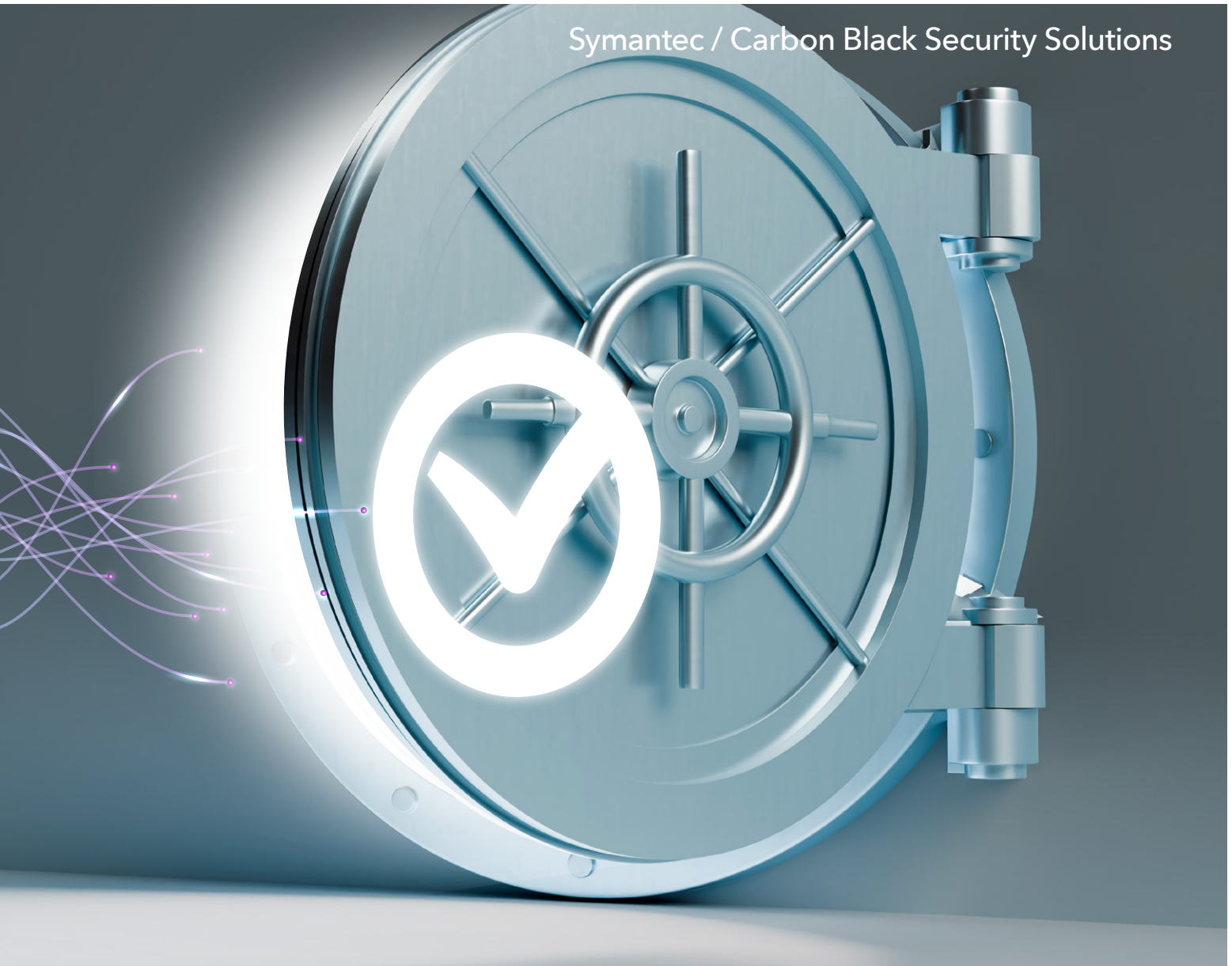


シマンテック/カーボンブラック 製品カタログ

Symantec / Carbon Black Security Solutions



DX化をはじめとしたビジネスの推進において サイバーセキュリティ対策は 避けて通れない重要な課題です

迅速な導入・展開や柔軟な拡張性を可能とするとともに、
運用コストを削減するクラウド活用は今のビジネスでは当たり前になっています。
また、働き方改革により、オフィスという場所に縛られない働き方も一般的になりました。
このようにビジネスの環境が大きく変わる中で、課題となっているのがサイバーセキュリティ対策です。
サイバーセキュリティの脅威は近年ますます高まるばかりです。
シマンテックとカーボンブラックのセキュリティ製品は
さまざまなセキュリティの脅威からお客さまを守ります。



ウイルス対策ソフトは導入していますが、
未知のマルウェアや攻撃に
迅速に対応できるか不安です。

SES

04
ページ

エンドポイント（パソコンやスマホ）を
マルウェアから保護します
エンドポイントセキュリティ
Symantec Endpoint Security (SES)



Webサービスの利用が増えています。
社員が脅威のあるサイトへ
アクセスしないか心配です。

WPS

06
ページ

Webサイトへのアクセスを監視・制御
して、ユーザーとデータを守ります
Webセキュリティ
Symantec Web Protection Suite (WPS)



機密データが破損・盗難に遭うと業務が
停滞し、経営に大きなダメージを与えます。
機密データの破損・盗難が心配です。

DLP

07
ページ

機密データの流出を監視・防止します
データセキュリティ
Symantec Data Loss Prevention



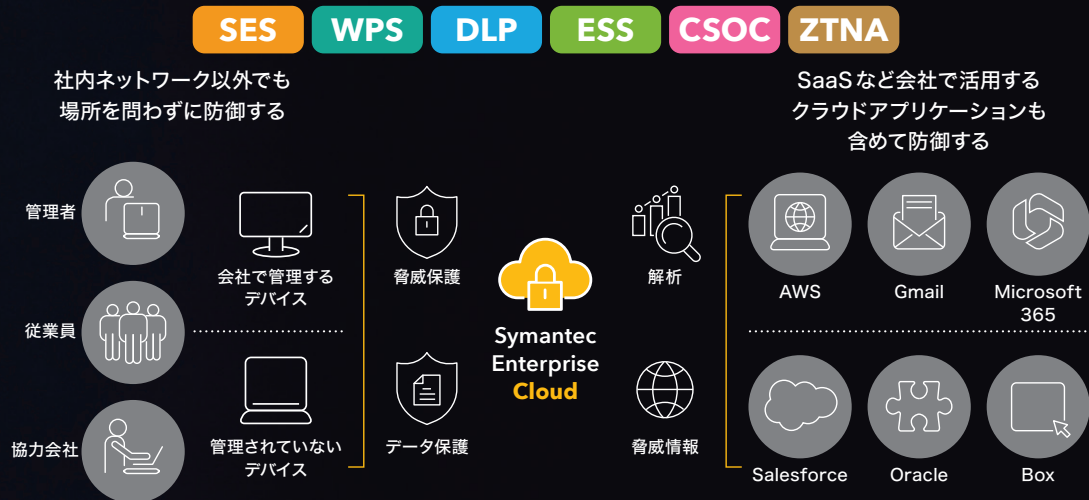
ランサムウェア攻撃や標的型攻撃が増えて
いるようです。また、スパムメールを止めて
業務効率を下げない対策も必要です。

ESS

08
ページ

メールからの攻撃（ランサムウェアや
標的型攻撃）を防御します
メールセキュリティ
Symantec Email Security.Cloud Service (ESS)

クラウドで実現できる防御機能



社内サーバー（オンプレミス）でも 運用できる防御機能



クラウドでの作業が増えています。
社員がクラウドベースのシャドーアプリで
事故に遭わないか心配です。



クラウド内のセキュリティ事故に
迅速に対応できます
クラウドセキュリティ
Symantec CloudSOC



テレワークでのクラウド利用がますます
増えています。VPNを導入していますが、
より安全なネットワークが必要です。



VPNに代わって安全にユーザーを
接続します
リモートアクセスセキュリティ
Symantec Zero Trust Network Access



パソコンの新規導入とOSの移行時に、多量
のパソコンに必要なソフトをインストール
したり、設定したりする作業が大変です。



キッティングの手間と時間を大幅に
削減します。
クローニングツール
Symantec Ghost Solution Suite (GSS)



少人数でさまざまな
セキュリティ対策を講じ、
運用するのは困難です。



EDRを中核に、未知の脅威まで検知・
防御できる高度な保護を提供します
EDR
Carbon Black EDR & Endpoint Security

Symantec Endpoint Security SES

多層防御機能でサイバー攻撃から保護



➤ エンドポイントセキュリティ

エンドポイント（パソコンやスマホ）をマルウェアから保護します。

パソコン、スマホ、サーバーなどのエンドポイントを最先端の多層防御機能であらゆるサイバー攻撃から保護。

オンプレミス/クラウド/ハイブリッドのいずれの環境にも対応します。

■ シマンテックエンドポイント製品の比較

		SEP	SES エンタープライズ	SES コンプリート
システム要件	対象端末	パソコン・サーバー	パソコン・サーバー・モバイル	
	対象OS	Windows OS, Mac OS, Linux	Windows OS, Mac OS, Linux, iOS, Android	
	運用方式	オンプレミス	オンプレミス、クラウド、ハイブリッド	
防御機能	EPP & NGAV	●	●	●
	安全なネットワーク	●	●	●
	USBデバイス管理機能	●	●	●
	1エージェント1コンソール	●	●	●
	モバイル対策	—	●	●
	適応型保護	—	—	●
	EDR	—	—	●
	脅威ハンティングサービス	—	—	●
	Active Directoryの保護	—	—	●

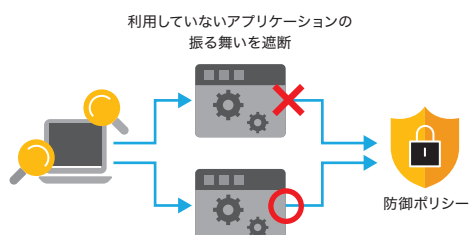
SEP: シマンテックエンドポイントプロテクション、EPP: エンドポイント保護プラットフォーム、NGAV: 次世代ウイルス対策、EDR: エンドポイント攻撃検知・対応

■ 独自機能の保護

環境に合わせた防御ポリシー設定をサポート

適応型保護

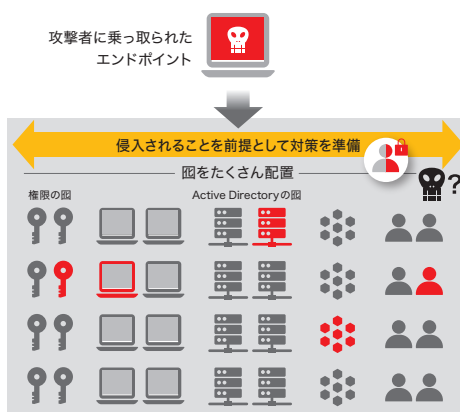
お客様のご利用環境を90日間学習し、攻撃の踏み台にされるツールや振る舞いを「見える化」します。利用状況と脅威情報を照らし合わせてお客様それぞれに合わせた防御ポリシーを提案します。



管理者情報を守り情報流出を防ぐ

Active Directoryの保護

偽の情報（ID、サーバー）を表示し、攻撃者を絡めとり、ADを保護。管理者情報の乗っ取り、ラテラルムーブメント（横展開）を防止します。



全てのデバイスとOSで
業界最高レベルの
保護を実現



Windows OS, Mac OS, Linux,
iOS, Android対応

全ての機能は1つの
エージェントで利用可能



複数社製品でセキュリティを構築
した場合、平均7つのエージェント
が必要となり、管理コストがか
さむ

クラウドの
セキュリティ管理を実現



管理サーバー不要で総コストを抑
えられます。オンプレミスとクラ
ウドを組み合わせたハイブリッド
も管理できます。

Carbon Black EDR & Endpoint Security

Carbon Black

未知の脅威まで検知・防御



EDR

EDRを中核に、未知の脅威まで検知・防御できる高度な保護を提供します。

あらゆるアクティビティデータを継続的に収集・可視化し、迅速な調査・対処を可能にする可視性の高さが強みです。

統合エージェントと統合コンソールによるシンプルな運用で、環境を問わずセキュリティを一元管理できます。

Carbon Black Endpoint & Workload

- EDRで既知・未知の脅威を高度に検知・防御し、攻撃の全体像を可視化
- 単一エージェントと統合コンソールでセキュリティ運用を簡素化
- 仮想マシンの脆弱性管理・挙動監視・EDRを統合的に提供し、運用負荷を削減

Carbon Black エンドポイント製品の比較

提供機能	Foundations 予防	Advanced + リスクを特定する	Enterprise + 脅威ハンティング
NGAV	●	●	●
行動ベースの EDR - Behavioral EDR	●	●	●
デバイス制御 - Device Control	●	●	●
ライブクエリ - Live Query		●	●
脆弱性管理 - Vulnerability Management		●	●
エンタープライズ EDR - Enterprise EDR			●

Carbon Black Workloads 製品の比較

提供機能	Foundations 予防	Advanced + リスクを特定する	Enterprise + 脅威ハンティング
資産インベントリ - Asset Inventory	●	●	●
ライブクエリ - Live Query	●	●	●
CIS ベンチマーク - CIS Benchmarks	●	●	●
vCenter プラグイン - vCenter Plug-in	●	●	●
ライフサイクル管理 - Lifecycle Management	●	●	●
脆弱性管理 - Vulnerability Management	●	●	●
NGAV		●	●
行動ベースの EDR - Behavioral EDR		●	●
エンタープライズ EDR - Enterprise EDR			●

Carbon Black のオンプレミス用製品

Carbon Black EDR

- 高度なエンドポイント検知、スレットハンティング、フォレンジック調査を実現
- 攻撃チェーン全体の記録とオンプレミスでのデータ管理
- 正確な調査、根本原因の特定、迅速な封じ込めを可能に
- 規制対応環境、エアギャップ環境、データ主権が求められる環境に最適

Carbon Black App Control

- デフォルト拒否のホワイトリスト方式で、信頼済みアプリのみを重要システムで実行可能に
- 豊富な信頼情報に基づくデフォルト拒否モデル（単純なハッシュ管理ではない）
- 信頼されていないコードの実行を未然に防止
- インシデント数とSOC 負荷を大幅に削減し、レガシー／重要システムを保護

クラウドネイティブな
EDR、分析機能を
単一プラットフォームで
提供



高度な
エンドポイント検知、
スレットハンティング、
フォレンジック調査を実現



アプリケーションの
ホワイトリストリングと
システムロックダウン
(App Control)



Symantec Web Protection Suite WPS

Webサイトへのアクセスを監視・制御



Webセキュリティ

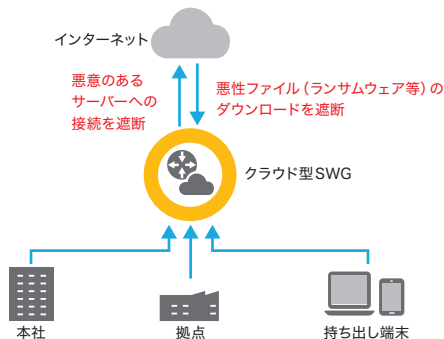
Webサイトへのアクセスを監視・制御して、ユーザーとデータを守ります。

クラウドアプリケーションやWebサービスに安全にアクセスするための機能を集約して提供するサービス SSE (Security Service Edge)。

Webセキュリティの根幹となるSWG (セキュアWebゲートウェイ) の各種機能をオールインワンパッケージで提供します。

オンプレミス/クラウド/ハイブリッドのいずれの環境にも対応します。

Web経路の脅威を多層的に防御するWPS



> URLフィルタリング

悪性URLへの接続を遮断

> アンチウイルス

既知の悪性ファイルのダウンロードの遮断

> サンドボックス

未知の疑わしいファイルをエミュレート

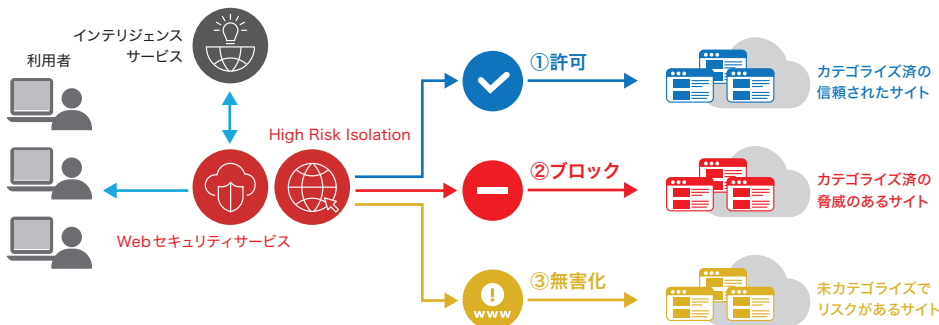
> Web分離

一定のリスクレベルを超えるWebサイトを安全なコンテナ内でレンダリングし、ユーザーにインタラクティブなグラフィックファイルのみを提供

同カテゴリで、
他社製品を圧倒する
フィルタリング検知精度



セキュリティとユーザビリティを両立する自動Web分離機能

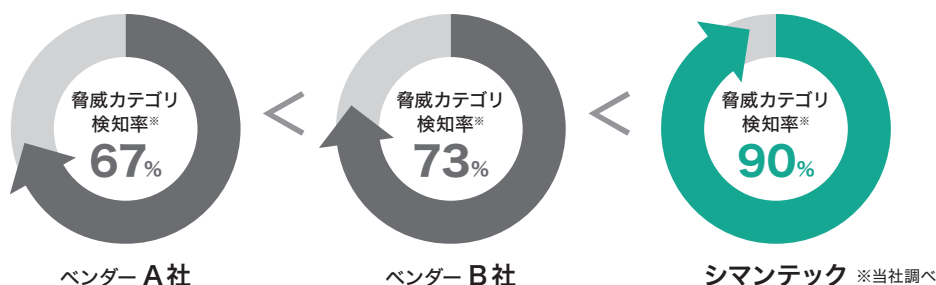


強固な
セキュリティレベルと
ユーザビリティを両立した
自動Web分離機能



Symantec Cloud SWGと競合他社の URLフィルタリング機能を比較

Symantec Cloud SWGのURLフィルタリング機能では、フィッシングサイトやマルウェア配布サイト等の疑わしいサイト (脅威カテゴリ) を高確率で検知。



Symantec Data Loss Prevention DLP

機密データの流出を監視・防止



データセキュリティ

SES、CloudSOCなどの各ソリューションとの連携により機密データを検知・保護します。
オンプレミス/クラウドのどちらの環境にも対応。ストレージ・メール・ネットワーク・エンドポイント・クラウドなど
さまざまな流出経路での機密データの漏洩を防ぎます。

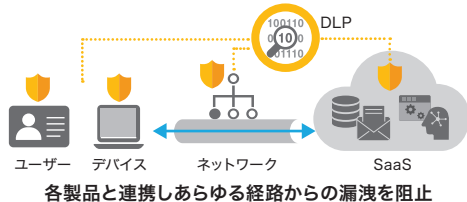
■ SaaS利用の加速で情報漏洩の発生リスクが上昇

現状のゼロトラストセキュリティの問題点

ユーザー 認証による管理	従業員の情報流出 従業員による情報持ち出しを 管理できない
デバイス デバイスの挙動を 監視	誤操作/誤送信 マルウェアではなく人間起因に よるインシデントに対応できない
ネットワーク 通信/操作の制御	SaaSの機能制限 制限による対策はSaaSの 利便性を損なってしまう

解決策 ゼロトラストにデータセキュリティを追加

データ自体の監視/保護を行うDLPが有効



各製品と連携しあらゆる経路からの漏洩を阻止

SymantecDLPで課題を解決

課題	解決策
従業員の 情報流出 ユーザー	外部向けの重要データ送信を制限 通信を精査し機密データが含まれる 通信を制限 WPS & DLP
誤操作/誤送信 ユーザー	機密データの検知をシステム化 許可のない機密データ送信を 検知/遮断 ESS & DLP
SaaSの機能制限 	SaaS上の機密データを詳細制御 機密データを制御して セキュリティと利便性を両立 API連携

豊富な検知手法と 日本向けテンプレート



- インデックス検出に加え、画像
様式検出など豊富な検知手法
- ユースケースごとに設定テン
プレートを提供

豊富な 国内導入実績



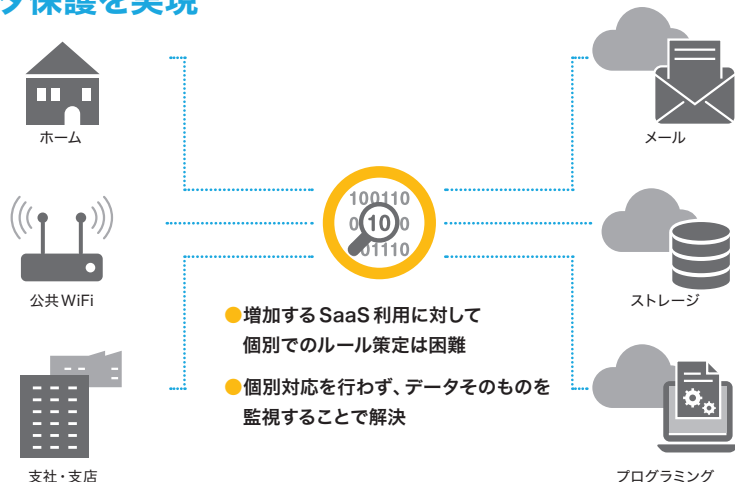
- 大手金融機関
- エネルギー
- ヘルスケア など

高い運用性



- わかりやすい
ユーザーインターフェース
- 完全日本語ドキュメント
- 運用支援サービス

■ 利用SaaS全てに共通ポリシーを包括的に適用し データ保護を実現



Symantec Email Security.Cloud Service ESS

ランサムウェア攻撃などから保護

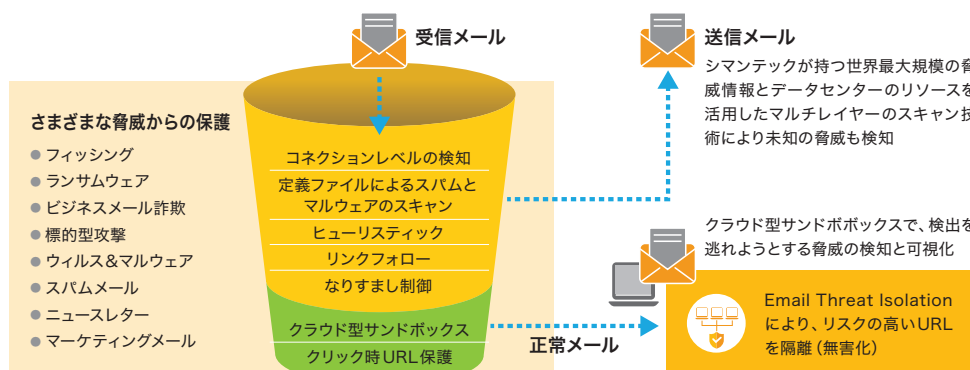


メールセキュリティ

メールからの攻撃（ランサムウェアや標的型攻撃）を防御します。
世界トップレベルの評価を受けている多層防御メールセキュリティサービスです。
クラウド型なので新たにサーバーを準備する必要がなくすぐに導入できます。

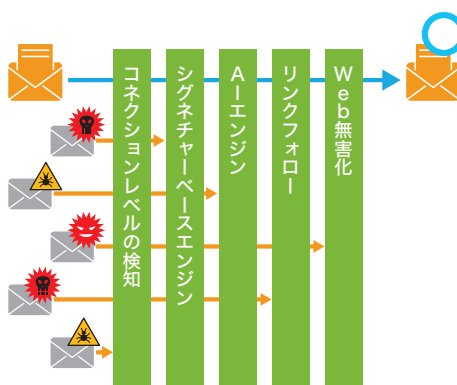
ESSの提供機能

メールの受信ルートにシマンテックのデータセンターを経由させることで、全てのメールをスキャンし、安全なメールもしくは脅威を排除したメールをお届けすることができます。



シマンテックのデータセンターを経由することで脅威のあるメールを排除

ウイルス保護の有効性でSLA保証を提供しています。SLAにてメールウイルス保護100%(未知ウイルスを含む)、稼働率100%を保証します。さまざまなセキュリティ対策技術を利用して、安全なメールのみをお客様に配信します。



導入が容易 管理者ポータルで 一元管理



シマンテックのクラウドインフラを利用するため、導入も簡単に運用コストを大幅に削減できます

クラウド型の 多層防御システム



多層防御システムをクラウド上に実装。より高い精度でメール脅威を検知します

導入時の作業

- メールサーバーのDNS情報内のMXレコードの設定変更(制限がある場合)
- メールサーバー側の送受信設定／ファイアーウォールの設定変更

便利な管理ポータル

管理者用ポータルサイトでは、スパム、ウイルス等の状況や、必要な情報の確認や設定、レポート作成ができます。管理者の運用負荷を軽減します。



トップレベルの実績



全世界で約32,000社／1,400万人が利用。国内でも多くの企業で導入いただいています

Symantec CloudSOC

シャドー IT 対策に

クラウドセキュリティ

クラウド内のセキュリティ事故に迅速に対応できます。クラウドアプリケーションの利用状況の可視化や制御を実施。約100のサンクションアプリに加え、約40,000のシャドーアプリに対応。ユーザーの振る舞い分析による情報漏洩も検知します。

Symantec CloudSOCの主な機能



クラウドアプリの利用を可視化

組織内のシャドー ITを発見し、数千のアプリケーション全体で深い可視性を備え、アプリケーションとデータが全てのコンプライアンス要件 (EUの定めたGDPR、医療業界のHIPAA 等) を満たしているかどうかを評価します。



機密データの保護

クラウドに保存されている機密データを正確にモニターし、偶発的な損失や内部者の盗難から保護します。



機密データの検知と制御

ファイル名ではなく情報の中身で情報種別を特定し、リアルタイムにポリシー違反を検出/制御を行うことで情報漏洩を防止します。

業界トップレベルのアプリケーション検出数



閾値や機械学習を用いた
ユーザー振る舞い検知

Symantec CloudSOCのCASB機能

シャドー IT 対策

- クラウドアプリケーションの安全性評価
- クラウドアプリケーションの利用状況の可視化と評価
- SWGと連携した確実なWebアクセスコントロール
- 40,000以上のクラウドアプリケーションに対応

サンクションIT対策

- シャドーデータの可視化と制御
- デフォルトで100以上のクラウドアプリケーションに対応
- SWG連携を用いたクラウドアプリケーション制御



閾値や機械学習を用いた ユーザー振る舞い検知



導入ステップ

シャドー IT 対策 (ステップ1)



サンクションIT対策 (ステップ2)



クラウドSWG連携によるリアルタイムアクセスコントロール



Symantec Zero Trust Network Access ZTNA

より安全なネットワーク環境構築



▶ リモートアクセスセキュリティ

VPNに代わって安全にユーザーを接続します。

リモート環境から社内サーバーやその他の社内リソースへの安全なアクセスを実現します。
ゼロトラストの新しい概念であるソフトウェア定義境界 (SDP) により、
エージェントがインストールされていないデバイスからのアクセスもセキュアに対応します。

■ Symantec ZTNAは次の3つを実現

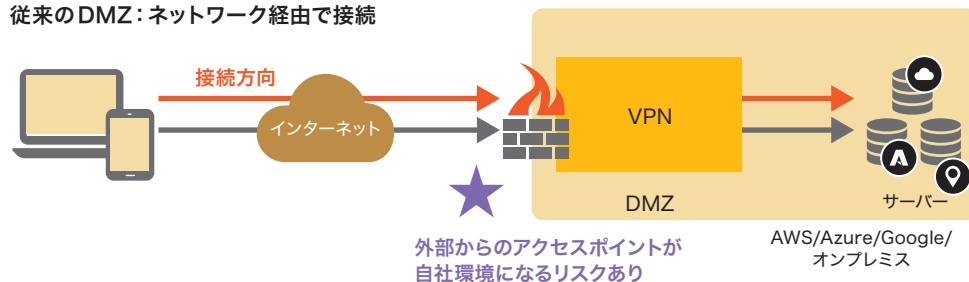
特定の「アプリ」だけに繋ぐ
最小権限のアクセスを実現

「動的」な情報を検知
(例: 端末脅威、ユーザー状況)

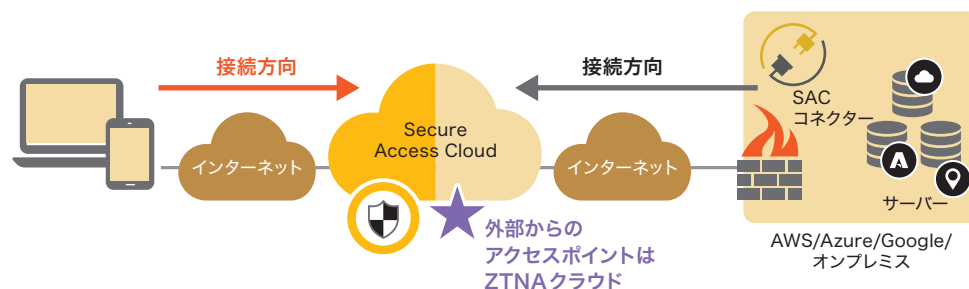
クラウド経由でのアクセスの
ため、**直接の攻撃起点無し**

■ VPNのリスクを構造で回避

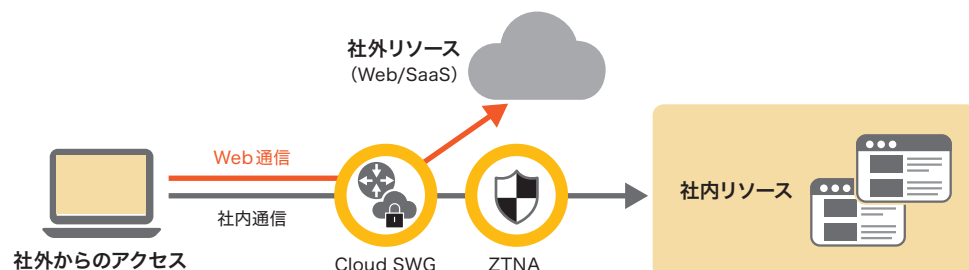
従来のDMZ: ネットワーク経由で接続



Symantec Secure Access Cloud - SDPベースのクラウドネイティブ接続



■ Cloud SWGとの連携により、 徹底したアクセスコントロールを実現



最小権限での
アクセスを実現



特定のアプリにだけ接続を許可

要望に応じて
エージェントモード/
エージェントレスモード
を選択可能



- 差分はプロトコル権限の有無のみ
- 委託会社や外部の社員に対しても柔軟に設計可能

Google Cloud Platform
上で設計された
ソリューションにより
スループットが向上



スムーズに自社リソースにアクセ
ス可能

Symantec Ghost Solution Suite GSS

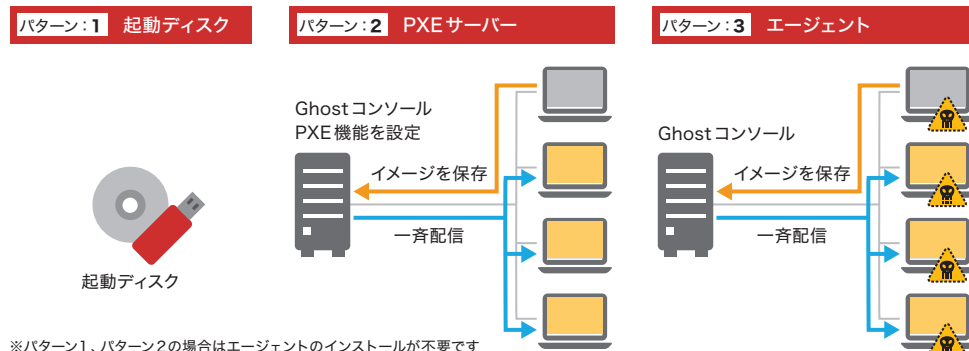
キッティングの手間と時間を大幅に削減



➤ クローニングツール

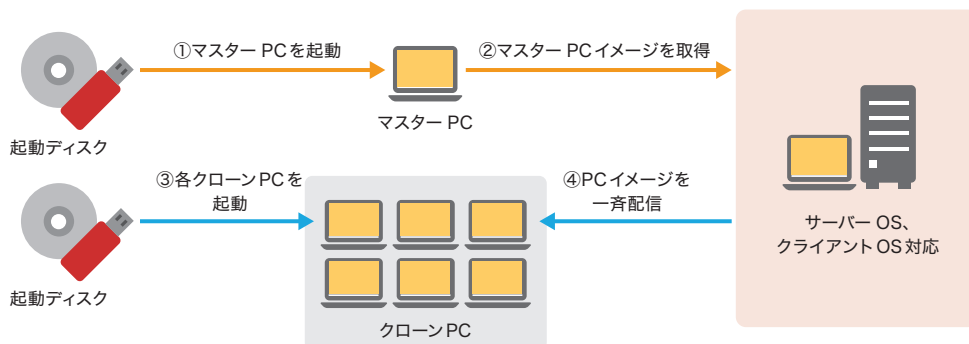
GSSは、マスターとなるパソコンと同じ構成を作成するクローニングツールです。
パソコンの新規導入やOSの移行などを一括設定することで、
キッティングの手間と時間を大幅に削減します。

■ クローニング方法



クローニングフロー例 パターン:1 起動ディスク

起動ディスクでマスターとなるパソコンを起動し、イメージを取得。クローン対象パソコンとGhostキャストサーバーをネットワーク接続し、大量の複製を行います。各パソコンにエージェントのインストールは不要です



■ 資産管理・データ消去 (Gdisk)

Ghostの管理コンソールで、社内パソコンの一元管理を実現します。パソコンの仕様やCPU、メモリーサイズ、ディスクの空き容量、OSのセキュリティ更新プログラムが正常にインストールされているかなど、ソフトウェア・ハードウェアイベントリ収集機能でネットワーク上のパソコンをチェックできます。また、付属のGdisk (米国国防総省準拠のツール) を使用することで、パソコン廃棄時に、企業内部情報や個人情報を完全に消去します。

環境に合わせた3種類のクローニング手法を用意



企業の環境に合わせて、3つのパターンから最適な手法を選べます

作業ミス防止、設定漏れ防止

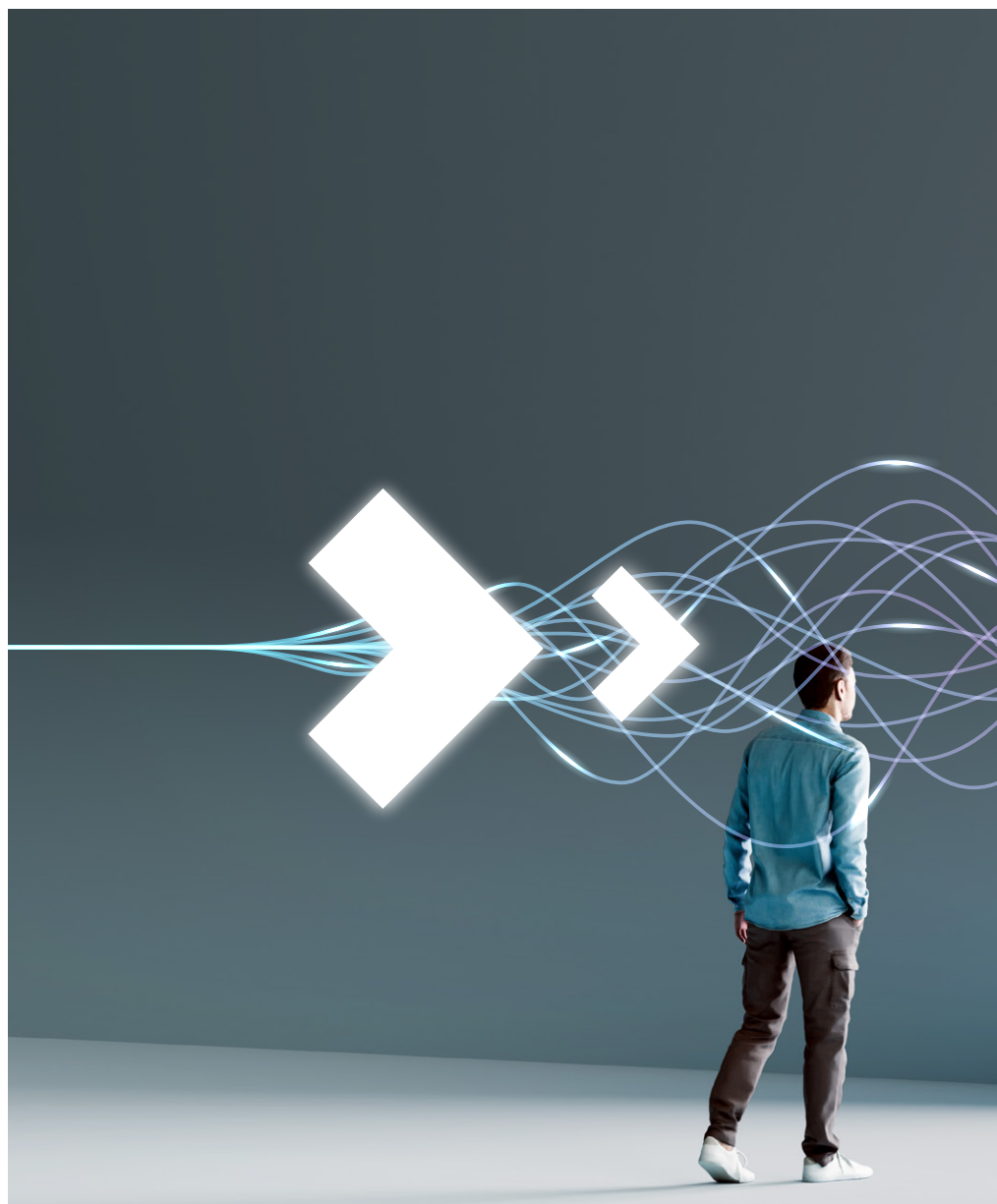


マスター PC を丸ごと複製するため、設定時の作業ミスや設定漏れのパソコンの発生を防止します

脆弱性パッチの適用やOSの移行、廃棄も安全に



ユーザー変更・アプリケーション更新・OSアップデート・脆弱性パッチの適用も一括配信



TD SYNnex 株式会社

〒108-0023 東京都港区芝浦3丁目1-1
msb Tamachi 田町ステーションタワー N 21階
<https://jp.tdsynnex.com>

©TD SYNnex K.K. All rights reserved. 記載されている会社名および商品・サービス名は各社の登録商標または商標です。