次世代エンドポイントセキュリティの基盤構築と運用

System Infrastructure Construction and Operation of Next-Generation Endpoint Security

卯 月 義 文，岡 田　遥

要　約　ネットワーク境界のセキュリティ対策製品だけではセキュリティインシデントを完全に防ぐのは困難であるため，エンドポイント上で被害を食い止める次世代エンドポイントセキュリティ対策製品の導入の必要性が増している．本稿では，筆者が経験した次世代エンドポイントセキュリティ対策製品（EPP 製品）の導入事例から得た製品情報と基盤構築・運用のノウハウについて解説する．

「設計・構築フェーズ」については，自社に導入するバージョンを慎重に選定すること，および自社のセキュリティポリシーとの整合性を取り，機密情報を含むファイルのクラウドへのアップロード可否を検討することが重要である．「試行フェーズ」については，多様な環境やソフトウェアを使用している部署やグループ会社を試行対象に選定することが重要である．「全社展開フェーズ」については，ユーザへの業務影響を極力減らすため監視モードで展開することおよびソフトウェア配布ツールを使用して展開することが重要である．

全社展開後は防御モードへの移行，クラウド化の検討，運用自動化の検討を行い，運用方針を実現する．

Abstract　It is difficult to prevent security incidents completely, only with network edge security products. So, there is a growing need to install next-generation endpoint security products that stop the damage on the endpoint. This article describes product information and know-how on System Infrastructure construction and operation obtained from the case study of the next generation endpoint security countermeasure product (EPP product) experienced by the author.

In the “design and construction phase”, it is important to carefully select the version to be installed into your company, and to interface with your own security policy, and to consider whether files containing confidential information can be uploaded to the cloud. In the “trial phase”, it is important to select departments or group companies that use various environments or software for trial. In the “company-wide deployment phase”, it is important to deploy in the monitoring mode and deploy using a software distribution tool in order to minimize the business impact on users.

After company-wide deployment, we will shift to block mode, consider to cloud migration, and consider operational automation to realize the operation policy.

1. は じ め に

近年のサイバー攻撃では，未知のマルウェアの使用や，ソフトウェアにおける脆弱性情報の公開直後の攻撃など，攻撃の巧妙化が進んでいる．独立行政法人情報処理推進機構（IPA）が公開した情報セキュリティ 10 大脅威 2019（組織）[1]によると，「組織」向け脅威の 1 位は「標的型攻撃*1 による被害」，同 3 位は「ランサムウェア*2 による被害」となっている．標的型攻

撃の攻撃手法やランサムウェアの感染経路としては，「メールの添付ファイル」や「ソフトウェアの脆弱性を悪用した攻撃（エクスプロイト[*3]）」や「未知のマルウェアの実行」によるものが多い．エクスプロイトに対しては，修正プログラムの適用等の迅速な対応能力が求められる．特にゼロデイ攻撃[*4]では，対応の遅れが致命的な損害を与える可能性があるため，より迅速な対応が求められるものの，これまでの人手を介した対応には限界がある．このようなサイバー攻撃の変化に対して，従来のパターンマッチング型のウイルス対策製品[*5]では防御が困難となってきている．

そのため，プログラムが動作する一連のプロセスの中に含まれるエクスプロイトに罠を仕掛け，その攻撃の根幹をなす共通のテクニック（以降，根幹テクニック）を封じ込めて，悪意のある活動が動作する前に攻撃を阻止する，振る舞い検知機能を持つ次世代エンドポイントセキュリティ対策製品の導入が効果的である．内閣サイバーセキュリティセンター（NISC）が2018年改訂した政府統一基準[2]にも，「エンドポイント検知による未知の不正プログラムの被害の未然防止/拡大防止」の記載が追加されていることから，社会全体としてエンドポイントにおけるセキュリティ機能の強化が求められていることがわかる．本稿では，筆者が経験した次世代エンドポイントセキュリティ対策製品の導入事例（以降，本事例）から得た製品情報と基盤構築・運用のノウハウについて解説する．

2. 次世代エンドポイントセキュリティ対策製品の特徴と導入における注意点

本章では，まずエンドポイントセキュリティの動向について述べる．本事例における次世代エンドポイントセキュリティ対策製品の特徴，導入における注意点についても解説する．

2.1 エンドポイントセキュリティの動向

近年のサイバー攻撃は手口が極めて高度化・巧妙化しているため，ファイアウォールなどのネットワーク境界のセキュリティ製品だけでは，セキュリティインシデントを完全に防ぐのは困難である．そのため，ネットワーク内に侵入したマルウェアが実際に活動を行うエンドポイント上で被害を食い止めることの重要性が増している．そこで登場してきたのが次世代エンドポイントセキュリティ対策製品である．それらは，防御が主体のEPP（Endpoint Protection Platform）製品と検知が主体のEDR（Endpoint Detection and Response）製品の大きく二つの種類に分類される．

EPP製品は「エンドポイントをマルウェア感染から防御するためのもの」であり，従来のパターンマッチング型のウイルス対策製品もEPP製品に分類される．しかしながら，新種のマルウェアが大量に増加している現在，パターンマッチングで用いるパターンファイル[*6]の更新・配布が間に合わず，未知のマルウェアを使った攻撃に対応しきれないケースが多く発生している．特に標的型攻撃では未知のマルウェアやエクスプロイトを利用した攻撃手法が用いられるため，従来のパターンマッチング型のウイルス対策製品では防ぐことが困難である．そこで，マルウェアや悪意のあるプログラムを検知し，実行を防御する新たなEPP製品が登場し，その重要性を増している．EPP製品は，NGAV製品（次世代アンチウイルス製品）と表されることもある．

一方EDR製品は，防御をすり抜けエンドポイントが標的型攻撃やマルウェア感染することを前提とした「エンドポイントに到達した脅威を早期に検知し，対応するためのもの」である．

EDR 製品はマルウェアそのものを検査するのではなく，感染したエンドポイントでのマルウェアの挙動や標的型攻撃をクラウドサービス上で相関分析することで，脅威を検知し，被害の拡大を防ぐための対応を迅速に実施することができる．

本稿では，エクスプロイトやランサムウェア等の脅威を検知・防御することをセキュリティ対策の主体と考え，振る舞い検知機能を持った EPP 製品の導入事例について紹介する．

2. 2　次世代エンドポイントセキュリティ対策製品の特徴

標的型攻撃では，主にメール経由でエクスプロイトを仕掛け，システムに侵入してマルウェアを送り込み，実行させることで機密情報を持ち出すといった手法が一般的である．本事例の次世代エンドポイントセキュリティ対策製品は，エクスプロイト防御やマルウェア防御などの防御機能によって，標的型攻撃のようなサイバー攻撃から総合的に防御することができる．

2. 2. 1　構成するコンポーネントとその特徴

まずは次世代エンドポイントセキュリティ対策製品を構成するコンポーネントとその特徴について解説する．図 1 のような主要コンポーネントで構成されている．

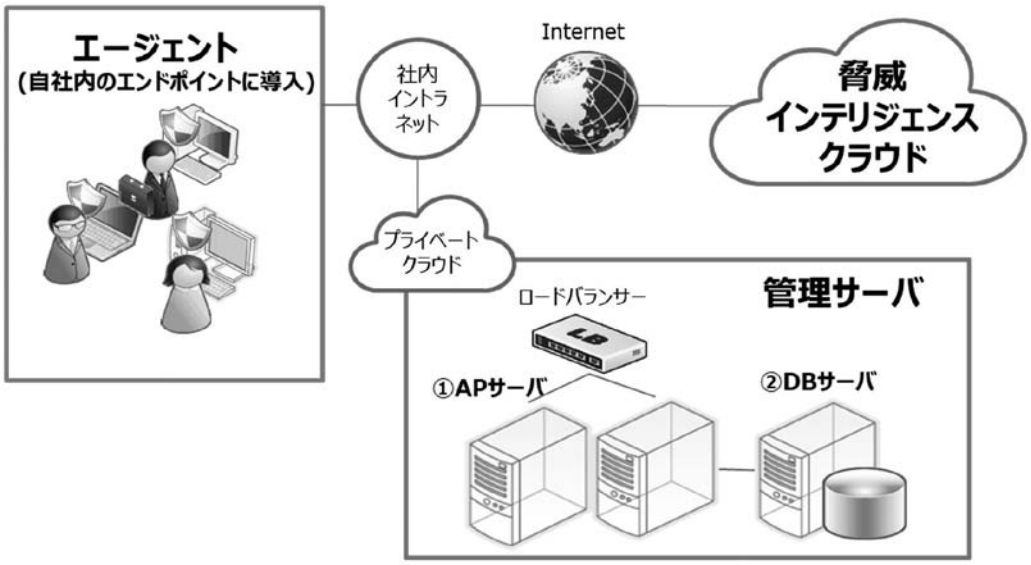

図 1　次世代エンドポイントセキュリティ対策製品のコンポーネントとその構成

・エージェント

　エンドポイント上に導入し，エクスプロイト攻撃やマルウェアによる攻撃の実行を未然に阻止する．エージェントが軽量であり，定常的に既存環境に影響を与えないことが重要である．

・管理サーバ

　各エンドポイントに導入されているエージェントを管理するための以下の二つの機能を持つ．管理サーバはプライベートクラウドにオンプレミスで構築している．

　① AP サーバ

DB サーバやエージェントや脅威インテリジェンスクラウドと情報をやり取りする機能を持つ．AP サーバは DB サーバから定期的にセキュリティポリシーを取得し，すべてのエージェントに配布し，各エージェントはセキュリティイベントに関連する情報を AP サーバに送信する．AP サーバは複数台設置しロードバランサー等でエージェントからの通信を負荷分散する．システムに何らかの障害が発生した場合でもシステム全体の機能を維持し続けられるよう冗長化構成を採用することが望ましい．

② DB サーバ

管理情報，セキュリティポリシー，エンドポイントの履歴，およびセキュリティイベントやログに関する情報を保存する機能を持つ．

・脅威インテリジェンスクラウド

エージェントから提供されるマルウェアの可能性を含む未知のファイルを検査し，その検査結果を一元的に可視化し，結果をフィードバックする．世界中から収集したマルウェア情報を基に検査するため，未知のマルウェアにも迅速に対応できる．

2.2.2　エクスプロイト防御

次世代エンドポイントセキュリティ対策製品のエージェントは，アプリケーションの脆弱性を利用したエクスプロイトを検知し防御する機能を保有している．エクスプロイトの種類は数多くがあるが，使用される根幹テクニックの種類は限定的である．エクスプロイトは，複数の根幹テクニックを連鎖的に実行することで目的を達成する．次世代エンドポイントセキュリティ対策製品では，それぞれの根幹テクニックに対して防御機能を備えているため，エクスプロイトに対する多層的な防御ができる．当該機能は研究者が常に最新の攻撃手法を研究し製品に適用しているため，既知のものだけでなく，未知のエクスプロイトに対しても防御することができる．エクスプロイトを利用して感染するランサムウェアに対しても有効である．

2.2.3　マルウェア防御

世界中の企業で検知された大量の未知検体を解析した結果を蓄積している脅威インテリジェンスクラウドとの自動連携，機械学習による静的解析，サンドボックス[*7]による動的解析などの複数の検知技術により，従来のパターンファイルによるパターンマッチングを用いた防御とは異なった方法で，マルウェア防御を実現している．

・既知のファイルのハッシュ値照合

検知されたファイルと脅威インテリジェンスクラウドに格納されている脅威情報とのハッシュ値の照合により，既知のマルウェアを検知・防御する．

・未知のファイルの動的解析

脅威インテリジェンスクラウドに情報がない未知のファイルの場合でも，ファイルをクラウドへアップロードし，サンドボックスで動的解析を実施して，マルウェアかどうかを判定する．その判定情報がクラウドに蓄積され世界中で共有されることで，未知のマルウェアが即時に既知のものとなり，より速い防御ができる．

・機械学習による静的解析

未知のファイルを検知しサンドボックスで動的解析している間，エージェントの機械学習エンジンにより，未知のファイルが静的解析され，実行前制御される．この機能により，

サンドボックスによる動的解析の間，エンドポイント端末がマルウェア感染することを防いでいる．

・感染後の検知機能

正常なプログラムも含めて動作したプログラムを管理サーバが常に記録しており，万が一感染前に防御できなかった場合でもリアルタイムに通知することで，マルウェア感染の可能性を即座に把握し，感染の疑いのある範囲を調査することができる．

2.2.4　ネットワークセキュリティ製品との連携

脅威インテリジェンスクラウドは，エンドポイントだけではなく，ネットワークセキュリティ製品とも連携しており，様々なレイヤのセキュリティ製品で検知した脅威情報を格納している．そのため，脅威インテリジェンスクラウドと連携することで，様々なレイヤのセキュリティ製品と脅威情報を共有することができる．

2.3　次世代エンドポイントセキュリティ対策製品導入における注意点

ここまで次世代エンドポイントセキュリティ対策製品の特徴を述べてきたが，本節では，導入においての注意点について解説する．

2.3.1　従来のウイルス対策製品との併用

一点目は次世代エンドポイントセキュリティ対策製品を導入しても，セキュリティ対策が万全というわけではないという点である．従来のパターンマッチング型のウイルス対策製品では使用できていた機能（リアルタイムスキャン[*8]やウイルスの隔離・駆除等）が，次世代エンドポイントセキュリティ対策製品には備わっていない場合があるためである．自社に導入する次世代エンドポイントセキュリティ対策製品が，従来のウイルス対策製品の機能をすべてカバーし得るものなのか検討することが重要となる．本事例では，ウイルスの隔離・駆除機能を利用するため，従来のウイルス対策製品と併用する方式を選択した．

2.3.2　過検知によるユーザに対する業務影響と新たな運用負担

二点目は次世代エンドポイントセキュリティ対策製品を導入することで，ユーザに対する業務影響と新たな運用負担が発生する点である．振る舞い検知機能がプログラムの怪しい動きを検知・防御するため，検知したものが正規のプログラムでも動作を止めてしまうこと（以降，過検知）が高頻度で発生する可能性があるためである．過検知は，正常なプログラムが攻撃者の用いる攻撃手法と類似した挙動をした際に発生することが多い．攻撃者が用いる攻撃手法と，それに対する次世代エンドポイントセキュリティ対策製品の防御機能，当該防御機能で過検知されやすい攻撃手法と類似したプログラムの挙動についての例を表１に示す．

表 1　過検知が発生する例

攻撃手法	防御機能	攻撃手法と類似した プログラムの挙動（例）
エンドポイント内のデータを暗号化し，データを復旧するための身代金を要求する攻撃（ランサムウェア）	主要なフォルダに，ユーザからは見えないおとりファイルを配置する．起動したプログラムが本来ユーザは操作できないファイルに対し，変更（書込）をかけてくる行為を検出した場合，そのプログラムを強制終了する	不要ファイルを削除するツールが，フォルダ内のファイルを削除する
Office ファイルのマクロを実行させることにより，外部のサイトから，未知のマルウェアをダウンロードし，実行させる	ユーザが利用するプログラムにおいて，特定のプログラムを外部から呼び出すことを許可，または禁止することにより，攻撃を防ぐ	PC 起動時に，イントラネットのトップページを表示させるスクリプト（自動起動）が，プロセスを自動起動して，http で外部と通信する
Web ブラウザなどの正常なプログラムに対して DLL（Dynamic Link Library）[*9] を注入することにより，その正常なプログラムの実行時にマルウェアを実行させる（DLL インジェクション）	信頼できないコード領域から，DLL のメモリアドレスを取得する行為を防ぐ	内部監査ツール等が，DLL を正常なプログラムに注入し，PC 上のプログラム動作情報を取得する

悪意のあるものなのかどうか明確でないグレーな検知に対して，疑わしいものは防御するということがセキュリティにおける原則であるため，過検知は切り離せない事象である．しかし，過検知の発生によりユーザは検知されたプログラムを利用できなくなり業務影響が発生する．未知の攻撃に対する防御を保ちながら，過検知による業務影響を低減させるためには，運用担当がホワイトリスト登録[*10] のように，過検知したプログラムを検知対象外に設定し，その後の過検知を発生させなくする作業（ポリシーチューニング）を行うことが有効である．この作業はユーザの業務停止時間が短くなるよう迅速な対応が求められる．

3.　セキュリティ基盤構築

本事例における基盤構築では，次世代エンドポイントセキュリティ対策製品導入によるユーザの業務影響を極小化することを基本方針の一つとしている．

基盤構築の工程は「設計・構築フェーズ」「試行フェーズ」「全社展開フェーズ」の三つのフェーズで行っている．本章では，各フェーズで考慮すべき点について解説する．

3. 1　設計・構築フェーズ

本節では，設計・構築フェーズで考慮すべき点について解説する．

3. 1. 1　バージョンの選定

日々進化を続けるサイバー攻撃に対応すべく，次世代エンドポイントセキュリティ対策製品も短いサイクルで新たなバージョンが次々とリリースされている．将来どのような機能が提供されるのか，導入する製品がどのように変化を遂げていくのか（プロダクトのロードマップ）

を確認しながら，以下のポイントについて検討し，自社に導入すべきバージョンを選定することが重要となる．

・バージョンの動作の安定性
　バージョンが新しいものには新機能が追加されることが多いが，新機能には不具合が含まれ，動作が不安定となるリスクがある．自社に導入後，多数のユーザへの業務影響が発生しないよう，不具合が改修済で他社でも導入実績がある，動作が安定したバージョンを導入することを検討する．
・バージョンによるアーキテクチャの差分
　製品によっては，バージョンにより管理サーバのアーキテクチャがオンプレミスからクラウドへ変更される場合もある．自社のシステム構成などを鑑みて，バージョンを選定する．
・自社の環境との適合性
　自社で標準的に利用しているエンドポイント（クライアント PC）の OS やセキュリティ製品等，自社の環境への適合性を考慮する．例えば Windows 10 には FU（Feature Update）といった環境の差分がある．導入する次世代エンドポイントセキュリティ対策製品のバージョンによっては，自社の FU に対応していない場合もあるためシステム要件などを確認する．

3. 1. 2　自社のセキュリティポリシーとの整合性

自社に新たなセキュリティ製品を導入する際には，自社のセキュリティポリシーとの整合性を取らなければならない．次世代エンドポイントセキュリティ対策製品では，未知ファイルを検知した際，脅威インテリジェンスクラウドにアップロードし，サンドボックスで動的解析を行う．この一連の動作は自動的に行われるため，ファイル毎のアップロード可否をその都度判断することができない．そのため，機密情報を含んでいるファイルが脅威インテリジェンスクラウドに意図せずアップロードされる可能性がある．脅威インテリジェンスクラウドは情報管理に関して十分な安全性が確保されているが，自社のセキュリティポリシーに則り，脅威インテリジェンスクラウドへのアップロードを許可するファイルの種類を検討し，設定に反映しなければならない．

3. 1. 3　パラメータの管理

通常のシステムでは，設計・構築フェーズで定義したパラメータは，後から変更されることが少ない．しかし，次世代エンドポイントセキュリティ対策製品の運用においては，ポリシーチューニング等によりパラメータの変動が多い特性を持つ．そのため，設計・構築フェーズでパラメータを確定することに固執するのではなく，運用を行う中でのパラメータ変動に対してどのように柔軟に管理するのかを検討することが重要である．本事例では，運用管理における変更管理業務でパラメータの変更についても厳格かつ柔軟に管理している．

3. 1. 4　導入対象の選定

次世代エンドポイントセキュリティ対策製品の導入対象は，クライアント PC やサーバ，また OS 等で種類は多種多様であり，利用方法についても OA 用 PC や開発用 PC と様々である．本事例においては，エージェントが管理サーバと通信できない環境では，脅威インテリジェン

スクラウドとの自動連携などの主要防御機能を利用することができないため，プライベートクラウドと通信できることが条件となる．また一般的に標的型攻撃やランサムウェアの対象となるのはクライアント PC であることから，初期における導入対象は「社内イントラネットに接続するクライアント PC」としている．

インターネットに直接接続し，リスクの高いクライアント PC での運用を行いながら過検知の減少や製品の安定性を確認した上で，社内イントラネットに接続するサーバについても順次導入対象に追加していく．

3. 2　試行フェーズ

本事例では，全社展開フェーズにおける過検知の大量発生や，他ソフトウェアとの競合によるユーザへの業務影響発生のリスクをできる限り低減するため，全社展開を開始する前に一部組織を対象とした試行（先行導入）フェーズを設けている．

本節では，試行フェーズで考慮すべき点について解説する．

3. 2. 1　試行対象の選定

3.1.1 項で述べた通り，次世代エンドポイントセキュリティ対策製品のバージョンアップは短いサイクルで行われるため，試行期間中にバージョンアップしなくて済むよう，試行はできる限り短期間で行うことが重要である．短期間での試行で最大限の効果（他のソフトウェアとの競合を事前に発見する，および過検知をできる限り減らす）を出すために，多様な環境やソフトウェアで試行できるような試行対象の選定が重要である．例えば以下の点を考慮する．

- 独自のソフトウェアやハードウェアを使用している部署や，グループ会社に試行を依頼する．
- 一部署から多くの PC への試行協力を仰ぐのではなく，より幅広い多数の部署から数台の PC に試行を依頼する．

3. 2. 2　全社展開に向けた自社のポリシーチューニングのベースラインを作成

全社展開フェーズにおける，過検知の大量発生や他ソフトウェアとの競合によるユーザへの業務影響発生のリスクをできる限り低減するため，試行フェーズで自社において標準的に使用されるソフトウェア等を事前に動作検証を実施しポリシーチューニングを行うことで，全社展開に向けたポリシーチューニングのベースラインを定める．特に注意すべきは，既存のパターンマッチング型のウイルス対策製品が持つ振る舞い検知機能である．既存のウイルス対策製品は次世代エンドポイントセキュリティ対策製品と類似した機能を持っている可能性があり，互いの機能が競合して誤動作を引き起こすリスクがあるためである．競合が発生すると過検知が大量発生し業務に影響するケースも考えられる．対処策として，より防御レベルの高い，次世代エンドポイントセキュリティ対策製品の防御機能を優先し，既存のウイルス対策製品の振る舞い検知機能を無効化することを検討する．既存のウイルス対策製品と併用する際は，競合することがないか全社展開前の試行フェーズで事前に動作検証を行うことが必須である．

3.2.3　運用体制の整備や運用要員の育成

試行フェーズは，運用体制の整備や運用要員の育成の面でも重要なフェーズである．プロダクトの製品ベンダーが提供する運用支援サービスの支援を受ける OJT 期間中に，試行期間の運用を行うことで，運用要員はプロダクト固有の操作方法やセキュリティに関する知識を身につけ，全社展開に向けて運用体制を細かく整備していくことができるようになる．

3.3　全社展開フェーズ

全社展開時には，試行フェーズでは事前に検出できなかった未知のファイルが多く実行されることになるため，過検知が大量に発生することや，他ソフトウェアとの競合が発生することが予想される．また，セキュリティ製品においては，未導入の PC の存在がセキュリティホールとなるため，自社の PC に素早くかつ漏れなく導入することが肝要である．本節では，全社展開フェーズで考慮すべき点について解説する．

3.3.1　動作モードを監視モードで実施

次世代エンドポイントセキュリティ対策製品には，一般的に防御モードと監視モードの二つの動作モードがある．防御モードはセキュリティ脅威を検知した際，ユーザへ通知するとともに検知したアプリケーションの実行を停止する．監視モードはセキュリティ脅威を検知した場合でも，利用者への通知は行わず，アプリケーションも停止しない．監視モードの用途は，導入初期に過検知されるものを炙り出し，ポリシーチューニングを行うことで防御モードに移行した際の業務影響を極小化するための準備である．全社展開期間中は，まず監視モードに設定して過検知の発生でユーザへの業務影響が発生しないよう安全な配布を実施し，監視モードで全社への展開が完了後，過検知が収束したと判断した際に，速やかに防御モードに移行する．

3.3.2　ソフトウェア配布ツールによる段階的かつ漏れのない配布

次世代エンドポイントセキュリティ対策製品を全社に展開する際は，一斉導入するのではなく，ソフトウェア配布ツールを用いて段階的に自動配布を行うことが望ましい．これは，一斉導入による過検知の急増や他ソフトウェアとの競合が発生し，ユーザの業務に過大に影響することを避けるためである．またエージェントの導入を手動でインストールすると，導入進捗をコントロールすることが困難であり，全社展開期間内に未導入のユーザや機器が残る可能性がある．ソフトウェア配布ツールを使用し，自動で段階的に導入することで安全に漏れなく確実に導入する．

3.3.3　全社展開時期の設定

次世代エンドポイントセキュリティ対策製品の全社展開時期を設定する際には，他のソフトウェアのバージョンアップ計画と整合性を図る．他ソフトウェアのバージョンアップにより，競合や過検知が発生する可能性があるためである．特に Windows 10 における FU の適用や，既存のウイルス対策製品のバージョンアップについては注意を払う．次世代エンドポイントセキュリティ対策製品のバージョンによっては，FU の最新バージョンをサポートしていない場合もあり，既存のウイルス対策製品によっては，3.2.2 項で述べた通り一部の機能と競合する可能性もある．全社展開時期については，社内の FU や既存のウイルス対策製品のバージョン

アップ時期が重ならないような計画を策定することが重要である．

4. セキュリティ運用

本章では，次世代エンドポイントセキュリティ製品における運用について解説する．

4.1 次世代エンドポイントセキュリティ製品の運用業務

本事例で定義した運用項目を表2に示す．運用品質を正確に把握し継続的に改善するための「運用管理」，プロダクトに依存しないシステム共通のオペレーション等を行う「システム運用」，プロダクト固有のオペレーションおよび自社基準に基づいた判断や承認等を行う「プロダクト運用」のカテゴリに大別される．

表2 次世代エンドポイントセキュリティ製品の運用項目一覧

カテゴリ	運用項目	作業内容
運用管理	インシデント管理	システム監視やプロダクトが検出するエンドポイントからのアラート等（これをインシデントと呼ぶ）を取り除き，システムの利用を継続できるようにするまでの対応活動を管理する．
	問題管理	根本原因が未知または未解消のインシデント（これを問題と呼ぶ）の根本原因を取り除き，再発防止策を策定するまでの対応活動を管理する．
	構成管理	システムを構成する要素の最新の状態を把握するために，システムの設定情報やドキュメントを正確に維持管理する．
	変更管理 リリース管理	システムを安全かつ効率的に変更するための対応活動を管理する．
	サービスレベル管理	サービスレベルを定義し，合意，記録および管理するための一連のプロセスを管理する．
	キャパシティ管理	システムで利用するリソースの需要に合わせて，適時に最適な費用で必要量を確保するための活動を管理する．
	アカウント管理	システムで利用するアカウントを登録・削除および管理する．
システム運用	システム起動・停止	システムを起動・停止する．
	バックアップ	システムバックアップ/データバックアップを取得する．
	リストア	システムリストア/データリストアを行う．
	パフォーマンス監視	CPU使用率，メモリ使用率，ディスク使用率を監視する．
	定期メンテナンス（パッチ適用）	OSやDBのパッチを適用する．
	システムエラー対応	システムエラーを監視し，復旧対応を行う．
プロダクト運用	問合せ受付窓口（1次）	エージェント導入に関する問合せ対応を行う．状況に応じて問合せ受付窓口（2次）へエスカレーションする．
	問合せ受付窓口（2次）/問合せ対応	製品挙動に関する問合せ対応を行う． 状況に応じてCSIRT（Computer Security Incident Response Team）[*11]やプライベートSOC（Security Operation Center）[*12]へのエスカレーション，製品保守ベンダーへの問合せ等を行う．

プロダクト運用	アラート対応	エンドポイントからのアラート監視/分析/ポリシーチューニングを行う. 状況に応じてCSIRTやプライベートSOCへのエスカレーション，製品保守ベンダーへの問合せ等を行う.
	データメンテナンス	蓄積するデータ（ログ等）を削除する.
	管理コンソール アカウント管理	プロダクトの管理画面でアカウントの作成/削除/棚卸を行う.
	パスワード変更 （システムID）	プロダクトが使用するシステムIDのパスワードを変更する.
	パスワード変更 （エージェントアンインストール）	エージェントのアンインストール時に必須入力となるパスワードを変更する.
	サーバステータス チェック	プロダクトの管理画面で各管理サーバやエージェントの稼働状態を確認する.
	エージェント棚卸	一定期間以上，管理サーバと接続していないエージェントの状況を確認した上で管理コンソール上から削除する.
	ライセンス更新	エージェントのライセンスを更新する．ライセンス期限を超過するとエージェント利用不可となる.
	デフォルト設定更新	定期的にアップデートされるプロダクトのデフォルト設定を更新する.
	プロダクトバージョンアップ	管理サーバおよびエージェントのバージョンアップ対応を行う.
	月次報告	運用報告書を作成し，報告を行う.
	アラート通知先 メール宛先変更	アラート通知先メールの追加，変更，削除等を行う.
	アラート通知先 メール設定変更 （無効化/有効化）	アラートメールが大量送信された場合にアラート通知機能を無効化する.
	ポップアップ メッセージ変更	アラート検知時，エージェントに出力されるポップアップメッセージを変更する.

4.2　運用方針と運用体制

前節で示した「運用管理」「システム運用」「プロダクト運用」のカテゴリ毎に，本事例での運用方針を解説する.

・「運用管理」については，ITIL（Information Technology Infrastructure Library）[*13]に則った管理プロセスを定めている．IT部門は限られた要員で多くのシステムを維持管理しなければならない．運用品質を保持し継続的な改善を行うために，IT部門が定めた管理プロセスに次世代エンドポイントセキュリティ対策製品の運用を組み込み自営する方針としている.

・「システム運用」については，自社が管理する基盤上に管理サーバを構築するシステムにおいて一般的に実施しなければならない運用プロセスを定めている．一方で，製品ベンダーが管理するクラウド環境上に管理サーバおよび管理機能が実装されてサービスを利用できる製品も増えており，システム運用の大部分は不要になる可能性が高い.

クラウド利用に切り替えることでシステム運用負担は減少するものと想定されるが，エンドポイントの情報が管理サーバ上，つまり外部のクラウド環境にアップロードされることになる．本事例では，システム運用を自営し，自社セキュリティポリシーとの整合性を鑑みながら，将来的にクラウド利用への切り替えを検討する方針としている．

・「プロダクト運用」については，次世代エンドポイントセキュリティ製品を利用する上で不可欠な運用プロセスを定めている．運用負担が大きいプロダクト固有の知識や操作を伴う運用作業（アラート監視/ポリシーチューニング/各種設定変更等）は外部委託し，自社に蓄積すべき知見を得るため自社基準に基づき判断や承認を行う運用作業（ポリシーチューニング判断や承認/報告等）は自営する方針としている．

本事例で構築した運用体制を図２に示す．上記の運用方針に従い，次世代エンドポイントセキュリティ対策製品の運用組織を三つのレイヤに分けている．

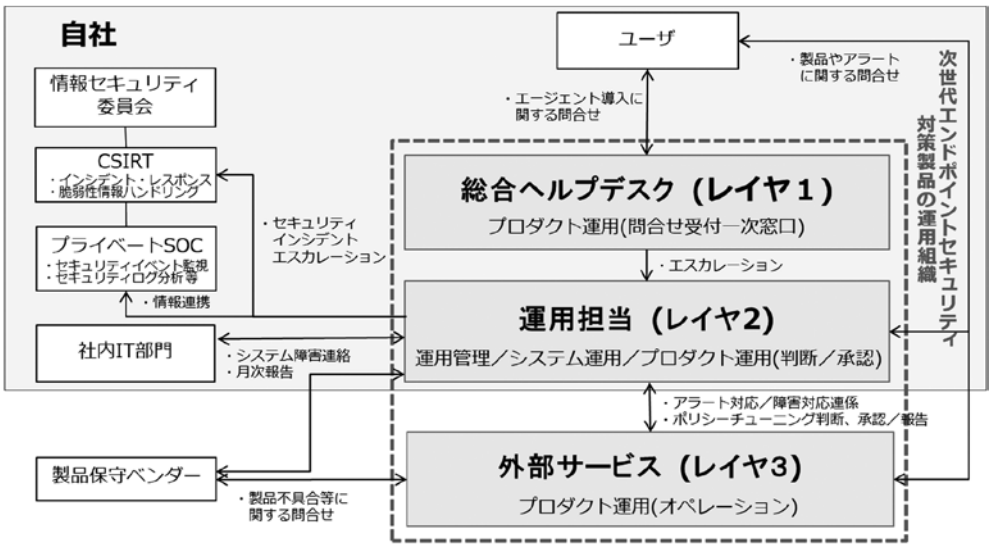

図２　運用体制図

レイヤ１は，次世代エンドポイントセキュリティ製品を利用するユーザからの問合せ受付一次窓口である．当該製品専任の窓口ではなく他システム等の導入サポートや問合せ受付窓口を兼任する．レイヤ２は，運用管理およびシステム運用が主であり，一部プロダクト運用（判断や承認等）を行う．レイヤ３は，主にプロダクト運用を行い，外部の運用サービスの活用も視野に入れる．

4.3　運用方針に沿った運用の実現

本節では，運用方針に沿った運用をどのように実現していくかについて時系列別に解説する．

①全社展開完了直後の運用

全社展開完了直後の運用では，ユーザへ業務影響が出ないよう安定性や品質を重視した運用がより求められる．全社展開フェーズと同様に，全社展開完了直後はアラート検知数

が多く，過検知も発生しやすいため，監視モードでの運用が望ましい．この監視モードのポリシーチューニングは，自社内に存在する多種多様なソフトウェアを検査することと同義である．その中で過検知されたものについて随時ポリシーチューニングを行うことで，アラート検知数を減少させ，防御モードへ移行した際のユーザへの業務発生リスクを軽減し，防御モードへの移行準備を整えていく．過検知は，ポリシーチューニングによる減少だけではなく，プロダクト自体の検知精度向上によっても順次減少していく．次世代エンドポイントセキュリティ対策製品運用における外部サービスでは，防御モードを想定したサービス仕様であることが多い．防御モードへの移行計画を立てながら，外部サービスへの運用委託の準備を進めていく．当然のことながら，監視モード期間中のセキュリティリスク対応についても充分に考慮する．

②アラート数収束後の運用

アラート数が減少して収束し，過検知によるユーザへの業務影響が発生するリスクが低いと判断できた場合は，防御モードへ速やかに移行し，プロダクト運用を外部サービスに委託する運用を開始する．運用体制が変更になっても運用の品質が下がらないよう，自社の要員における ITIL に則った運用管理業務により運用作業を適切に管理する．

③クラウドへの移行の検討

防御モードでの運用開始後，管理サーバのクラウドへの移行を検討する．しかし，管理サーバをクラウドへ移行後，自社で定義した運用業務の品質（バックアップの周期等）との差異が生じる可能性があるため，不要となった運用作業がベンダー側でどのように行われているのかをモニタリングすることが重要である．クラウドへの移行前にサービス仕様等を事前に確認することでクラウド移行のリスクを把握しておく．

④運用自動化への取り組み

次世代エンドポイントセキュリティ対策製品では，運用負担を軽減するよう，プロダクト運用における作業を自動化するような機能を組み込む方針を持った製品がある．運用の品質を保つことができるのか，運用の管理は行えるのか等，十分に評価を行い，運用自動化について継続的に検討する．

5. お わ り に

本稿では，次世代エンドポイントセキュリティ対策製品の中でも EPP 製品の基盤構築や運用について事例を基に解説した．近年，エンドポイントのセキュリティ強化が謳われているが，EPP 製品や EDR 製品等の様々な製品が乱立しており，製品の選定が困難な状況である．さらに EPP 製品と EDR 製品は互いの機能の相互拡張を進めている過渡期でもある．次世代エンドポイントセキュリティ対策製品の導入においては，運用の自動化や EDR 機能の拡張など，製品のロードマップから製品の将来性について評価・選定を行い，運用の品質を保持しながら，製品の機能を充足させていくアプローチが重要である．将来的には，EDR 機能の拡張を行うことによりエンドポイント上で収集できるようになるログデータや，ネットワーク，クラウドといった様々なレイヤのポイントから収集したログデータを脅威インテリジェンスクラウドに集約し，相関分析や挙動分析を強化することで，より高度なサイバー攻撃にも対応できるセキュリティ基盤の構築を行っていく．単一のセキュリティ製品として一時的に評価，導入するだけではなく，将来の機能拡張やセキュリティ製品間の連携を踏まえ，中長期視野で成熟をさ

せていく視点が必要となる領域である．

自社への次世代エンドポイントセキュリティ対策製品の導入を検討している読者に対し，本稿が有益なものとなれば幸いである．

＊1 特定の組織（政府/公共サービス期間/企業など）内の情報を標的にしたサイバー攻撃．一般的に当該組織の構成員宛にマルウェアを組み込んだ電子メールなどを送り，攻撃を開始する．
＊2 感染した端末のデータを暗号化し，元に戻すことと引き換えに「身代金」を要求する悪意のあるプログラム．
＊3 OSやソフトウェア内部に存在する脆弱性を悪用した攻撃．
＊4 OSやソフトウェアの脆弱性が発見された後，修正プログラムが提供されるより前にその脆弱性を狙う攻撃．
＊5 判明している既存のマルウェアの情報が格納されたファイルをエージェントに配布し，これに合致するマルウェアを検知し，防御する製品．
＊6 判明している既存のマルウェアの情報が格納されたファイル．
＊7 検知した疑わしいファイルを動作させ悪意のある挙動が行われないかを分析するために構築された，攻撃されても被害を受けない隔離された環境
＊8 エンドポイント上で使用しているソフトウェアやファイルの動きを常時監視し，マルウェアの挙動を検知した瞬間に駆除，隔離，削除等の処理を実行する機能
＊9 単体では動作せず，他のプログラムの実行時に呼び出されて機能するプログラム
＊10 セキュリティ製品で検知したプログラムが，正常であると判断された場合，そのプログラムをホワイトリスト（無害なものリスト）に登録することで，その後検知されないように設定すること
＊11 組織内のセキュリティインシデントに対応するためのインシデント対応チーム．
＊12 サイバー攻撃の検出や分析を行う役割を持つ，自組織内で構築された部門や専門組織．
＊13 ITサービスマネジメントにおけるベストプラクティスをまとめた書籍群．

参考文献 ［1］ 情報セキュリティ10大脅威 2019～局面ごとにセキュリティ対策の最善手を～，独立行政法人情報処理推進機構，2009年4月
https://www.ipa.go.jp/files/000072668.pdf
［2］ 政府機関等の情報セキュリティ対策のための統一基準群の見直し（骨子），NISC（内閣サイバーセキュリティセンター），2018年4月
https://www.nisc.go.jp/conference/cs/dai17/pdf/17shiryou03.pdf

※ 上記参考文献に含まれるURLのリンク先は，2019年7月8日時点での存在を確認．

執筆者紹介 卯 月 義 文（Yoshinori Uzuki）
2004年日本ユニシス(株)入社．流通業向けアプリケーション開発にはじまり，クラウドサービスの提案支援や新サービス企画開発等を経験．2016年から社内情報システムの企画導入に従事．

岡　田　　遥（Haruka Okada）
2017年日本ユニシス(株)入社．情報システムサービス部にて社内情報システムにおける新規システムの企画・導入に従事．