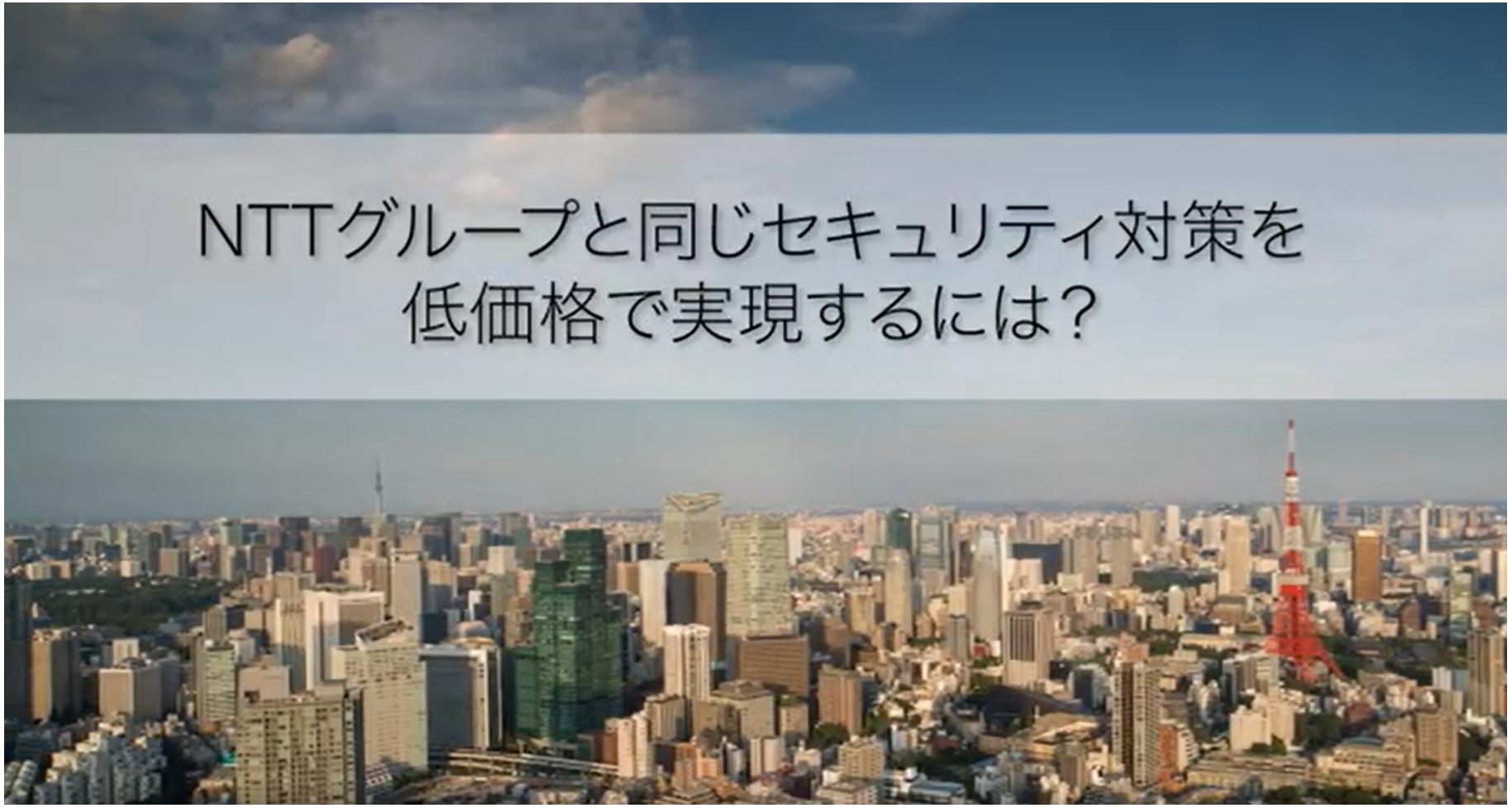
s-WorkProtector
（統合セキュリティサービス）

会社ネットワークから端末までセキュリティ運用をトータルサポート

s-WorkProtector紹介動画



https://youtu.be/if_C_l-OgCc

s-Work Protector

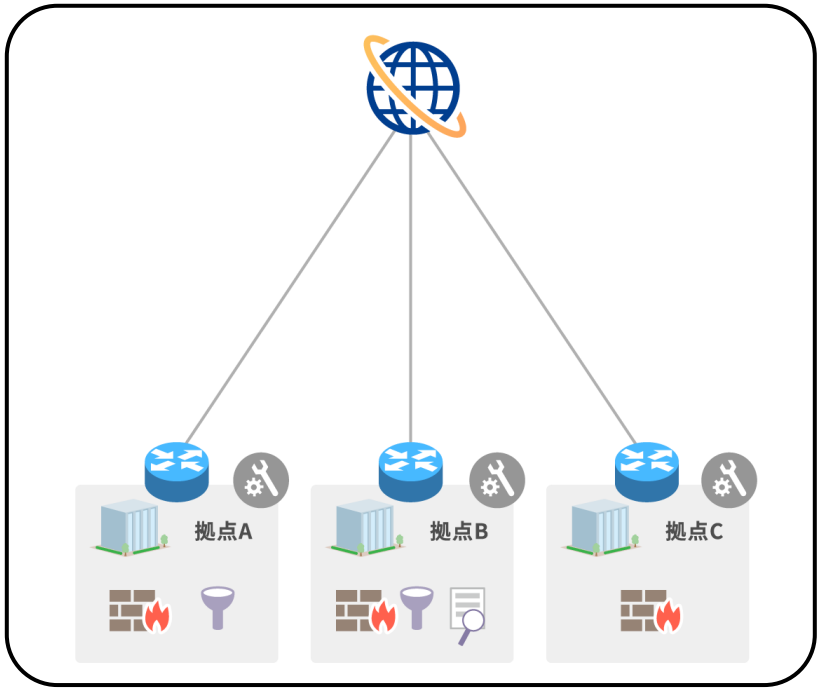
サービス概要

s-WorkProtectorとは

長年のドコモグループでの運用ノウハウで、貴社のセキュリティ運用をすべて代行します。
アプライアンス機器の設置や維持運用は不要です。

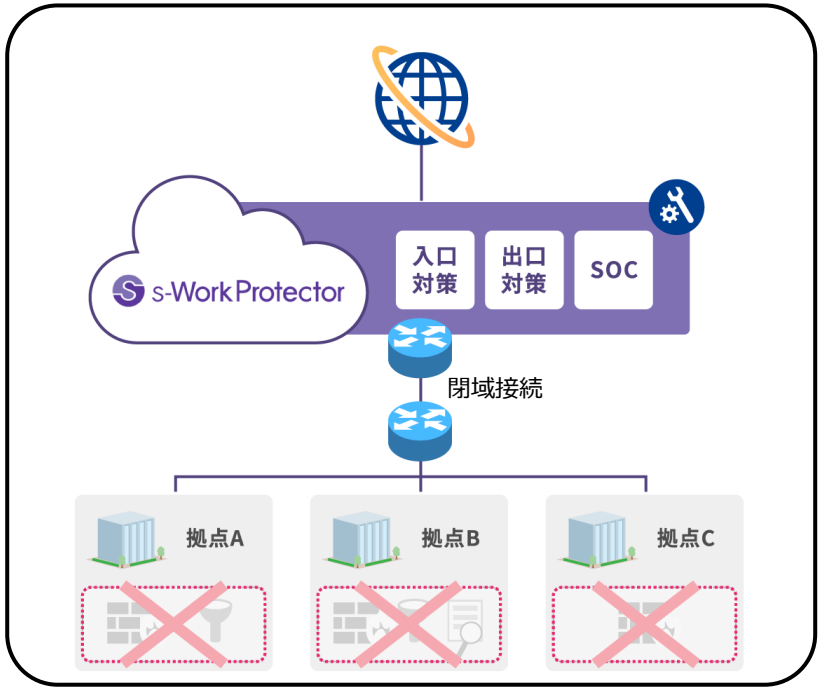
s-WorkProtector
導入前

- アプライアンス機器を拠点ごとに設置するため、機器の導入・運用の工数・コストがかさむ
- 拠点ごとにセキュリティ対策が統一されていない



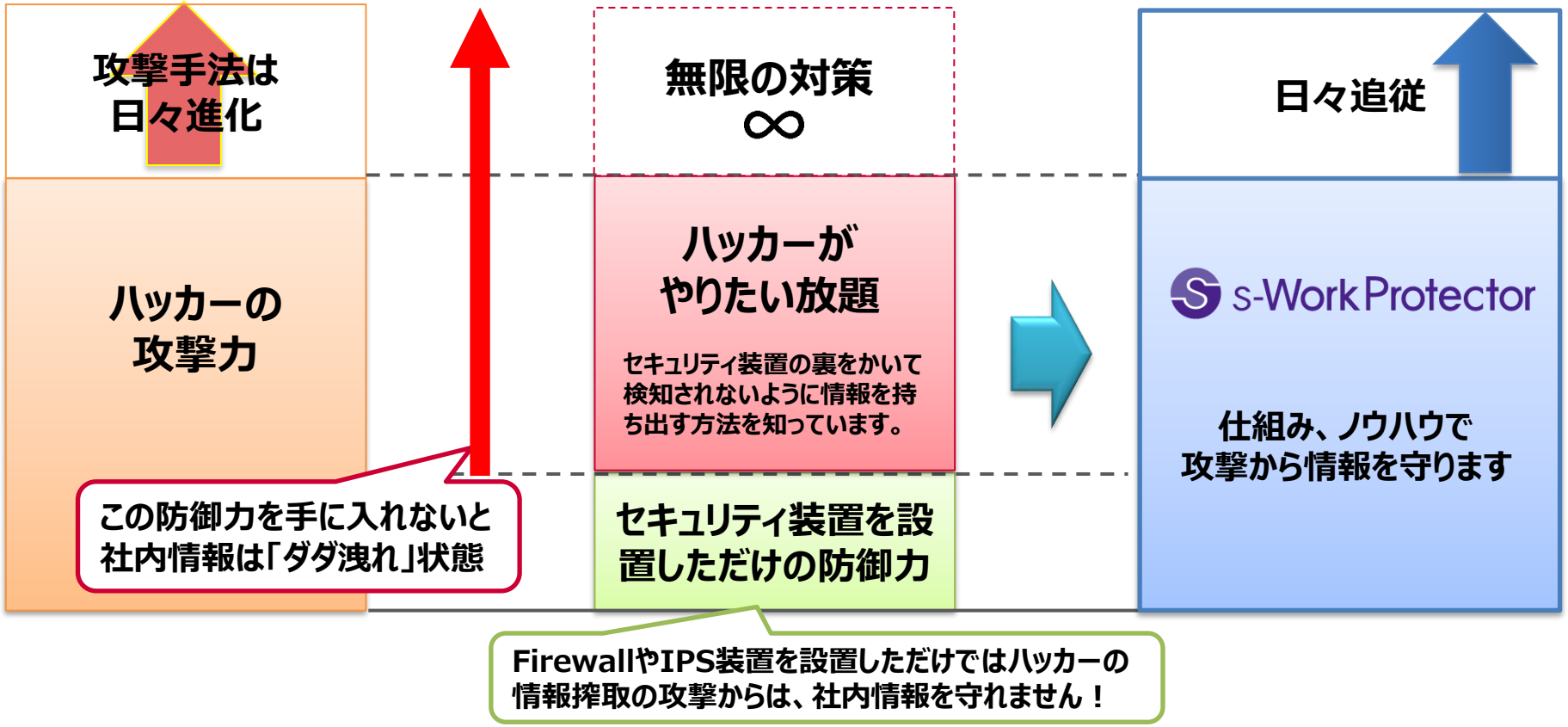
s-WorkProtector
導入後

- アプライアンス機器の設置不要で、機器の導入・運用の工数・コストを削減
- s-WorkProtector側から全拠点に同じレベルで最新のセキュリティ対策を実現



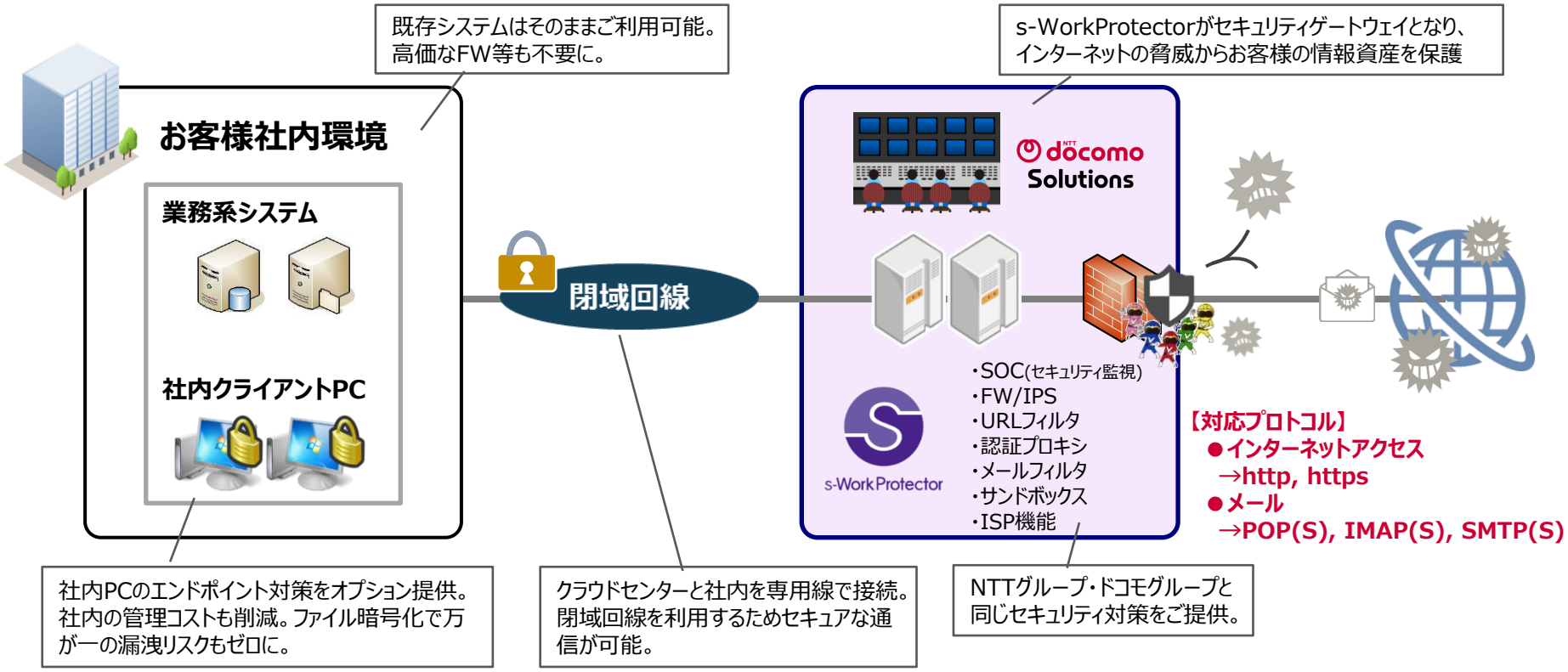
一般的なセキュリティ対策と問題点

攻撃手法は日々多様化し、対策には無限のコストが必要



必要な対策をオールインワンでご提供

「特定のプロダクト・メーカーに依存しない入口・出口対策、端末対策」、「SOCによるセキュリティ運用」を兼ね備えたセキュリティサービス

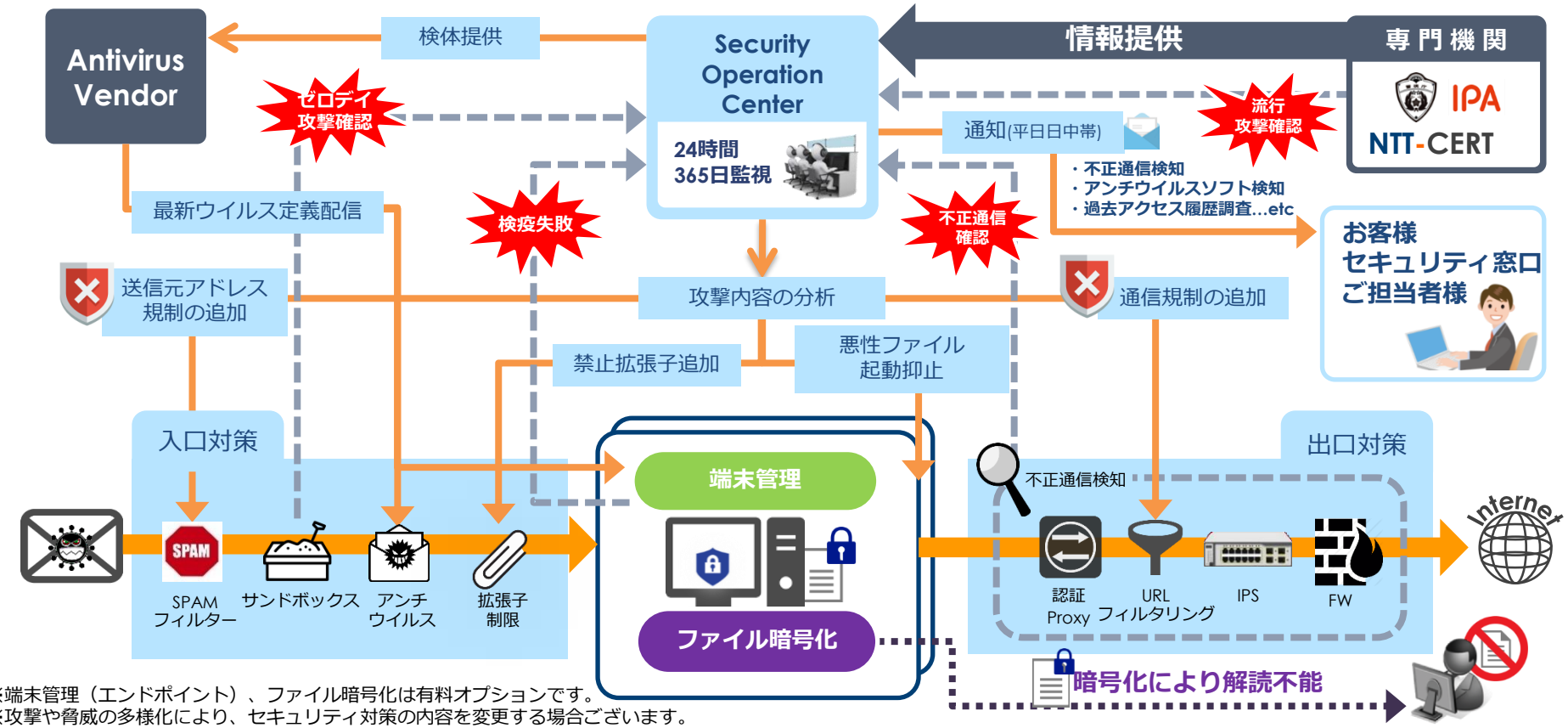


特長 1	入口出口対策からSOC機能まで標準提供。エンドポイントまで拡張も可能。
特長 2	SOCが入口出口対策を常に最新化。最新のセキュリティ脅威への対処も安心。
特長 3	クラウド型のためセキュリティ対策や運用を簡単にアウトソース。

23万人規模のSOC運用に裏付けられた信頼とノウハウ

s-WorkProtectorは、「特定のプロダクト・メーカーに依存しない入口・出口対策、端末対策」、「SOCによるセキュリティ運用」を合わせたセキュリティサービスです

多層防御によりセキュアな環境をご提供します。



※端末管理（エンドポイント）、ファイル暗号化は有料オプションです。
※攻撃や脅威の多様化により、セキュリティ対策の内容を変更する場合ございます。

入口対策機能のご紹介

	機能	概要
	**スパムメール対策**	スパムフィルタでは、主に以下の判定により悪性メールを検知・削除します。 ・IPレピュテーション / 第三者中継拒否 / 流量制限(IP・Fromアドレス・ホスト名でブロック) また、スパムメールが疑われるメールの件名に【SPAM】を付与し、注意喚起します。
	**メール添付ファイル 拡張子制限**	禁止拡張子制限では、禁止した拡張子の添付ファイルを削除します。 ※ご契約者様へは削除通知が付加されたメール本文が届きます。
	**ウイルスメール対策**	ウイルス対策(メールサーバ)では添付ファイルを駆除します。 ※ご契約者様へは削除通知が付加されたメール本文が届きます。
	**サンドボックス**	サンドボックス解析では、スパムフィルタを通過したメールのうち、 下記の悪性メールを検知します。 ・サンドボックス解析の結果、添付ファイルにマルウェアを含むメール ・既知の不正なURLを含むメール

出口対策機能のご紹介

機能	概要
IPS	不正通信を検知しパケットを自動で遮断します。
ファイアウォール	メールおよびインターネットアクセス(http/https)以外の通信をブロックします。
URLフィルタ	ホワイトリスト運用により、日々現れる脅威のあるサイト閲覧をさせない対策を実施しています。 検知や外部機関からの情報をもとに日々悪性URL情報をブラックリストに登録しています。
通信ログ分析・規制	Proxyサーバの通信ログを分析、不正な通信を規制します。
認証proxy	インターネットに接続する場合にユーザ認証(ID/パスワード)が必要なります。 添付ファイルのマクロ実行等による、ブラウザを経由せずに通信をしようとする場合ブロックされます。

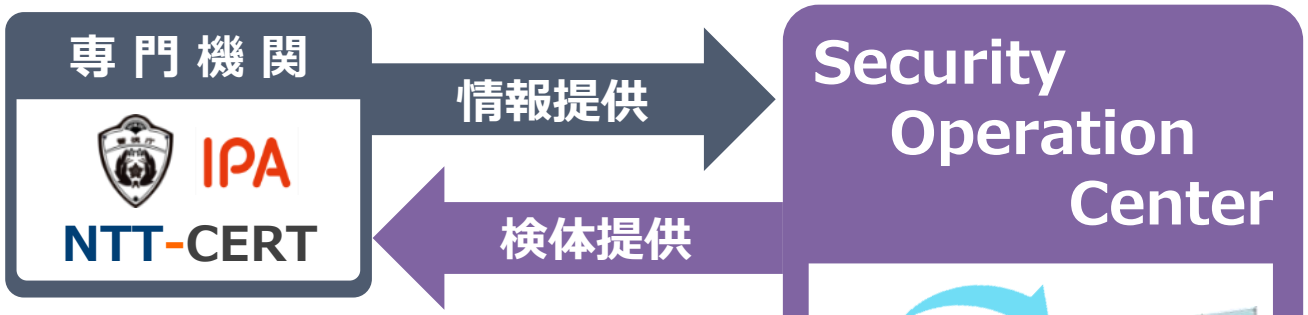
端末対策機能のご紹介

機能	概要
 **ウイルス対策**	PCにウイルス対策ソフトを提供し、継続的な更新を行います。 検知した検体はセキュリティベンダに提供し、ウイルス定義への早期反映を図ります。 また、検疫失敗を確認した場合はお客様に報告することで脅威残存を防止します。
 **パッチ自動適用**	Microsoftセキュリティ更新プログラム、Adobeバージョンアップなどの資材配布を自動で行います。
 **ソフトウェア起動抑止**	業務に不必要なソフトウェアや特定のアプリケーションを検出し使用またはインストールを禁止します。 ブラックリストにより不正とみなしたファイルの起動も抑止します。
 **ファイル自動暗号化**	クライアント端末内のデータを自動で暗号化します。 万が一、外部に漏れた場合も暗号化により解読不能。

SOC（Security Operation Center）のご紹介

機能	概要
専門機関との連携	日々検知したウイルスの検体をセキュリティベンダに提供することで、ウイルス定義への早期反映を図ります。
セキュリティ対策の最新化	発生している攻撃内容をSOCが解析し、入口/出口対策を最新化します。 ゼロデイ攻撃に対し、対策が最新化されるまでの空白期間をSOCがカバーします。 収集した情報をSOCが分析。規制すべきアドレスやURLを精査することで過検知・誤規制による業務影響を最小限にします。
セキュリティ資材の自動配布	Microsoftセキュリティ更新プログラム/Adobeバージョンアップを自動配布します。
月次レポート	毎月のセキュリティリスクを見える化し、レポートとしてご提供します。 お客様環境の不正通信やメール検知状況のサマリーからセキュリティリスクを評価し、推奨対応事項をご案内します。
通信ブロックの通知	不正な通信をブロック、不正なアプリの起動を抑止した場合にはお客様へ報告いたします。 ※該当端末の特定、アプリ起動抑止はオプションです。
ウィルス検疫の通知	アンチウイルスソフトによる検疫失敗を確認した場合は、お客様へ報告いたします。 検疫失敗を通知することで、対処漏れ（脅威残存）を防止します。 ※端末アンチウイルスソフトはオプションです。
アクセス履歴調査	外部専門機関からの情報入手時や、不正URLアクセス検知時に該当URLの過去アクセス履歴を調査し、検知洩れを防止します。アクセス履歴があった場合は、通信の成否や情報漏えいの有無を特定し報告いたします。 ※該当端末の特定はオプションです。

24時間365日監視で多様なサイバー攻撃に対応するSOC



Point

様々な外部の専門機関から情報を収集。
検知した検体は日次で外部の専門機関に連携。

Point

システムでの自動検知に加え、ログデータの収集や独自の分析ツールとアナリストによる相関分析を実施。

不正通信検知やメール検知状況、クライアントへの資材適用状況などを提供します。

Point

セキュリティ専任担当による24時間365日のシステム監視とインシデント対応

Point

問題点の把握、適切な対策・検証、次のアクションと言った、PDCAを継続的に回すことで、常に最新のセキュリティレベルを維持します。

月1回のセキュリティレポートにより、セキュリティ脅威への対処状況を可視化

資材適用状況収集　端末管理オプション

■ Microsoft®セキュリティ更新プログラム適用状況

WSUSによる配布が正常に行われていることの確認として、セキュリティ更新プログラムの適用状況をご報告いたします。適用状況は以下の通りです。

	前月配布分	当月配布分
配布開始日	yyyy年mm月dd日	yyyy年mm月dd日
データ抽出日	yyyy年mm月20日	yyyy年mm月05日
適用済み端末数	85	70
未適用端末数	15	30
適用率	85.00%	70.00%

セキュリティトピック

セキュリティ設定のチューニング状況等をトピックとして掲載します

トピック

参考として、当月のセキュリティ関連トピックを記載致します。
各トピックの詳細は、別途送付しております各通知内容をご参照ください。

■ セキュリティ設定のチューニング実施状況

yyyy年mm月dd日	禁止拡張子追加(xxx)

メール検知状況収集

■ 貴社の悪性メール検知状況(サンドボックス解析)

貴社の悪性メール検知状況(サンドボックス解析)を抜粋したものは、以下の通りです。

③検知数	80

不正通信発生状況収集

■ 不正通信検知状況(相関分析/システム検知/過去アクセス履歴)

貴組合の不正通信検知状況は以下の通りです。

相関分析	Critical	0
	Serious	1
	Medium	0
	Informational	0
システム検知	C&Cサーバへの外部通信	1
	悪意のあるURLへのアクセス	0
	攻撃コードの検出	0
	C&Cサーバへの名前解決	2
	悪意のあるファイルのダウンロード	0
過去アクセス履歴	-	1

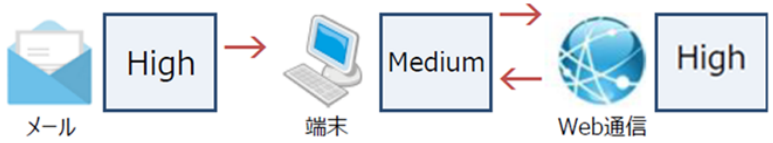
セキュリティリスク評価

セキュリティリスク評価

本レポート期間中における、貴社dDREAMS利用状況のセキュリティリスク評価は以下の通りです。

セキュリティリスクを評価し推奨対応事項をご案内します

セキュリティリスク



ファイルの暗号化

どんな対策を施しても、情報流出のリスクはゼロにはならない
万が一のファイル流出に備え、ファイルの自動暗号化で情報漏洩を抑止

安心のポイント①

- **ファイル保存時に自動で暗号化**
  クライアント端末にファイルを保存した直後に自動で暗号化されます。なお、暗号化は、システム管理者が指定した所定のフォルダでのみ解除することができます。

安心のポイント②

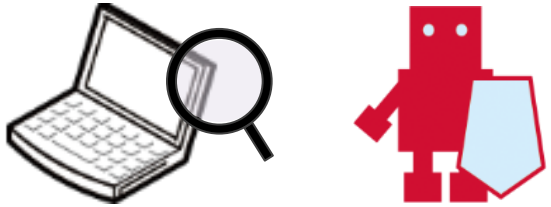
- **常に暗号化した状態でファイルの操作が可能**
  暗号化したファイルは、s-WorkProtector端末であれば誰でもそのまま参照や編集が可能です。

安心のポイント③

- **s-WorkProtector端末以外ではファイルを開けません**
  暗号化したファイルは、s-WorkProtector端末以外で開くことは出来ません。なお、 s-WorkProtector端末でもファイル暗号化機能がインストールされていない場合は、ファイルを開くことが出来ません。

その他

- **巡回ツールについて**
  巡回ツールで、定期的に端末内を検索し、保護対象のファイルを探し出します。
  保護対象を発見した場合、自動で暗号化を行います。



EDR（Endpoint Detection and Response）

従来のアンチウィルソフトのパターンマッチング方式では検知できない未知のマルウェア(例：ファイルレスマルウェア)や端末と端末間のやり取り(横展開)を、端末上の振る舞いから 検知することが可能。

さらに、
・エンドポイント端末の情報(ファイルやプロセスの挙動/レジストリ変更/ネットワーク通信情報等)収集可能
・エンドポイント端末の隔離、攻撃経路や感染範囲の特定、端末の修復を行うことができる

サービス利用料

お客様のニーズに合わせ、3つのサービス提供プランを用意

Basicプラン

・セキュアインターネットGW
　不正通信による情報漏えいや外部からの不正アタックをブロック

・メールフィルタ
　マルウェア感染リスクの軽減やメールによる情報漏えい対策

ファイル暗号化オプション

メールフィルタ | 端末管理オプション

セキュアインターネットGW

セキュリティオペレーションセンタ

月額 ¥950/id

Basicプラン(＋オプション)

・端末管理オプション
　ランサムウェアなどの拡散リストの軽減

ファイル暗号化オプション

メールフィルタ | 端末管理オプション

セキュアインターネットGW

セキュリティオペレーションセンタ

月額 ¥2,450/id

Premiumプラン

・ファイル暗号化
　万が一、外部にファイルが持ち出された場合も暗号化による情報漏えいを抑制

ファイル暗号化オプション

メールフィルタ | 端末管理オプション

セキュアインターネットGW

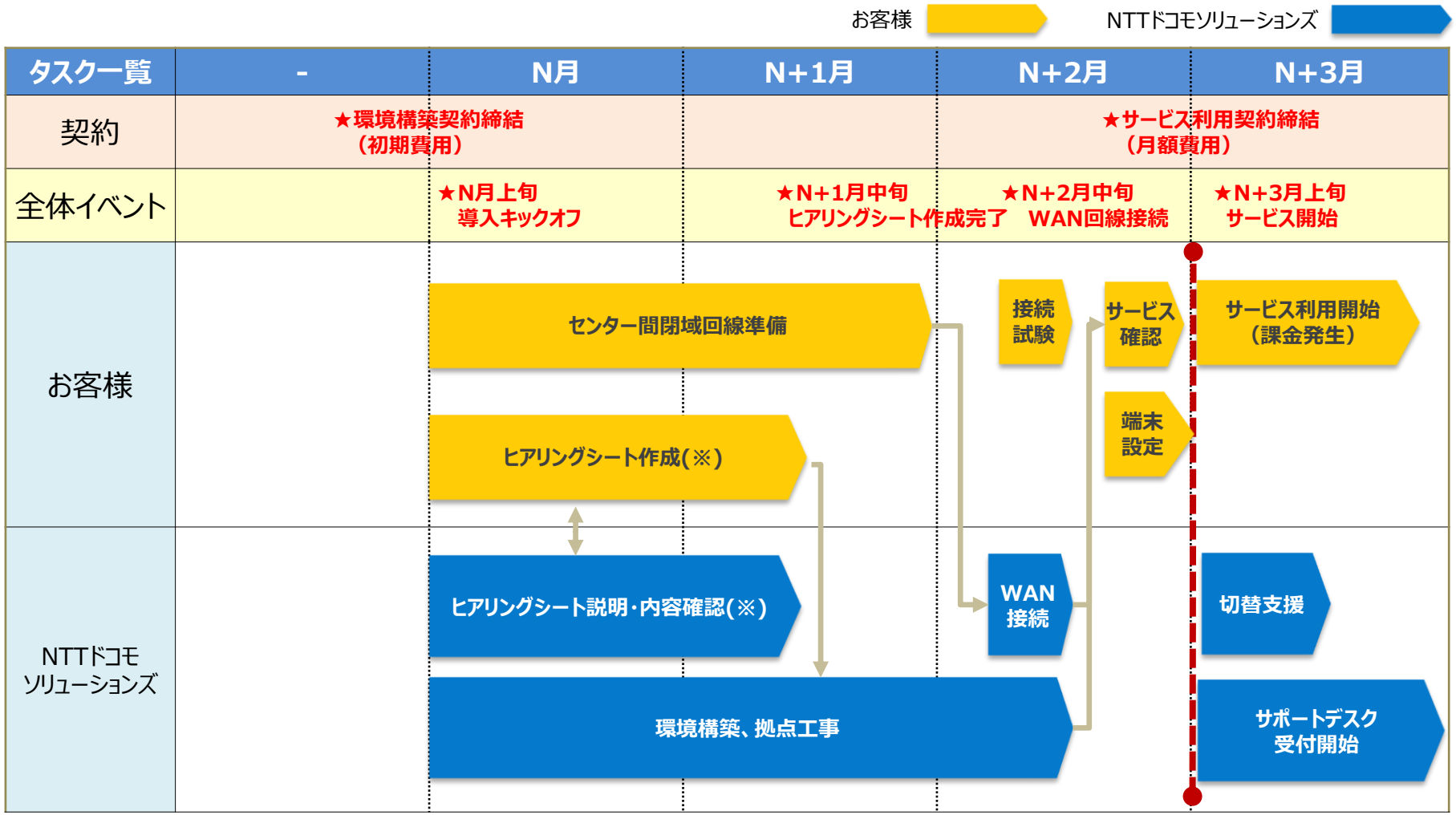
セキュリティオペレーションセンタ

月額 ¥3,600/id

EDR　￥300～￥740/id

※別途環境構築等の初期費用をご請求させていただきます。

ご契約から、最短3ヶ月でのサービス開始



（※）環境構築における設定値をヒアリングシートに記入いただきます。（期限はキックオフ時にWBSで提示）