キーワードは「アタリマエ」
これからのＩＴセキュリティはこう考える

ソフォス株式会社

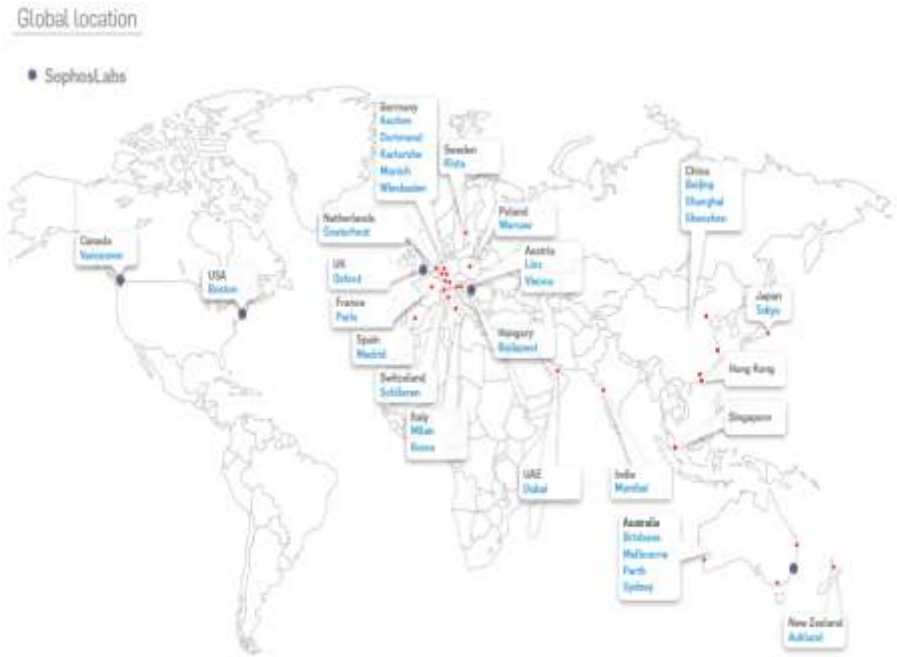
2015年3月29日

鈴木　敏通

SOPHOS

Sophos Limited

最高経営責任者
クリス　ヘイゲルマン　Kris Hagerman
本社所在地
イギリス　オックスフォード
アメリカ　ボストン
設立
1985年　イギリス　オックスフォードに設立
販売地域
世界150ケ国（ユーザー数１億人以上）
オフィス
イギリス、アメリカ、ドイツ、カナダ、オーストラリア、
日本、イタリア、フランス、シンガポールなど
従業員数
約　2,300 名以上（全世界）



ソフォス株式会社

代表取締役社長
纐纈　昌嗣（こうけつ　まさつぐ）
所在地
東京都港区六本木1-6-1　泉ガーデンタワー10F
設立
1997年　ソフォス製品国内販売開始
2000年　ソフォス株式会社設立
事業内容
法人向けITセキュリティ関連製品
サービスの開発、販売およびサポート
（日本市場でのソフォスソリューションを販売・サポート）

お客様：　国内約 3,500社以上

岩波書店、大興電子通信、サングループ、芝浦工業大学、
新日鉄ソリューションズ、早稲田大学、東京大学、など
その他、官公庁、地方自治体、銀行、大学、大手自動車メーカー
電機メーカー 、コンピュータメーカーなど

（約40% 官公庁・地方自治体、15% 教育・研究機関、企業向け拡大）



芝浦工業大学　早稲田大学
TOSHIBA　NTT PC COMMUNICATIONS　IIJ　asahi.com
REVLON　accenture　Microsoft　GE
MIRAPOINT　webroot SOFTWARE, INC.　CISCO　BlueCoat

会社沿革

- グローバルに展開 150,000以上の顧客ベース（日本国内約3,500社）
- **法人に完全特化**
- 従業員数 2,300人 (日本法人 50人)
- シンプルな統合ITセキュリティ・ソリューションの提供および、脅威解析センター “Sophos Labs” からサービスを提供

【年表】

- 1985年 英国に設立した統合セキュリティ対策ベンダー
- 2000年 日本法人 (ソフォス株式会社) 設立
- 2003年 カナダActive State社買収、スパム対策市場参入
- 2005年 アメリカ エンドフォース社を買収、NAC技術を取得
- 2008年 ウティマコセーフウェアを買収、暗号化技術を獲得
- 2011年 UTMベンダー、ドイツ Astaro 社買収
- 2012年 MDMベンダー、ドイツ Dialogs Software 社買収
- 2014年 Cyberoam Technologies社買収

ソフォスのテクノロジー

SophosLabs

ソフォスのテクノロジーは、各種アワードを多数受賞しています。
世界 5 ヶ所 (オックスフォード、バンクーバー、シドニー、ボストン、ブダペスト) にある SophosLabs では、経験豊富なアナリストが 24 時間 365 日、ウイルスやスパムなどさまざまな種類の脅威を統合的に解析しています。SophosLabs が持つ 100 万件以上のマルウェアサンプルと、1 日最大 4 万件更新している有害サイトの URL 情報は、クラウド上のデータベースで共有されているため、最新の脅威対策を即座に提供することが可能です。
ソフォスのテクノロジーは業界でも高く評価されており、多数のセキュリティベンダーやサービスプロバイダが、ソフォスの脅威検出エンジンを採用しています。

アワード受賞

ソフォスラボの迅速な対応と Genotype テクノロジーにより各種アワードを受賞

Virus Bulletin 100% (VB100%) 賞
2014 年 2 月時点

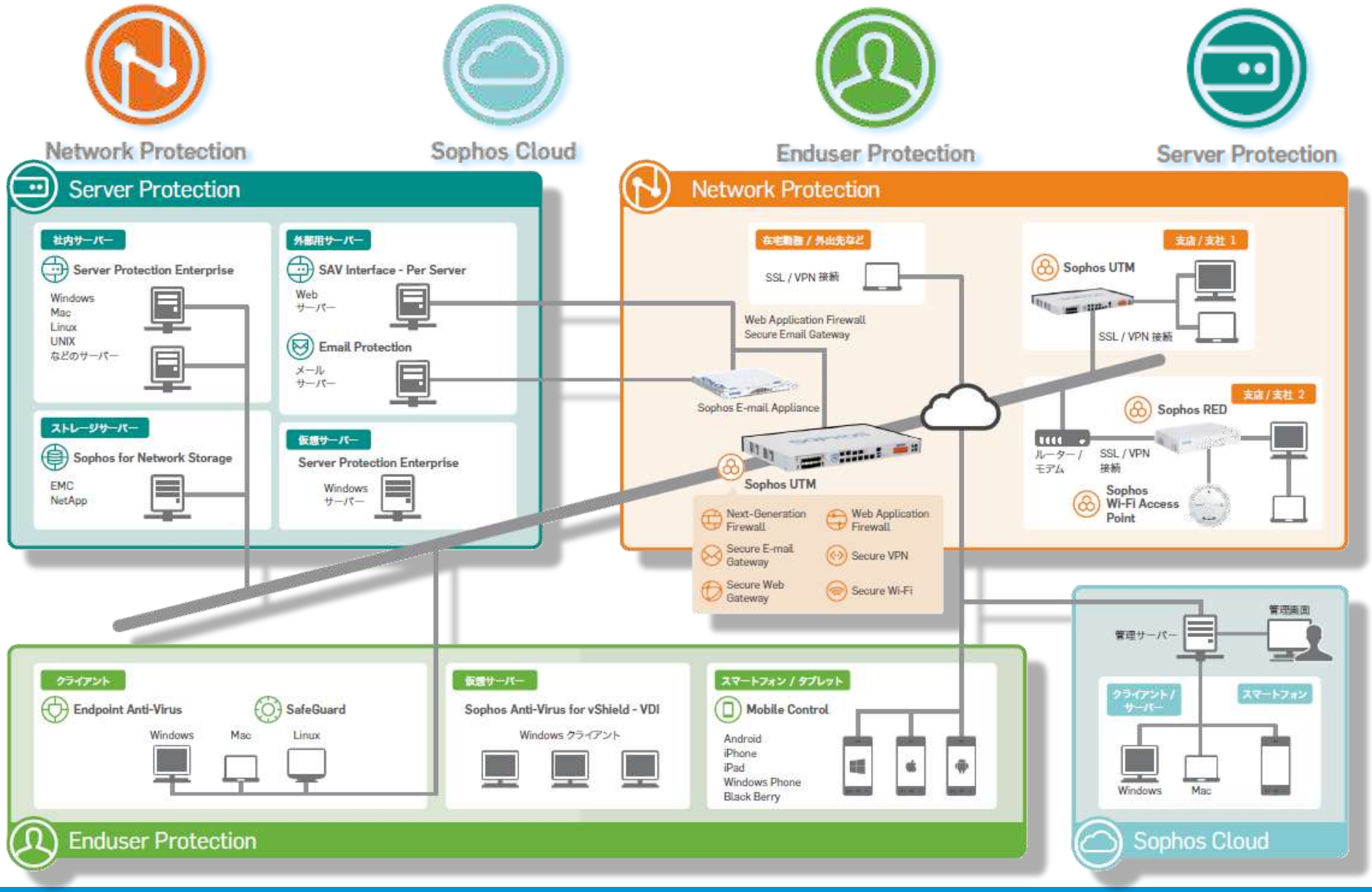
VB100% 受賞回数

ベンダー	ソフォス	A 社	B 社	C 社	D 社	E 社
受賞回数	70 回	16 回	57 回	49 回	52 回	66 回

- 信頼された技術
  →多くのベンダーへのエンジン提供

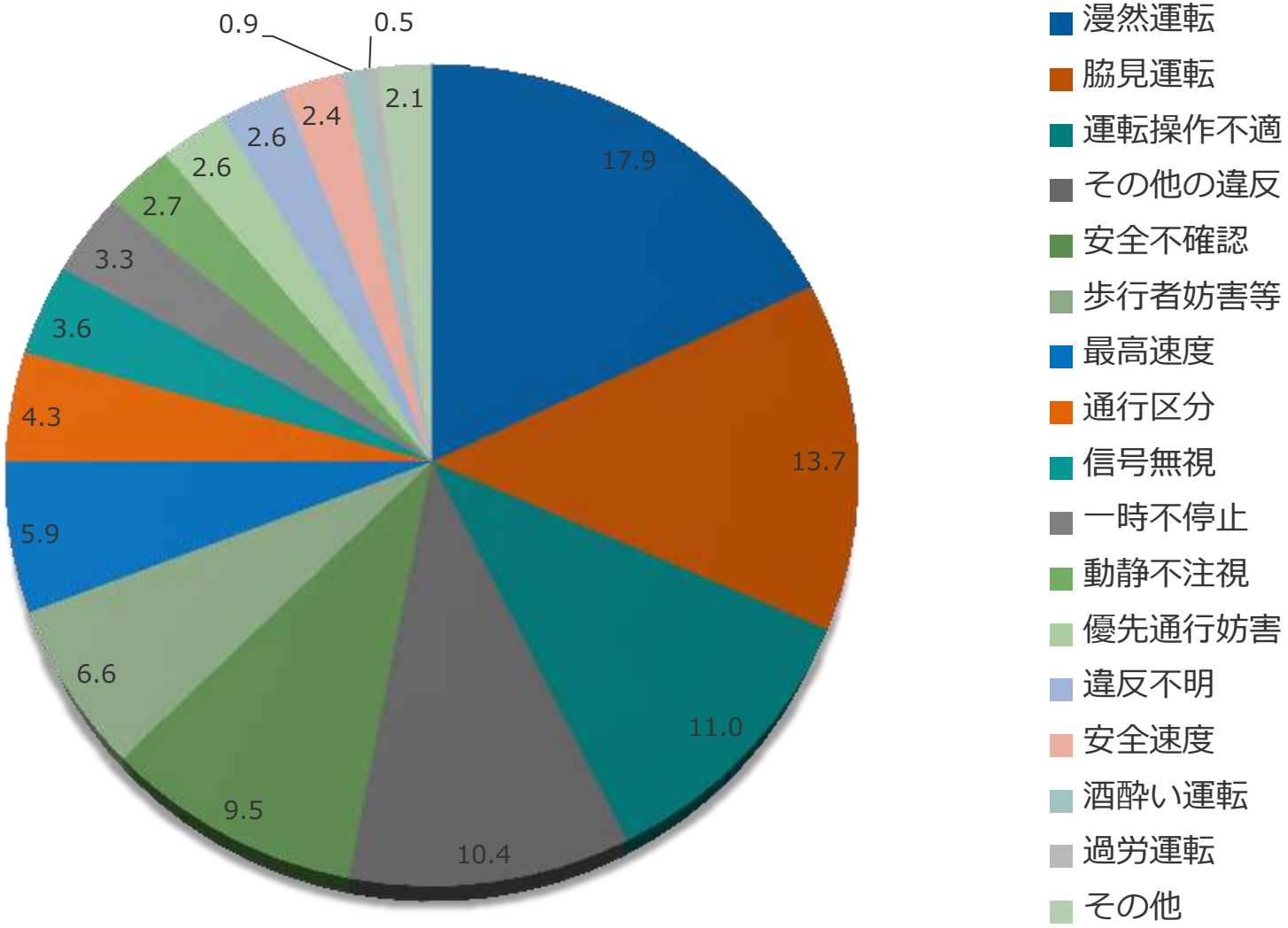
BlueCoat / MIRAPOINT / CISCO IronPort Email and Web Security / JUNIPER / crossbeam / CLEAR SWIFT / imatrix アイマトリックス 株式会社 / Webroot Spy Sweeper with AntiVirus

プロダクト・ソリューションマップ



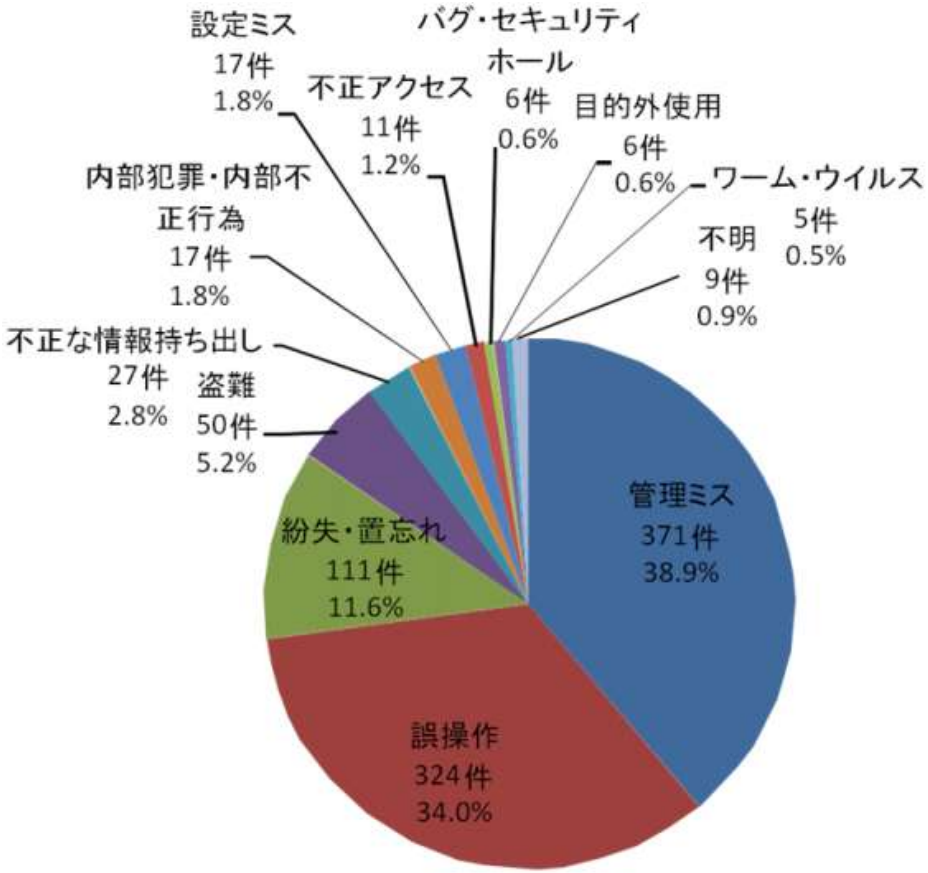
交通事故原因

- 事故の多くは　“ヒューマンエラー” -

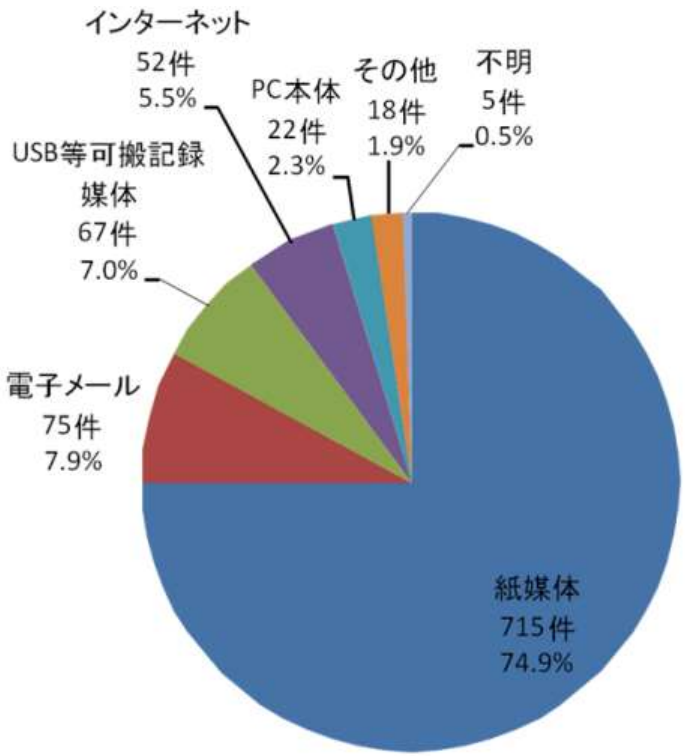


情報漏えい事故も同じ

- 事故の多くは　“ヒューマンエラー” -



情報漏えい原因



情報漏えい媒体、経路

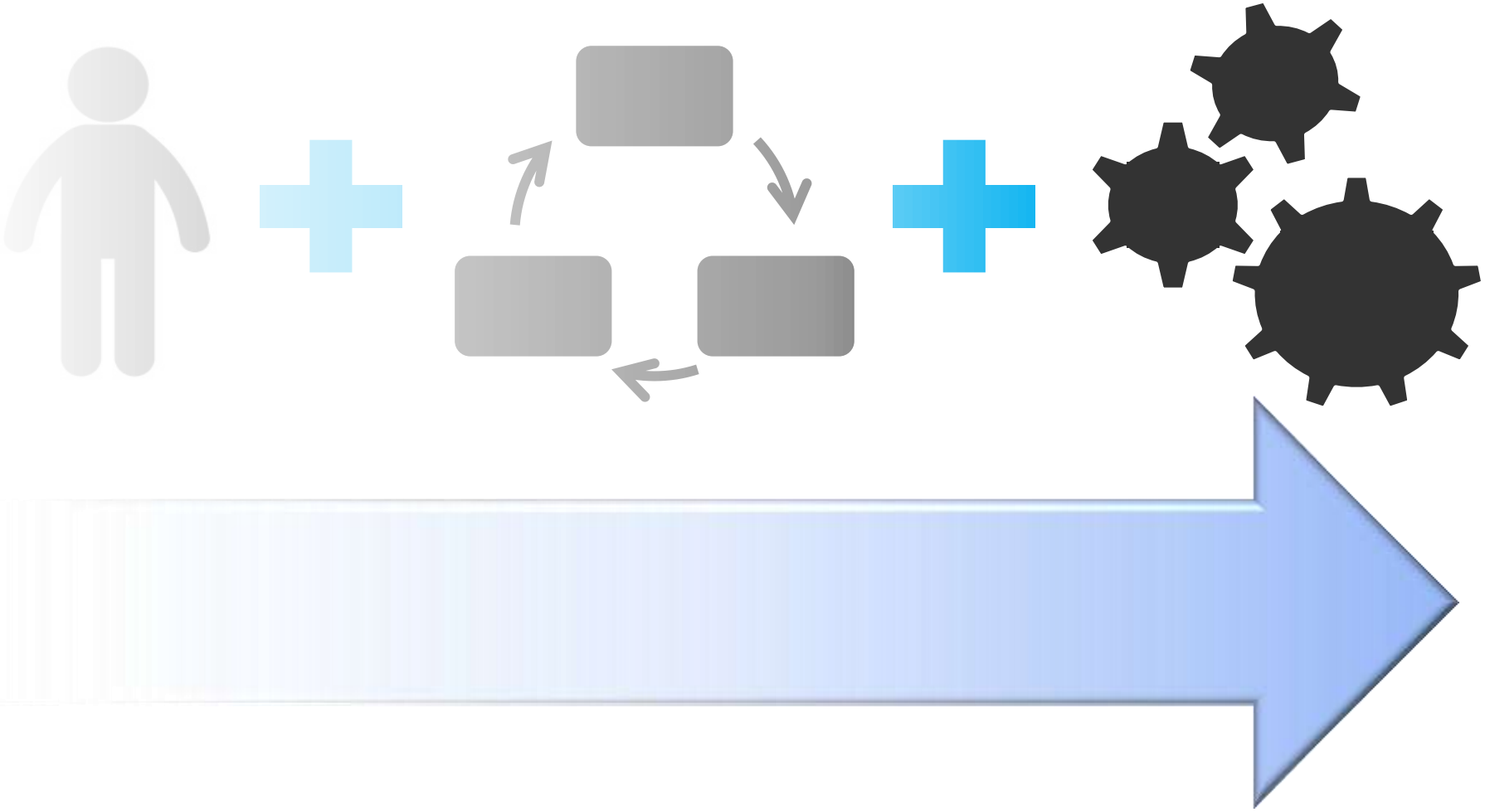
出展：NPO日本ネットワークセキュリティ協会「2012年情報セキュリティインシデントに関する調査報告書」より

ヒューマンエラーを無くすためには

- 人に頼らない “オートメーションテクノロジー” の導入が必要 -

ＩＴセキュリティも同じ

- ヒト ＋ プロセス ＋ テクノロジー -



“アタリマエ”の街角風景

- 安全対策も含めて“道路インフラ” -

対応すべき“課題”が盛りだくさん

- ビジネスチャンスも盛りだくさん -

マイナンバー制度の導入

テレワーク推進

ＩｏＴ

Windows Server 2003終了

例えば　“マイナンバー”

- ガイドライン“技術的安全管理措置” -

安全管理措置の内容（本則）	中小規模事業者における対応方法
F　技術的安全管理措置 事業者は、特定個人情報等の適正な取扱いのために、次に掲げる技術的安全管理措置を講じなければならない。	
a　アクセス制御 情報システムを使用して個人番号関係事務又は個人番号利用事務を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う。	○　特定個人情報等を取り扱う機器を特定し、その機器を取り扱う事務取扱担当者を限定することが望ましい。 ○　機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、情報システムを取り扱う事務取扱担当者を限定することが望ましい。
b　アクセス者の識別と認証 特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する。	○　特定個人情報等を取り扱う機器を特定し、その機器を取り扱う事務取扱担当者を限定することが望ましい。 ○　機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、情報システムを取り扱う事務取扱担当者を限定することが望ましい。
c　外部からの不正アクセス等の防止 情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する。	⇒
d　情報漏えい等の防止 特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講じる。	⇒

マイナンバーガイドライン入門～「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」（案）の概要～　より抜粋

例えば　“テレワーク”

- 職場意識改善助成金（テレワークコース）にて実施すべきセキュリティ対策-

テレワークのＩＣＴとセキュリティ対策

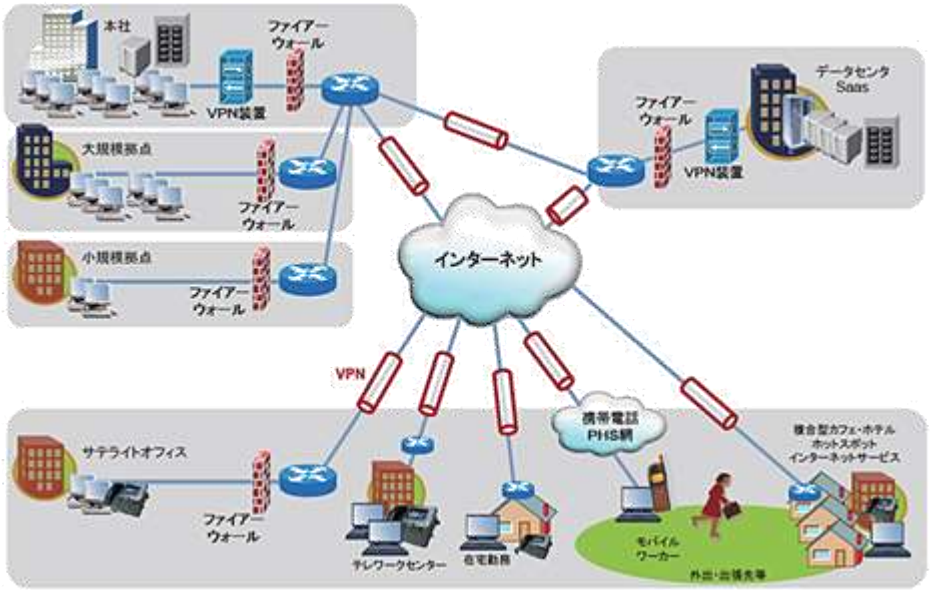
■ テレワークで必要となる ICT 設備の概念

ポイント

・テレワーカーがオフィス以外で仕事をする際でもオフィスにいる場合と同じ環境を整備する
・テレワーカーからの接続が安全に行えるようネットワークのセキュリティ環境を整備する

テレワーク環境で実施すべき対策一覧

分類	対策方法	内容
不正アクセス対策	ファイアーウォール導入	社内ネットワークと外部との境界を設定
不正アクセス対策	* IPS ／ IDS 導入	不正アクセスの進入検知もしくは排除
不正アクセス対策 データ盗聴、改ざんの防止	VPN 等導入	許可された者が外部から社内ネットワークにアクセスする際の認証および通信経路上でのデータの暗号化
端末管理情報漏えい対策	ウィルス対策ソフトウェアの導入	コンピュータウイルスの感染防止、駆除、被害拡大の防御
端末管理情報漏えい対策	・シンクライアントなどの端末の種類検討 ・端末操作制御ソフトウェアの導入	端末へのデータ保存や USB デバイスなどの外部記憶媒体への書き出しを制限
端末管理	検疫システムの導入	アクセスしてくる端末のセキュリティレベルの維持



例えば　“IoT”

- PC、サーバー、スマートフォン、モバイル端末・・・だけじゃない -

「レジ」標的ウイルス急増　国内でも６件確認、購入者のカード情報が狙いか

産経新聞 2月16日(月)21時35分配信

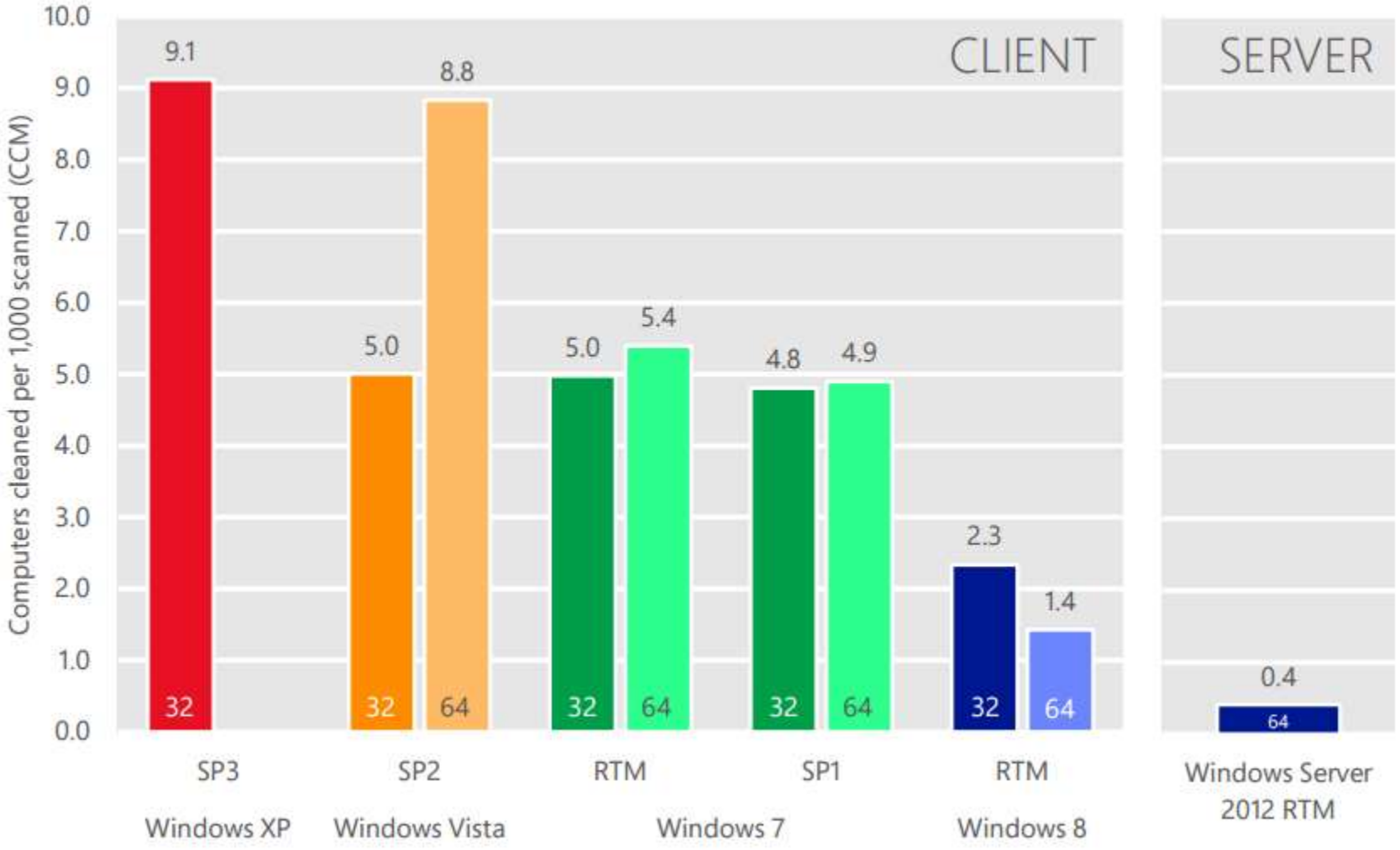
ツイート 242　シェア 274

「レジ」へのサイバー攻撃の仕組み（写真：産経新聞）

スーパーのレジなどを標的としたコンピューターウイルスの感染報告が昨年、全世界で４６７件に上り、国内でも６件確認されたことが１６日、分かった。サイバー攻撃とは無縁と思われがちなレジだが、在庫管理のため本社システムとインターネット接続されており、感染の恐れがあるという。購入者のクレジットカード情報を盗み出すのが狙いとみられ、実際に米国では「ブラックＰＯＳ」と呼ばれるウイルスによって顧客情報約１億１千万件が流出した。関係者は「企業側の対策が急務だ」としている。

例えば　“Windows Server 2003 終了”

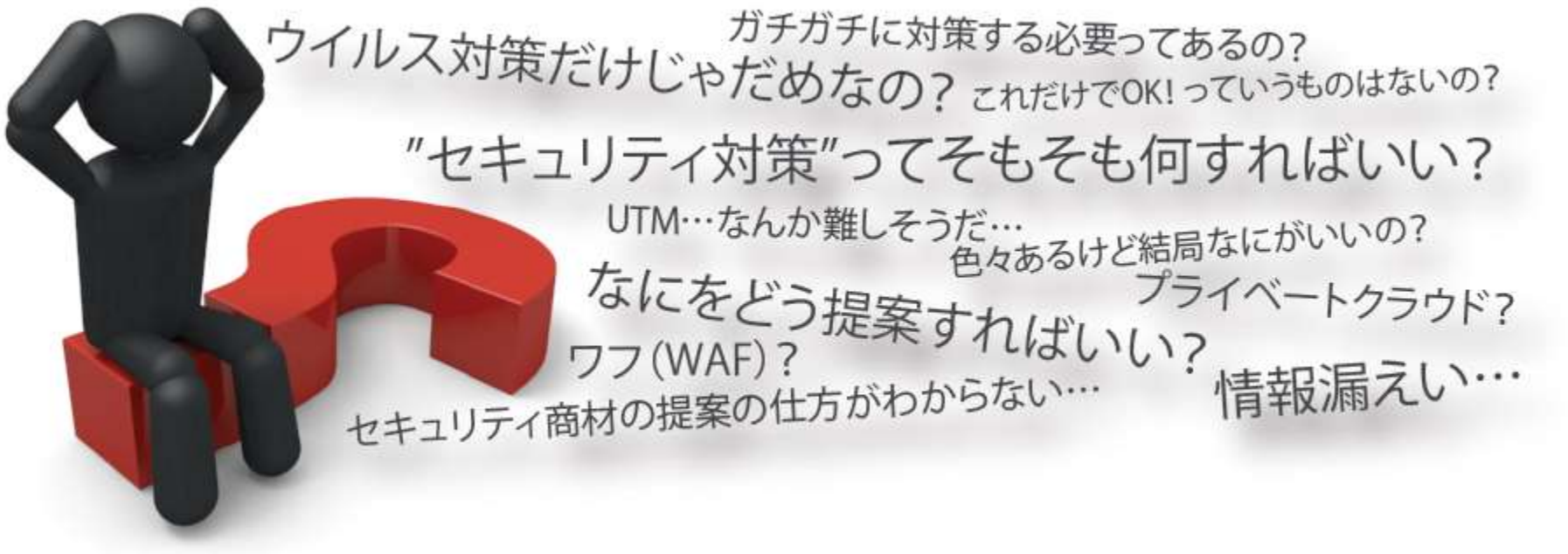
- 事実、旧OSは　“標的”　となりやすい -



出典：マイクロソフト セキュリティ インテリジェンス レポート第 14 版

対応すべき“手法”も盛りだくさん

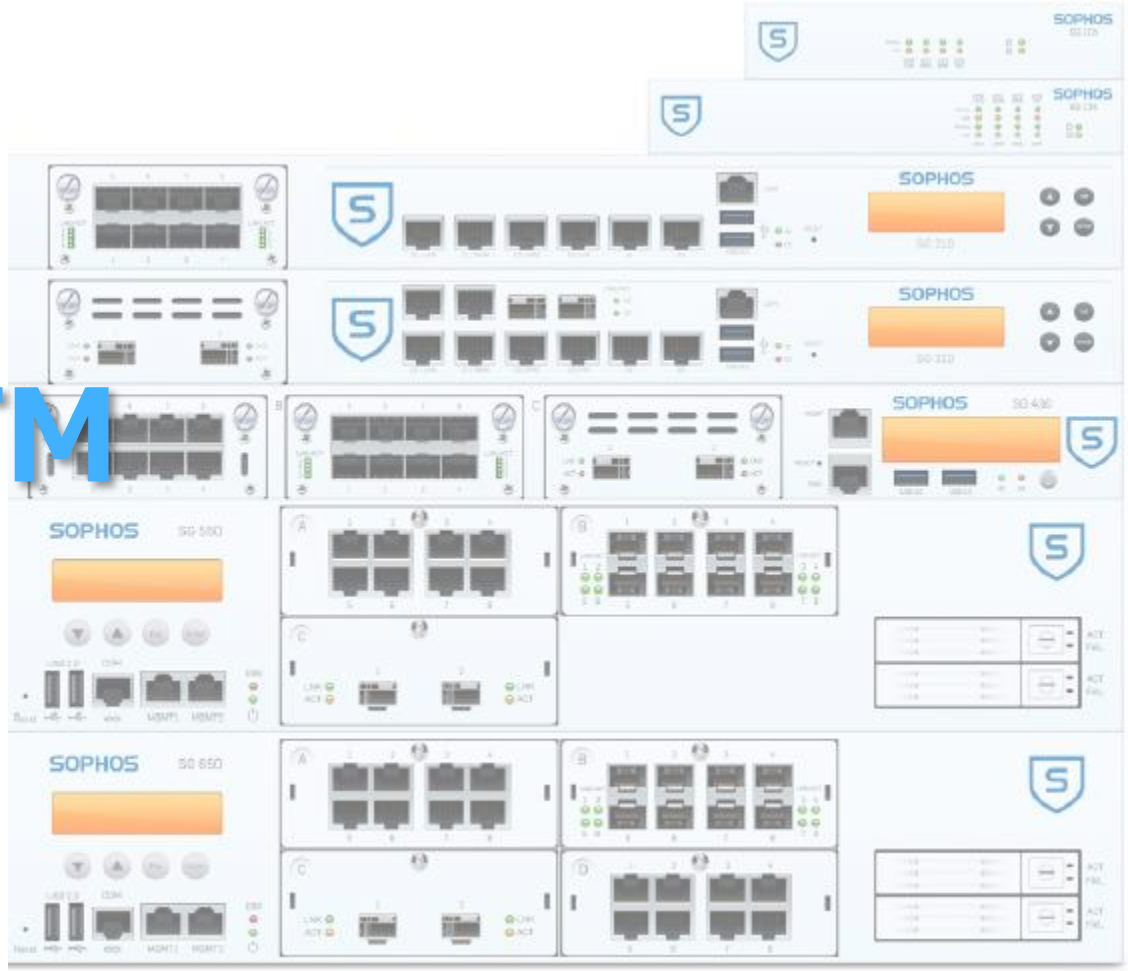
- 手間もコストも盛りだくさん -



ならば　“まとめて”

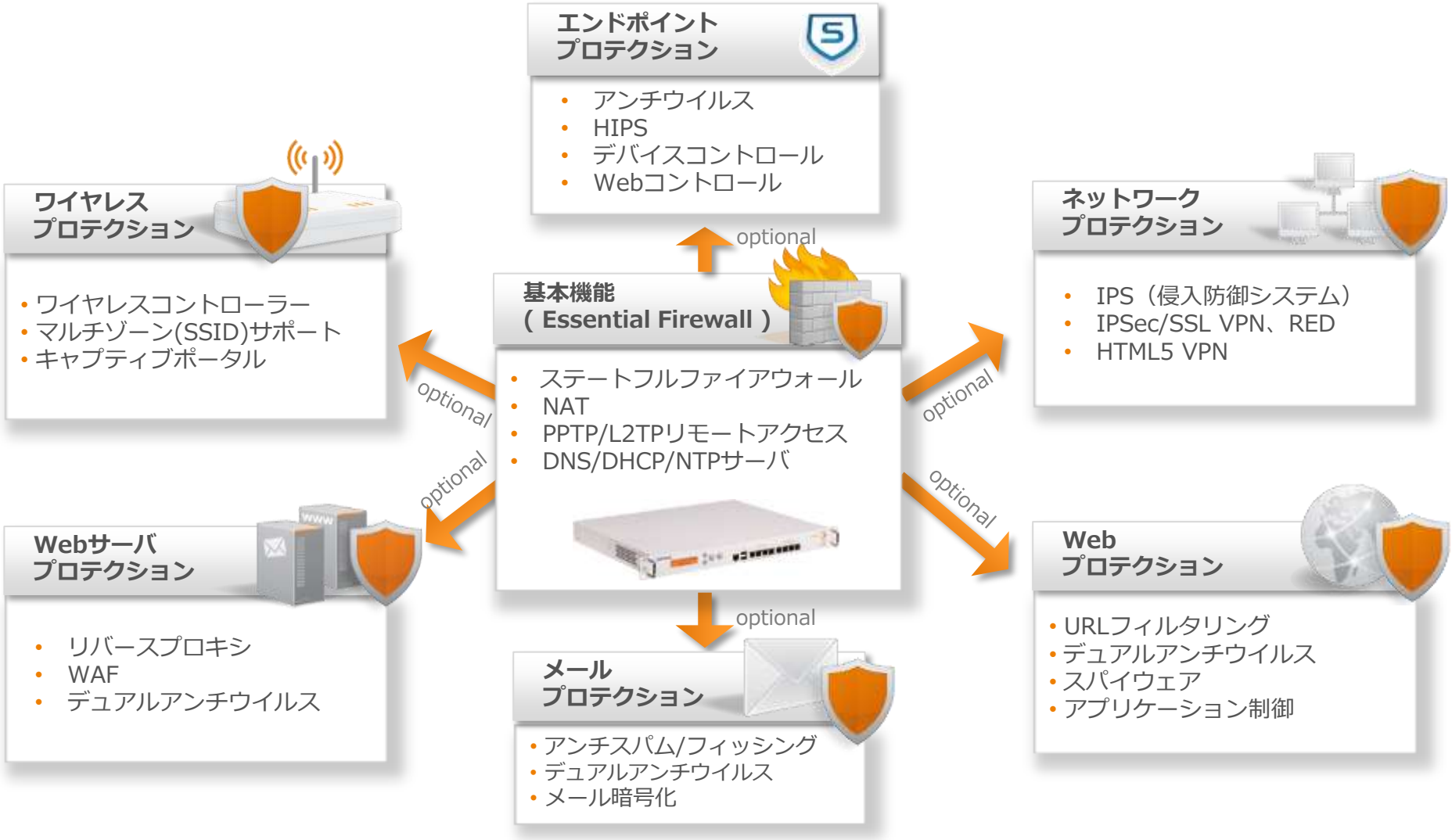
- オールインワン　“ネットワークインフラ”　ソリューション -

Sophos UTM



ソフォスの提供するネットワークソリューション

- セキュアネットワークのための “オールインワン”。 Sophos UTM -



UTMライセンス

- 用途に応じ、必要最低限な投資で最適な保護を実現 -

モジュール	主要機能	ライセンスサポート			
		個別モジュール	フルガード	TotalProtect Bundle	ベーシックガード
ネットワークプロテクション	• IPS • Ipsec/SSL VPN & RED • HTML5 VPN Portal	✓	●	●	◐
Webプロテクション	• URL フィルタ • アンチウィルス & アンチスパイウエア • アプリケーションコントロール	✓	●	●	◐
メールプロテクション	• アンチスパム　& アンチフィッシング • ２つのアンチウィルスエンジン • メール暗号化	✓	●	●	◐
ワイヤレスプロテクション	• ワイヤレスコントローラ • マルチソーン (SSID) • ポータルサービス	✓	●	●	◐
Web サーバプロテクション	• リバースプロクシ • WAF • アンチウィルス	✓	●	●	X
エンドポイントプロテクション	• アンチウィルス • HIPS • デバイスコントロール	✓	オプション (別売)	オプション (別売)	オプション (別売)
SGシリーズアプライアンス	• マルチテクノロジー • On-box ストレージ • スケーラブル	N/A	オプション (別売)	●	オプション (別売)

柔軟な導入形態

- オープンソースがベースだからこそ -

ハードウェア

ハードウェア、及び利用機能に関連するライセンスでご導入頂く形態です。利用ユーザー数等は、ハードスペックの限界次第。

ソフトウェア
仮想アプライアンス

利用機能に関連するライセンスを保護対象のIP数に応じ、ご導入頂く形態で、ハードは自由に選定可能です。

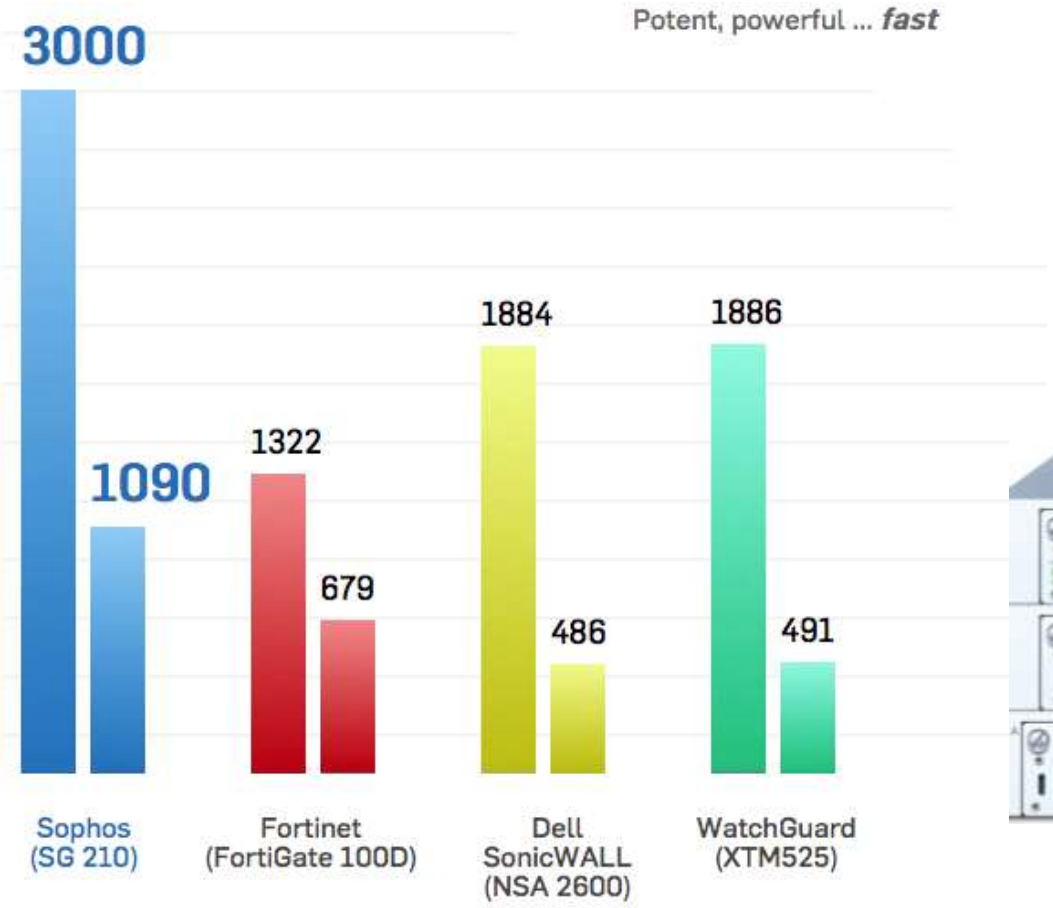
Amazon
マーケットプレイス

AWSで利用頂くライセンスです。マーケットプレイスからの購入で利用状況に応じて課金されます。

これらの導入形態の全てで、同一機能を利用可能です。

Miercom パフォーマンスリポート

- ASIC(Application Specific Integrated Circuit)を凌駕するパフォーマンス -



ピックアップ - Sophos RED -

- 容易で柔軟な導入、運用が可能なVPNソリューション -

導入はわずか4ステップ

①UTM側でREDサービスを有効化
(RED管理画面からクリック1回)

②REDをルータに接続
(REDはルーター機能はありません)

③UTM側でRED ID等の諸情報を入力
(ブランチ名、ホスト名、RED ID、IP)

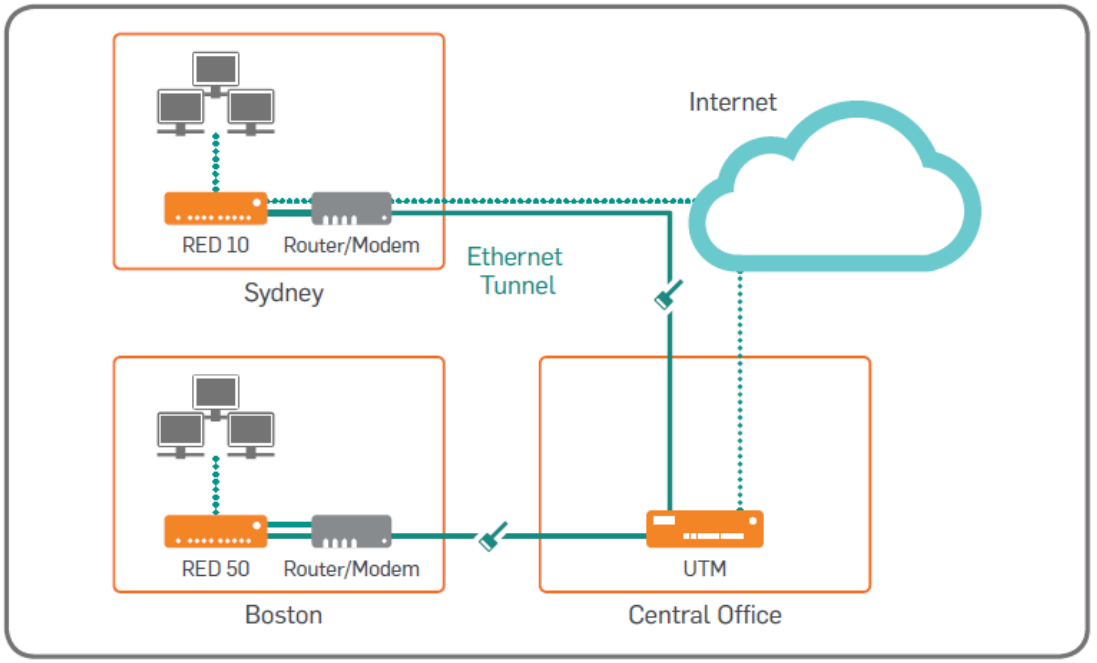
④「REDの導入」をクリック（完了！）

オンサイト対応不要

Sophos REDはルーター配下に接続し、リモートでUTM本体の管理画面から
IP設定、固有のシリアルID（RED ID）を打ち込むだけで接続完了。
電話越しに背面のID確認のみで導入・復旧が可能。

個別設定不要

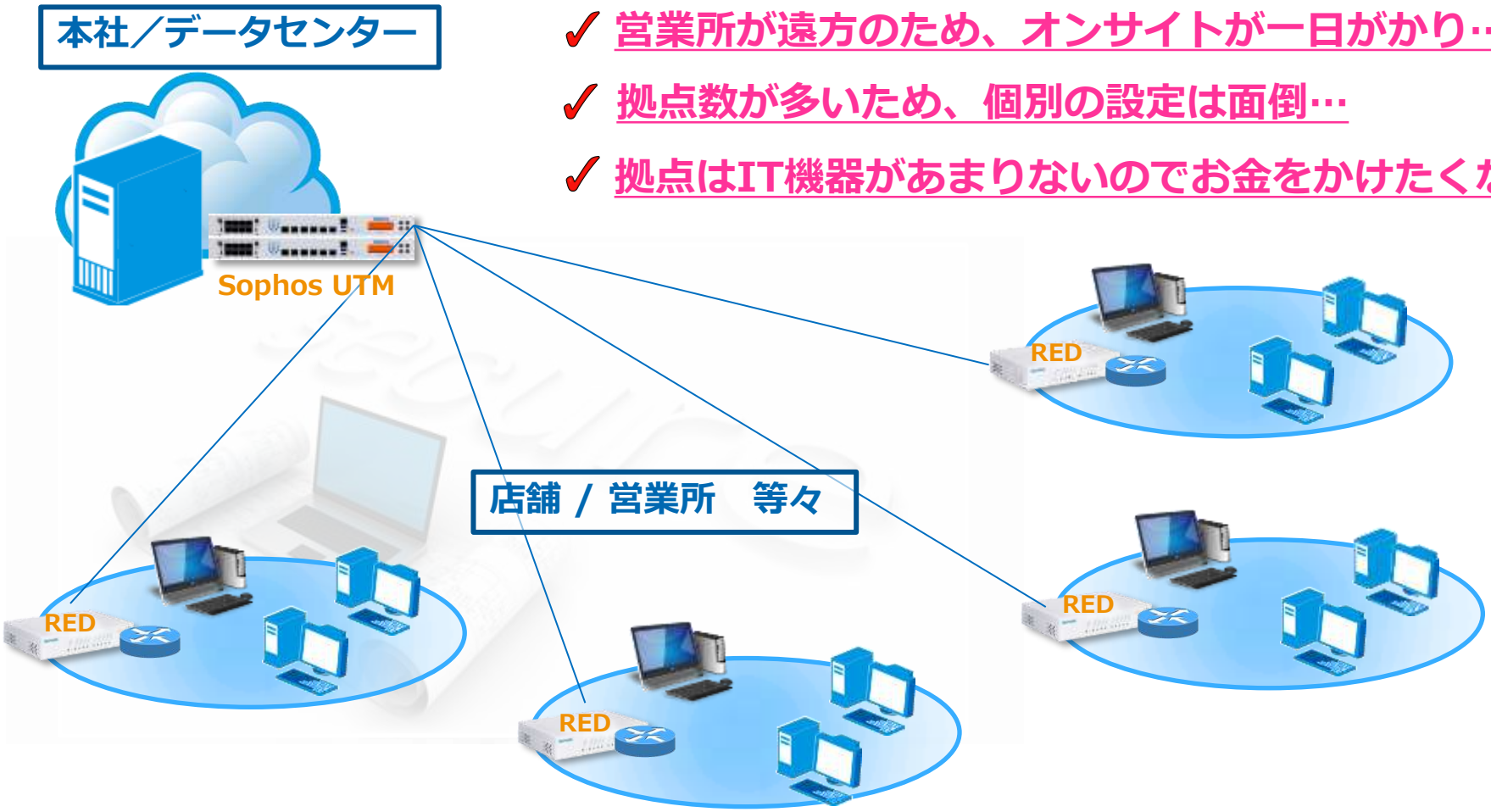
Sophos REDは設定済のUTMへ通信を転送する動作のみを行います。
そのため個別の設定は不要で、且つ設定済UTMと同じセキュアな
ネットワーク通信を簡単に実現することが出来ます。



ピックアップ - Sophos RED -

- Sophos REDを用いた容易にセキュアVPN構築 -

- ✓ 現地にITに詳しい人間がいないので管理が手間
- ✓ 営業所が遠方のため、オンサイトが一日がかり…
- ✓ 拠点数が多いため、個別の設定は面倒…
- ✓ 拠点はIT機器があまりないのでお金をかけたくない



Developers.IO ブログで掲載中

- 二部構成で設定の詳細をわかりやすく解説！ -

http://dev.classmethod.jp/etc/sophos-red10/

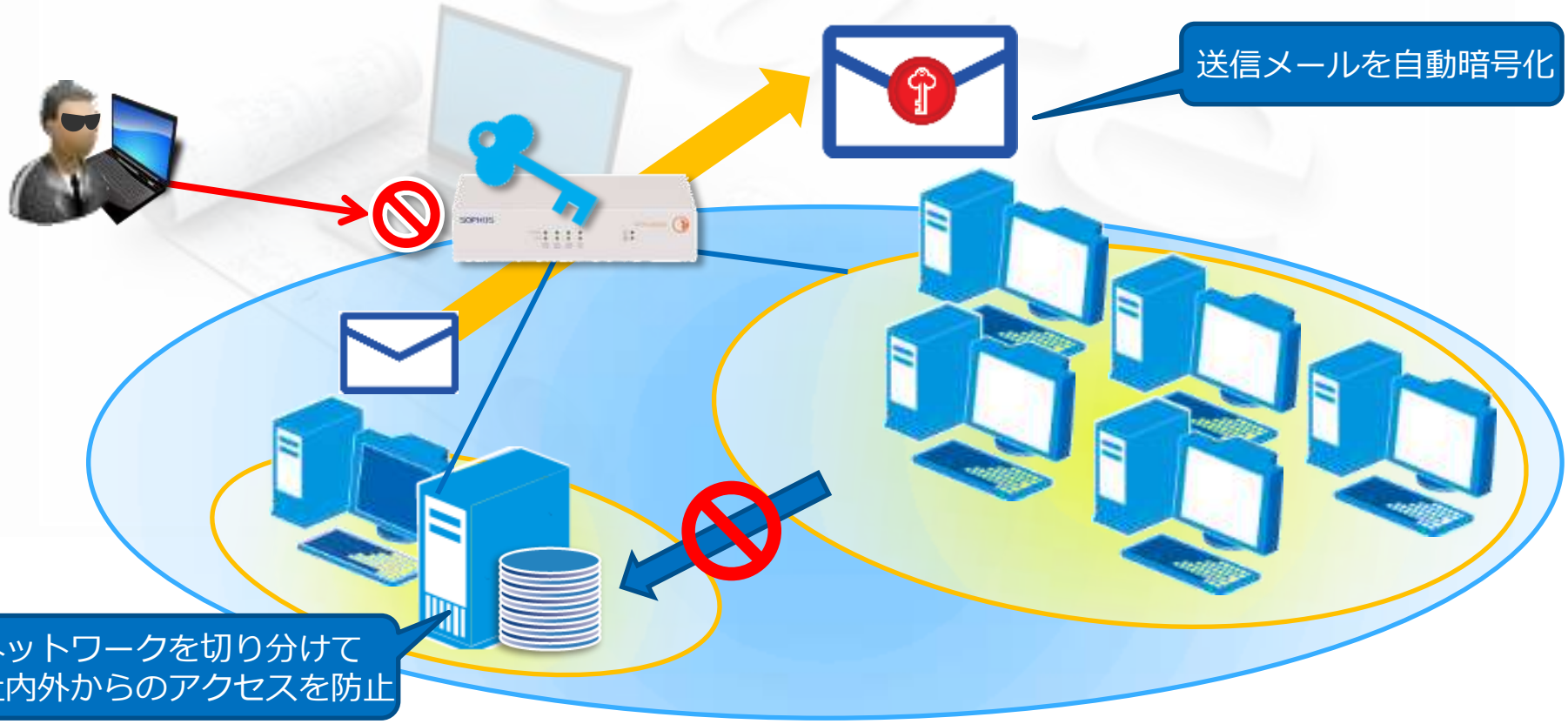
http://dev.classmethod.jp/etc/sophos-red10-no2/

マイナンバーへの対応

- カギは“情報漏えい対策” -

ネットワークプロテクション + **メールプロテクション**

不正アクセスの阻止、社内ネットワークの切り分け、情報漏えい対策（メール暗号化）

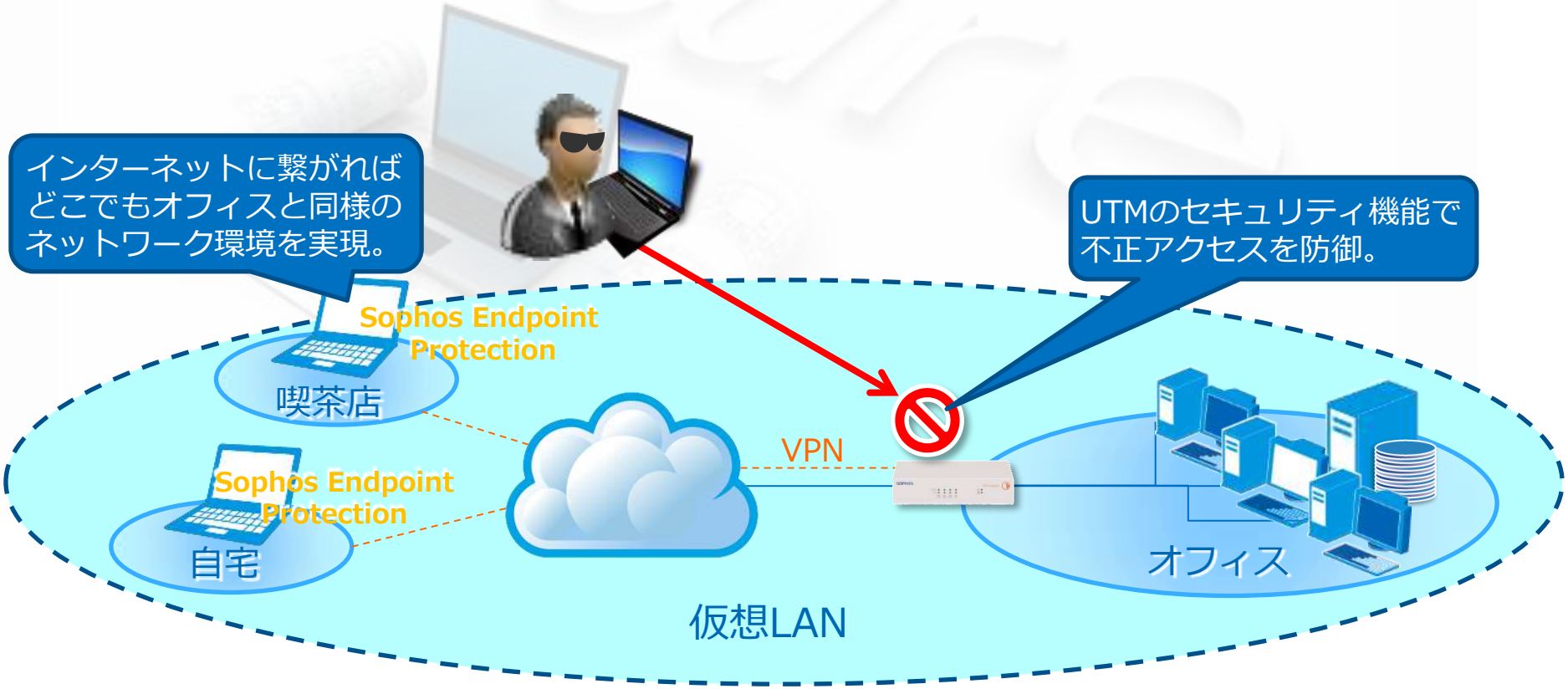


テレワークへの対応

- セキュアネットワークの構築とリモート接続を同時に実現 -

ネットワークプロテクション + **エンドポイントプロテクション**

不正アクセスの阻止、リモート機器のマルウェア対策、セキュアなリモート接続

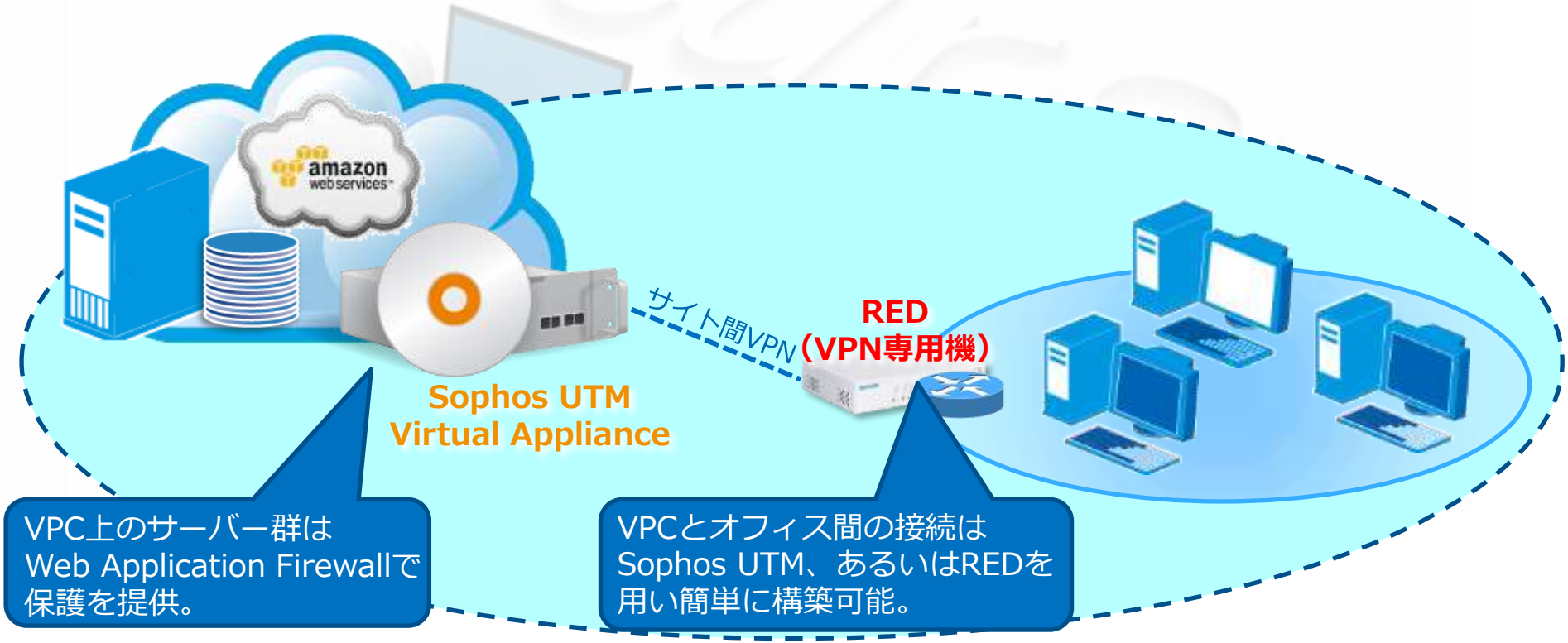


Windows Server 2003 終了　への対応

- “P2C”マイグレーション 。オンプレミスからクラウドへ-

ネットワークプロテクション + **Webサーバープロテクション**

データセンター上のサーバー保護、データセンター ↔ オフィス間接続



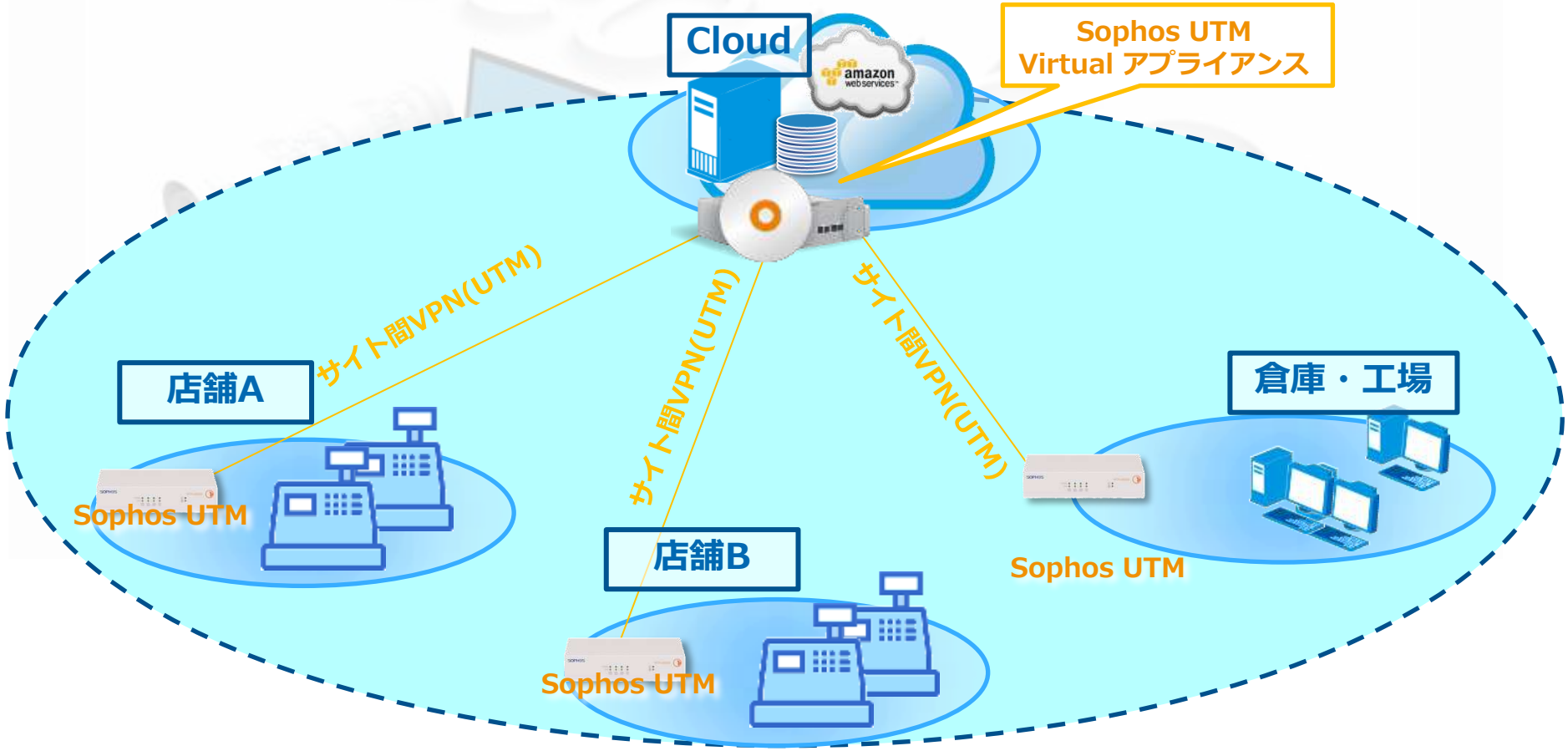
UTM＋UTMのVPNを組むことで、安全なハイブリッド環境の構築も可能

IoT への対応-

- 例えば、クラウドを利用したPOSシステムの場合 -

ネットワークプロテクション + **Webサーバープロテクション**

データセンター上のサーバー保護、データセンター ↔ 各拠点間接続、各拠点の保護



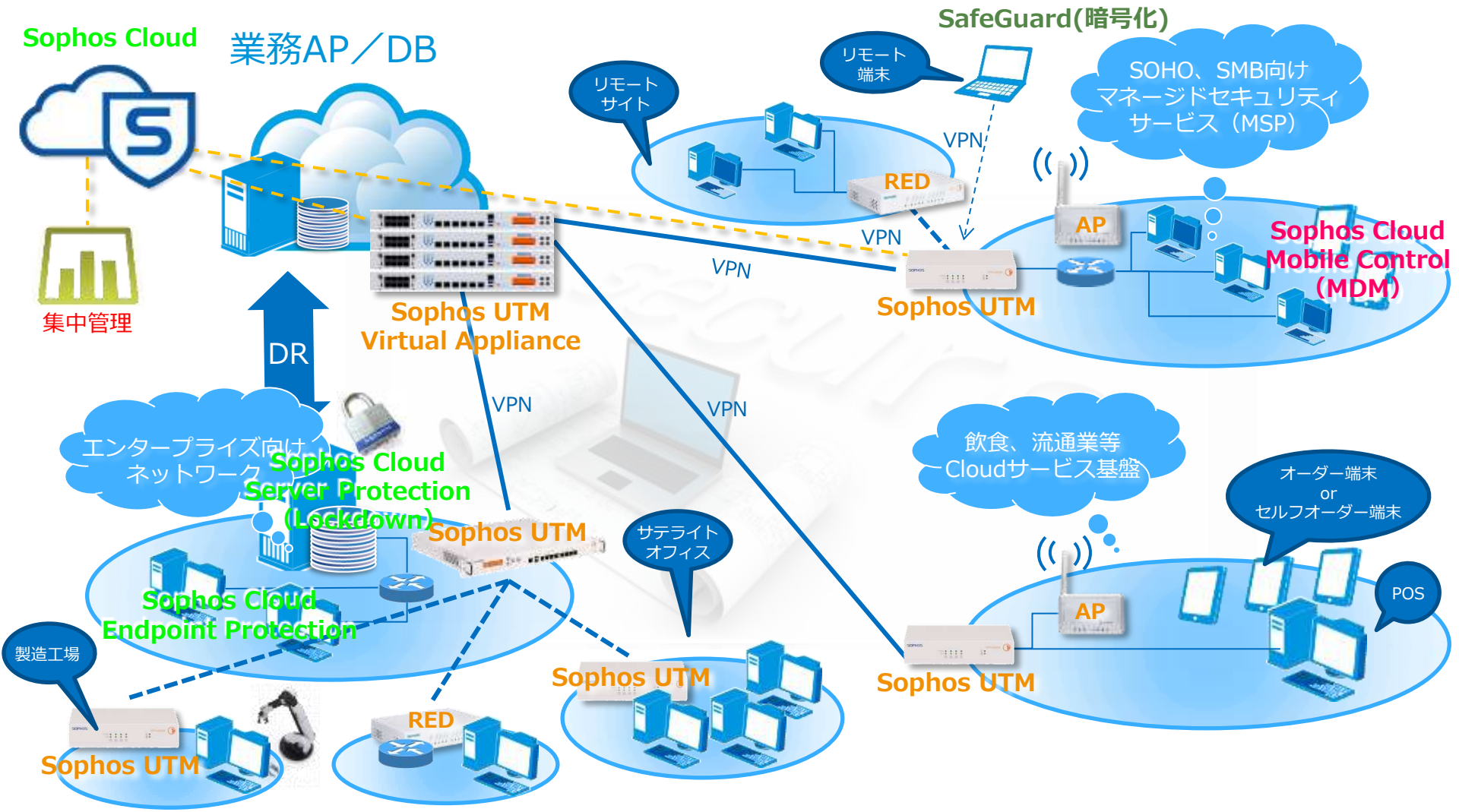
Sophos UTMとは

- いうなれば・・・-

セキュリティ屋さんの
ネットワーク機器

ソフォスで作る “セキュアネットワークインフラ”

- あらゆる業種、環境へ最適なセキュリティソリューションを提供 -



ソフォス　＝　Security Solution Provider

- 次世代のセキュリティ対策　ポイントソリューションから統合ソリューションへ -

ニュース　日経コンピュータ

「エンドポイントとネットワークの防御を連携」、ソフォスCEOが新戦略

2014/11/11
勝村 幸博＝日経コンピュータ（筆者執筆記事一覧）

記事一覧へ >>

シェア　ツイート　B! ブックマーク

「エンドポイントとネットワークのセキュリティ製品を連携させて企業を脅威から守るソリューションを、2014年から2015年にかけて順次発表する」。英国のセキュリティベンダーであるソフォスのクリス・ヘイゲルマンCEO（最高経営責任者）は2014年11月11日、同社の製品戦略などについて発表した（**写真1**）。

写真1●英ソフォスのクリス・ヘイゲルマンCEO
[画像のクリックで拡大表示]

ソフォスは、エンドユーザー向けのセキュリティソフトや、企業ネットワーク向けのUTM（統合脅威管理）製品などを手掛けるセキュリティベンダー。1985年に設立。同社によると、ワールドワイドでの顧客企業は20万社以上、ユーザー数は1億人以上に上るという。

写真2●ソフォスの嶺纐昌嗣 代表取締役社長
[画像のクリックで拡大表示]

ソフォスの日本法人は2000年に設立。現状では、同社製品は「主に官公庁を中心に導入されている」（嶺纐昌嗣 代表取締役社長、**写真2**）。

ソフォスと他のセキュリティベンダーの違いの一つとして、ヘイゲルマンCEOは「ミッドマーケット（中堅・中小企業向け市場）に注力している」ことを挙げる。「セキュリティベンダーの多くは、世界ランク2000社以内の大企業をターゲットにしている」（ヘイゲルマンCEO）。

エンドポイント製品で脅威が検知された場合、その事実をネットワーク製品に知らせることで、該当の通信を遮断できるようになる。また、ネットワーク製品で脅威を検出した場合には、その事実をエンドポイント製品に通知することで、クライアントへのマルウエア侵入などを阻止できるようになる　-記事より抜粋-

セキュリティ ＝“アタリマエ”

- 安全対策も含めて“ＩＴインフラ” -

Endpoint　Web　E-mail　Encryption　Mobile　Network

SOPHOS
simple + secure

SOPHOS