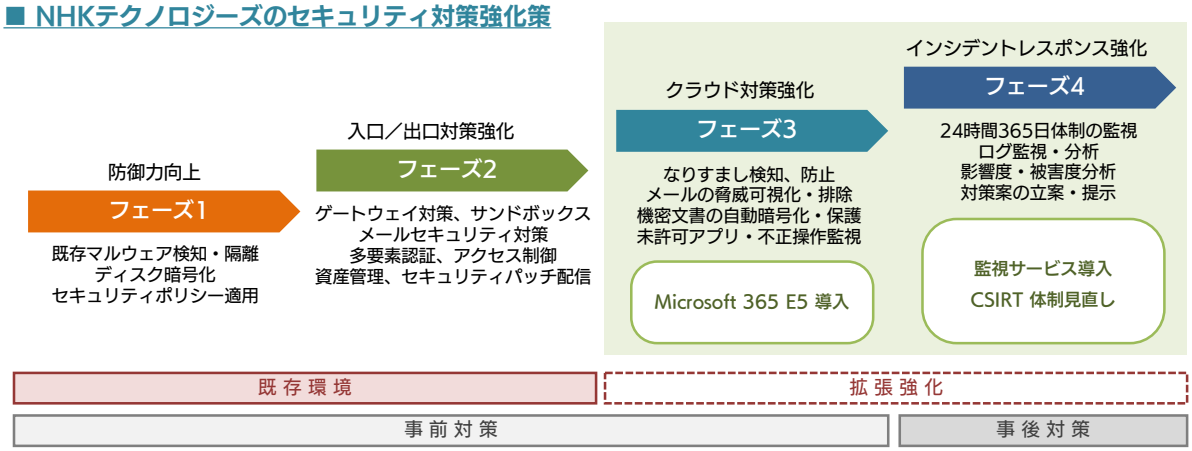
MSS を導入したことにより、常時監視する必要がなくなり、業務負荷を軽減させることができた。また、アラートとログを相関的に分析し、影響度、被害度の分析、考えられる被害と取るべき対策を SBT から提示されるようになったため、今何が起こっているのか、これからどうすればよいのか、迷うことなく即座に対応をスタートできる仕組みを構築できた。

「セキュリティエンジニアの不足を課題とされている企業があるとよく聞きますが、セキュリティ業務のアウトソーシングはそれを解消する有効な手段の1つと考えています。MSS を導入したことで、私たちはさまざまなセキュリティの監視から解放され、ユーザー対応に注力できる体制を整えることができました」（長村氏）

■ MSS 導入効果

- 夜間休日も現場で働く環境に合わせ、24時間365日の監視体制を実現
- アラートの調査・分析にかかる時間と業務負荷を軽減
- アラートの影響度・被害度・対策案を提示されるようになり、ユーザー対応に注力できる体制を実現

■ NHKテクノロジーズのセキュリティ対策強化策



セキュリティ対策のさらなる強化と、グループ展開に向けて

2019年9月から運用を開始した、Microsoft 365 E5 と MSS により、従来に比べ、より具体的に脅威に関しての状況を察知し、即座に対応できるようになったという。セキュリティの確保と、多様な働き方に柔軟に対応できる環境が整った同社は、今後さらなるセキュリティ強化を考えている。

2020年度中に『Azure Information Protection P2』を本格導入する予定だ。『Azure Information Protection P2』は Office 365 で作成されたドキュメントに自動的にラベリング・暗号化を行う。ファイルをいつどこで開いたかを監視するとともに、ファイルを暗号化することで社内外への機密情報の漏えいも防ぐことができる。運用開始に向け、どのファイルが機密情報であるのかなど整理を行う必要があるため、現在社内ルールの整備を進めている。また、2社の企業統合と新たなソリューションの導入により、インシデント発生時の体制を改める必要が出てきたため、CSIRT の見直しを進めている。

さらに長村氏は、今回のセキュリティ強化の施策をNHKグループ全体に展開していきたいと考えている。

「今回の導入により、効果的かつ合理的に一定の対策が施せていると感じています。自社導入により得られたノウハウを蓄積していき、グループ全体の『セキュリティ強化』の実現に向け、親会社である NHK とともにグループでの横展開を検討していきたいと考えています」（長村氏）

NHKグループにおける総合技術会社として NHKテクノロジーズは、サイバーセキュリティという現代的な課題に対しても、『ゼロトラスト』という新たなセキュリティモデルによって、公共メディアを支えていく。

■ 今後のセキュリティ強化に向けた対応

- 2020年度中の Azure Information Protection P2 本格導入を検討
- 2社の統合に加え、Microsoft 365 E5・MSS の利用開始に伴い CSIRT 体制の見直し

『働き方改革』に向けた Microsoft 365 のさらなる活用へ

脅威可視化アセスメントをきっかけに、Microsoft Office 365 から Microsoft 365 E5 を導入した同社だったが、今後はセキュリティ強化以外にも、『働き方改革』に向けた取り組みとして Microsoft 365 を活用していく予定だ。

その一つとして現在、モバイルデバイスを管理する『Microsoft Intune』を導入し、従業員が BYOD で利用する端末からメールやドキュメントを閲覧できるようにしている。万が一端末を紛失した場合には、会社に関わるデータのみ削除が可能なため、会社専用の端末を持ち出すことなく、生産性向上を実現している。

「これまではセキュリティの担保から、外部で社内の情報にアクセスする場合は、PC の利用申請をしてもらい、持ち出しを許可していました。Microsoft Intune の導入により、いつでもどこでも社内の情報にアクセスできるようになり、働きやすい環境とセキュリティを両立できるようになりました」（穂積氏）

さらに今後は社内の情報共有基盤として『SharePoint Online』や『Microsoft Teams』『OneDrive for Business』の活用を検討している。『Microsoft Teams』では、これまでメールで行ってきた社内の情報共有の一部を置き換え、より情報が必要な人に確実に届く仕組みとして代替できるのではないかと考えている。

「今、世界的に流行している感染病の影響から、出社しなくても業務ができる IT 環境を早急に整備しなくてはならない状況になりました。このような事態に対応するため、SharePoint や OneDrive、Teams の活用を早期に開始し、円滑な業務遂行ができる環境を提供することが重要だと考えています。可能な限り展開を速く進めるためには、当社だけの力では限界があるため、パートナーである SBT にはさらなる支援を期待しています」（長村氏）

新たなソリューションの導入をきっかけに、NHKテクノロジーズは働き方の変革にも積極的に取り組み、セキュリティを担保しながら、より働きやすい環境の整備に力を入れていく。

SBテクノロジー株式会社 岡野 丈夫（写真右）

■ Microsoft 365 の活用による『働き方改革』の推進

- 『Microsoft Intune』により、BYOD で外出先からメールやドキュメントの閲覧を可能に
- 新たな情報共有のツールとして『Microsoft Teams』の活用を検討

■ 関連するサービスページ（SBT Web サイト）

- Microsoft 365 導入・運用支援サービス
- MSS for Microsoft 365
- MSS for EDR

お客様窓口

SBテクノロジー株式会社
〒160-0022
東京都新宿区新宿 6丁目27番30号 新宿イーストサイドスクエア 17階

TEL：03-6892-3154
MAIL：sbt-ipsol@tech.softbank.co.jp
企業情報：https://www.softbanktech.co.jp/