らくらんセキュリティサポート

サービス概要説明書

Vol. 1.0

YODOQ
We keep chasing our dream

インターネットの脅威

「サプライチェーンの弱点を悪用した攻撃」を受けると、自組織が被害を受けるだけではなく、**攻撃に加担**してしまう恐れがあります。取引相手にも損害を与えてしまうことになるため、**業務の一時停止**や**損害賠償**を求められる可能性もあり、ビジネスに莫大な影響を及ぼす恐ろしい脅威です。この攻撃を防ぐには、**中小企業様も含めた自組織のセキュリティ向上が不可欠**です。

マイナンバーの取扱い

社員一人ひとりのマイナンバーを預かり安全に管理することが義務付けられます。その保管方法や取扱いルールを定める方法を決めかねていませんか？

不正アクセスや情報漏えい

コンピュータの技術向上に伴い、今までは対岸の火事だったハッカーの不正アクセスやウイルスによるPC乗っ取り事件が身近に起こる時代です。

ネットバンキング不正送金

2013年くらいから増え続けている不正送金被害、ありとあらゆる対策をくぐり抜け増加傾向に歯止めがききません。

情報漏洩があった場合に想定される企業の不利益

1. **企業の信用低下**
2. **損害賠償の負担**
3. **被害状況調査や報告にかかるコスト**
   - マルウェア感染調査
   - 内部不正調査
   - フォレンジック調査
   - その他

※被害状況調査と報告を怠った場合は、罰則が適用される可能性があります。

個人情報を一つでも把握していたら、
その取り扱いについての責任が生じます

- 氏名、住所、電話番号
- パスポートの番号
- 基礎年金番号
- 免許証の番号
- 住民票コード
- 個人番号（マイナンバー）
- 保険証の番号
- 在留カードの番号
- 特別永住者証明書の番号　等

YODOQ
We keep chasing our dream

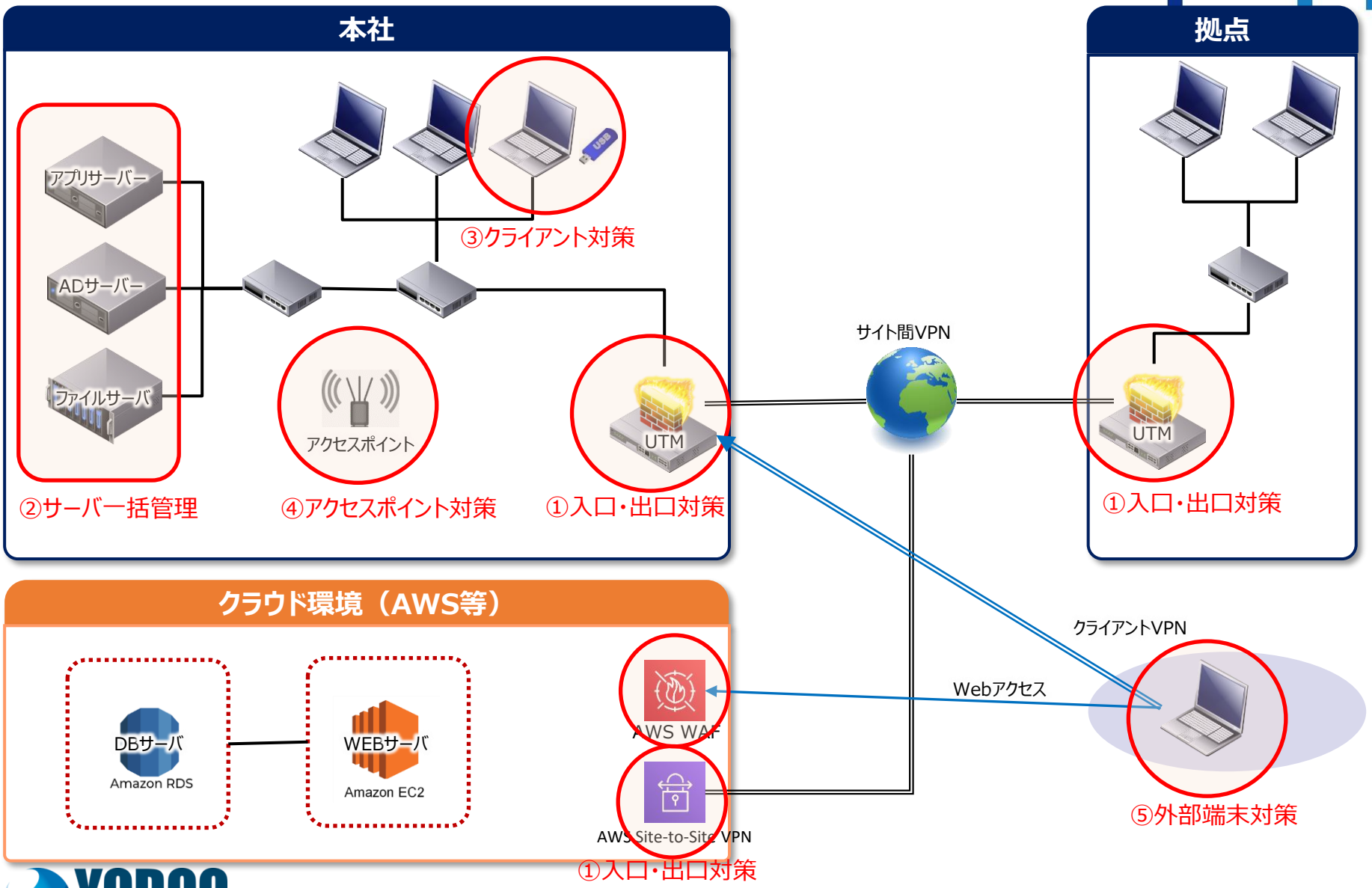
こんなご要望はありませんか？

- 安全・安心なネットワーク環境を構築したい
  - 入口・出口でのセキュリティー対策
  - クライアント端末へのセキュリティー対策
  - 各種管理レベルの向上

- セキュアーなVPN（拠点間接続・リモート環境）を実現したい
  - IPSec VPN（AES256-SHA256）
  - VPN接続ソフト（Check Point Remote Access VPN Clients）
  - 利用制限機能（SkySea・AD）

- 高度なセキュリティーシステムを活用したい
  - アンチウィルス/アンチスパム機能（AV/AS）
  - 不正侵入防止システム（IPS）
  - Webフィルタリング/アプリケーション制御

セキュリティー対策のポイント(ネットワーク環境)



セキュリティー対策のポイント(ネットワーク環境)

【視点】	【リスク】	【対策】
①入口出口対策	・外部からの侵入、ウィルスメール ・不正ソフトの利用	・外部からの侵入を防ぐことのできるファイアーウォール(UTM)導入 → 例）CheckPointの導入
②サーバー一括管理	・個々の端末設定の労力（IT資産管理、インストール、パスワード） ・ログの可視化 ・サーバデータへの不正アクセス ・不正PC接続	・ActiveDirectory導入 ・操作ログ取得 ・ネットワーク監視 → 例）ADサーバ導入
③クライアント対策	・不許可デバイスの使用 ・不正な印刷 ・不正な操作 ・ウイルス感染	・IT統合セキュリティーパッケージ導入 →例）SKYSEA Client View ・ウイルス対策ソフト導入 →例）ESET PROTECT
④アクセスポイント対策	・不正な端末接続 ・不正な盗聴	・macアドレス認証 ・ゲストポート設置
⑤外部端末対策	・紛失 ・ウイルス感染 ・データ漏えい	・暗号化ツール ・ウイルス対策ソフト ・IT統合セキュリティーパッケージ ・セキュアVPNクライアント

すべて行うには費用がかかる。最低限必要な対策は何か。
狙われにくい。状況の可視化。最新の対策へ更新。

YODOQ
We keep chasing our dream

よくある問題点

大きな問題点として・・・

①ほとんどの場合ソフトはインストールするだけで
高度な設定はされていない
→使いこなせていないのが実状です!!

②安価なソフトやルーターでは機能が不足
→実はまったく機能していないケースもあります!!

③複合機にはなにも対策がなされていない
→複合機には実は様々な情報が蓄積してます!!

④ウイルスは一度PCまで届いてしまう
→PC上の対策ソフトは一度届かないと機能しません!!

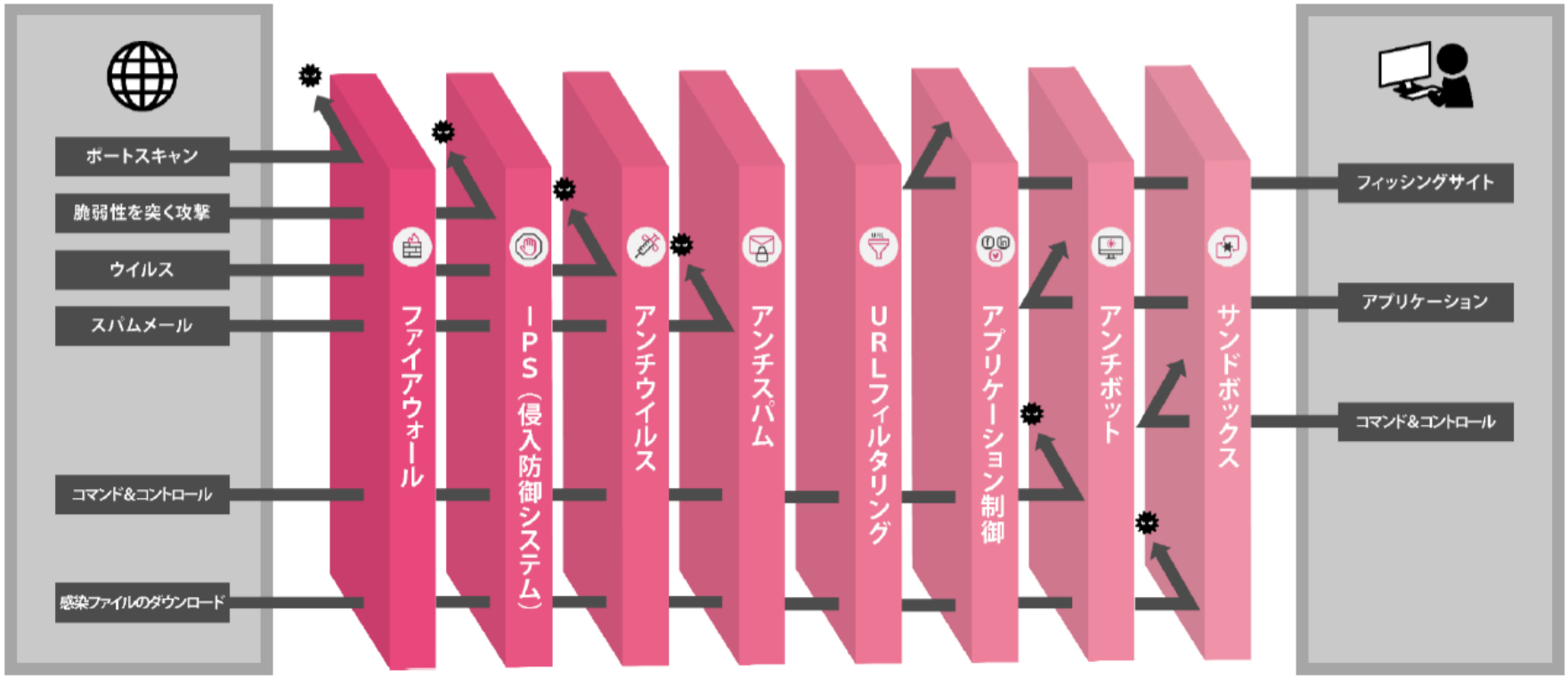
⑤設定がされていなければどんなサイトも閲覧できてしまう
→不用意なアクセスが感染を招きます!!

該当すれば実は危険が迫っています!!

UTMの提供機能

①入口出口対策

✓各セキュリティー機能を組み合わせることによって出入口双方からの多層防御を実現



UTM機能ご紹介（IPS：不正侵入防御システム）

①入口出口対策

IPS（Intrusion Prevention System）は、日本語では「不正侵入防止システム」と呼ばれており、ネットワーク上の通信を監視して**不正なアクセスをブロック**する役割を持ちます。

① 従来のシステムでは対応できない攻撃を検知できる

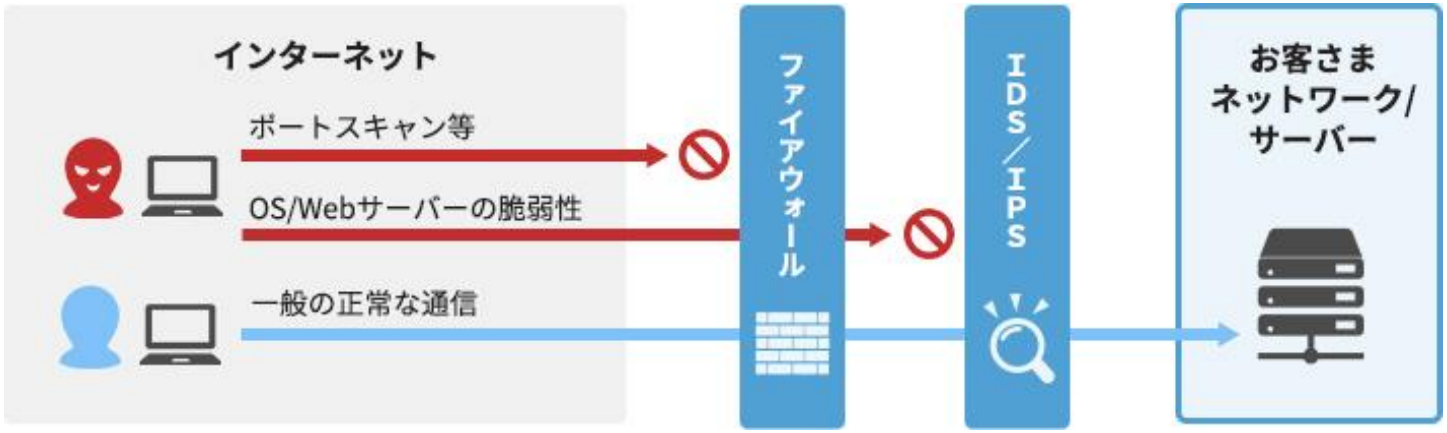
不正アクセスを防ぐセキュリティシステムには従来からファイアウォール（Firewall、FW）がありますが、IDS/IPSではファイアウォールでは対応できなかった攻撃を検知することができます。

② リアルタイムで検知・防御を実施できる

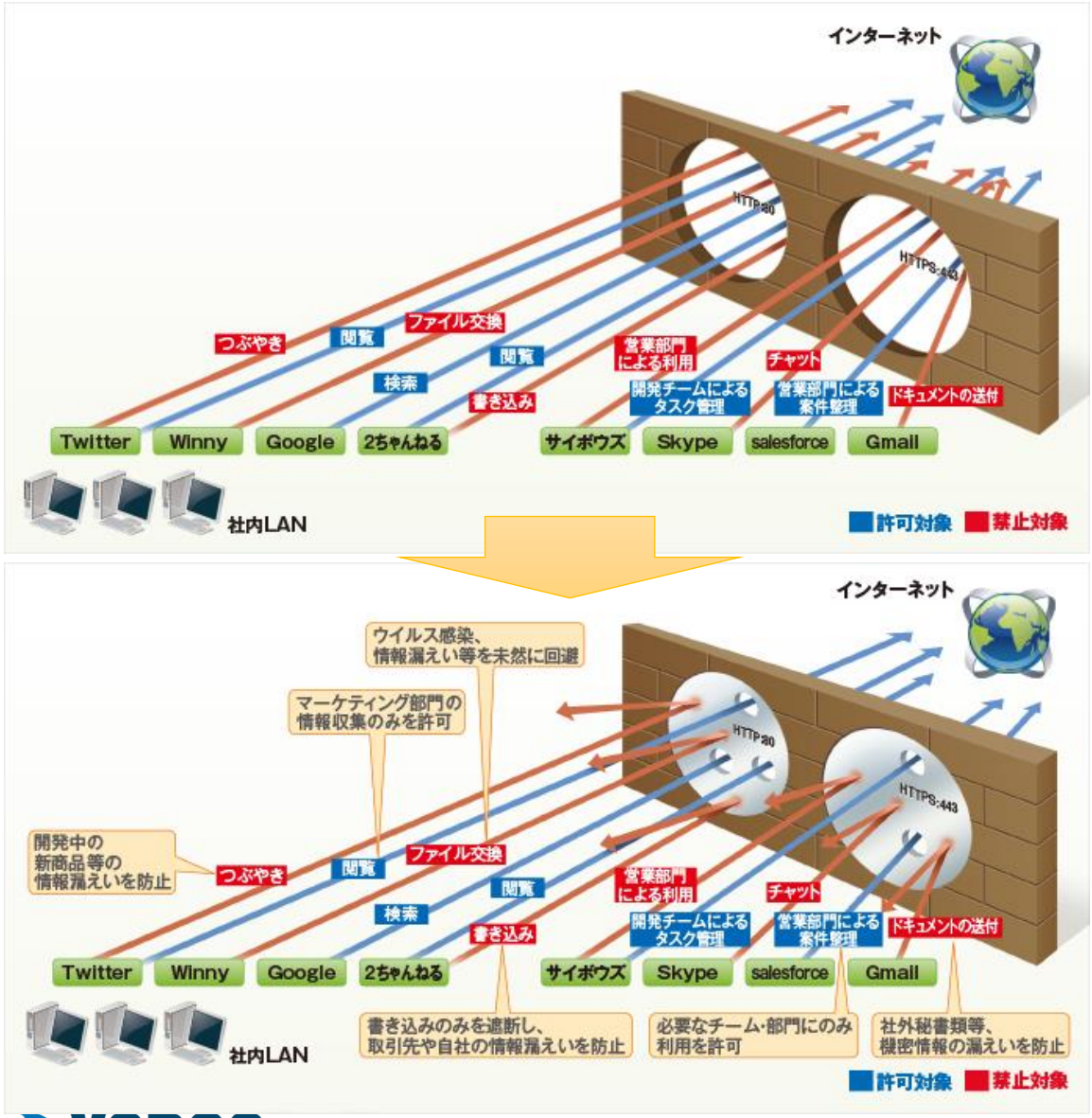
IDS/IPSの強みは、リアルタイムで異常を検知できる点にあります。アクセスログを解析して初めて不正アクセスがあったことに気がつくといった事態を防ぐことができます。

③ 柔軟な対応が可能

IDSでは、異常検知の報告があった後、いったんシステムを停止するか、暫定的な対策を施したうえでサービスを継続するかなど、柔軟な対応を取ることができます。また、IPSを活用すれば対策が急がれる攻撃に対して迅速な対処が可能です。



UTM機能ご紹介（アプリケーション制御）



アプリケーション制御が有効な理由

①セキュリティリスク

電子メールやFTPなどのデータを伝送するプロトコルは、データ流出の可能性があります。

②リソース使用量

ビデオ会議アプリなどは大量の高速ネットワーク帯域幅が必要になる場合があります。

③生産性への影響

電子メールやFTPなどのデータを伝送するプロトコルは、データ流出の可能性があります。

UTM機能ご紹介（サンドボックス）

サンドボックスは、特定のプログラムを実際の環境下で開く前に、いったん仮想環境下で開いて検証する役割を持っています。その上で、迷惑プログラムに該当しないか、ウイルス感染していないかなどを確認し、安全確認ができた後に実際のコンピュータで開く仕組みになっています。

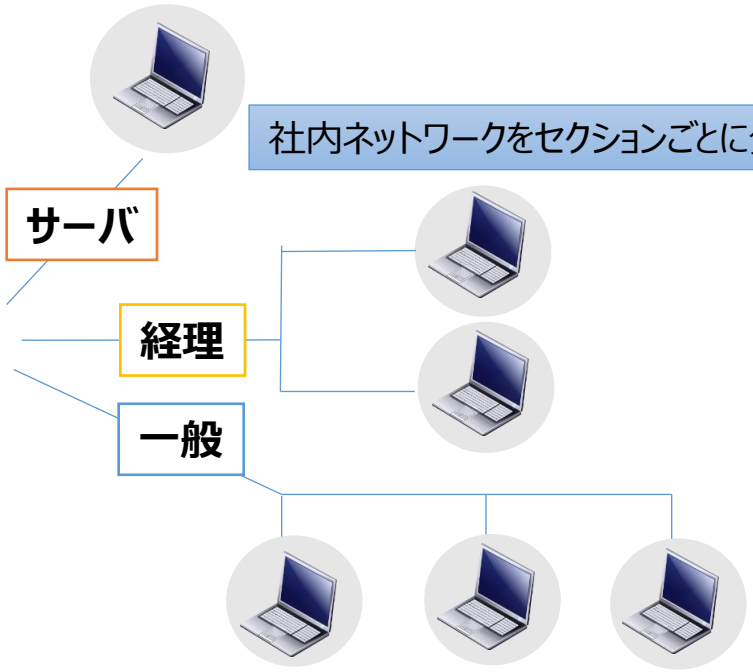
サンドボックスの仕組み

UTM導入後は・・・

①入口出口対策

外部からの脅威を総合的にブロック！

1台で複数のセキュリティー機能を搭載！
しかも管理や設定をサポート！



社内ネットワークをセクションごとに分割

問題のあるサイトへのアクセスをブロック！

セキュリティ機能のパッケージは、NGTPライセンスとNGTXライセンスの2種類がございます。

		ファイアウォール	アンチウイルス	アンチボット	アンチスパム	IPS	アプリケーションコントロール	URLフィルタリング	サンドボックス
NGTP	セキュリティ基本機能	●	●	●	●	●	●	●	
NGTX	セキュリティ基本機能＋サンドボックス	●	●	●	●	●	●	●	●

YODOQ
We keep chasing our dream

Check Point製品ラインナップ

①入口出口対策

	1535	1555	1575	1595	1600	1800	1900	2000
推奨台数※目安	15台	50台	80~100台	120~150台	200~250台	400台	800台	1000台
NGTXスループット（Smart Accel有効時）	440Mbps	600Mbps	650Mbps	900Mbps	2.0Gbps	2.6Gbps	–	–
NGTXスループット	340Mbps	450Mbps	500Mbps	660Mbps	1.5Gbps	2Gbps	4Gbps	5Gbps
NGFWスループット	600Mbps	800Mbps	970Mbps	1.3Gbps	3.2Gbps	5Gbps	8Gbps	10Gbps
モバイル・アクセス（同時接続）	標準100台 最大150台	標準100台 最大150台	標準200台 最大300台	標準200台 最大300台	500台	500台	500台	500台

Check Point	1535	1555	1575	1595	1600	1800	1900	2000
								

Fortigate	40F	60F	80F	100F	200F	400F

YODOQ
We keep chasing our dream

CheckPoint UTM基本サポート

基本サポートサービス

リモート保守・サポートをワンストップでご提供サービスです。ログの確認、設定変更、故障診断、先出センドバックの手配、セキュリティ診断レポートの配信など、幅広いサービスを提供しています。

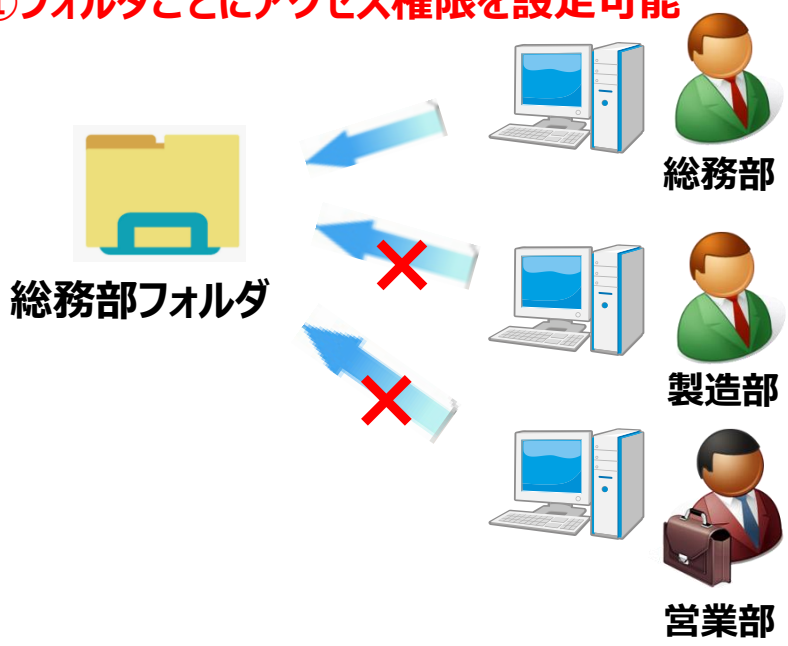
サービス項目		内容
保守	故障診断	障害時に遠隔でログを取得及び調査を実施
	先出しセンドバック	故障と判断した際の先出しセンドバック手配
サポート	問い合わせ対応	お客様からのお問い合わせに対し、機器状態の遠隔による確認、 設定変更手順等を案内
	設定	下記の機能に関する設定の追加、変更を遠隔で実施 ・アンチウィルス ・IPS ・アプリケーション制御 ・URLフィルタリング ・ファイアーウォール ・アンチスパム ・VPN ・アンチボット設定
	ファームウェアのアップデート	ファームウェアへのアップデート作業代行
レポート	セキュリティレポートの提供	メールによるセキュリティレポートを配信 ※月次/週次/日次より選択

ActiveDirectoryの特徴

Windows Server Active Directory

②サーバー一括管理

①フォルダごとにアクセス権限を設定可能



③windowsUpdateの制御が可能

windowsUpdateの
自動更新の停止を一括管理

④ネットワークドライブを一括設定可能

共有フォルダのドライブ設定を個人毎で設定せずとも、自動で表示されるようになります

②パスワードポリシーを設定可能

パスワード(NG)：123456

パスワード(OK)：arggtaf12Q

パスワードポリシー

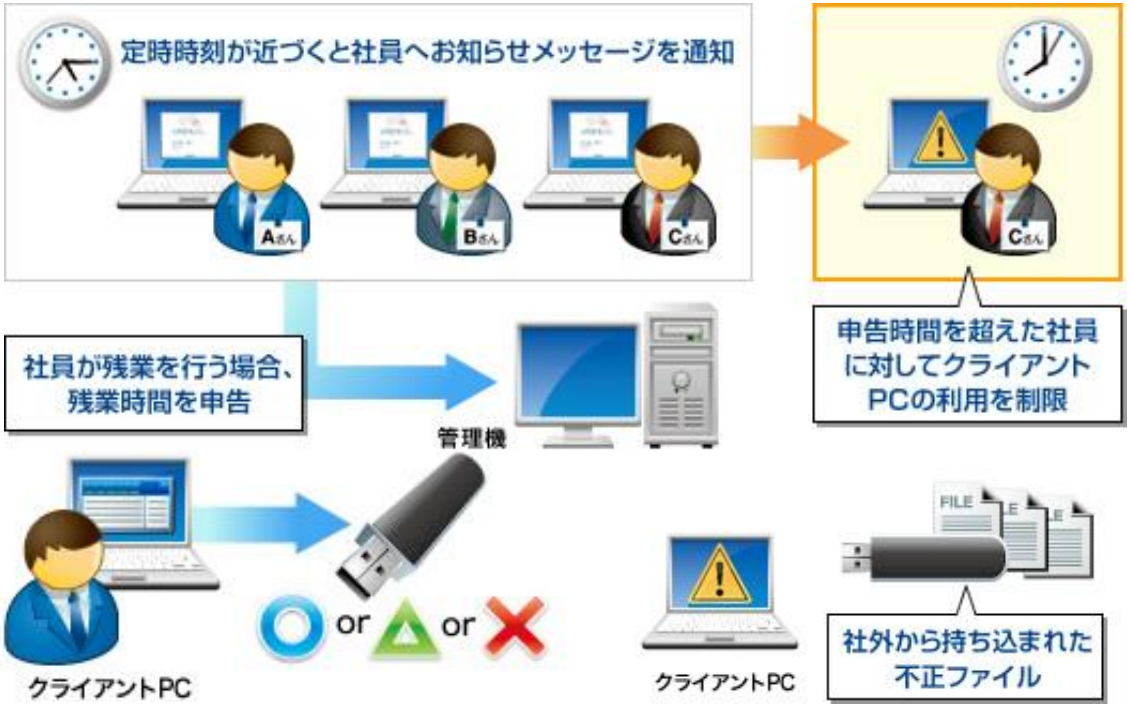
- 最低限の文字数の設定
- パスワードの有効期間の設定
- パスワードの履歴の記録
- 複雑さの要件を設定　など

YODOQ
We keep chasing our dream

クライアントセキュリティーの特徴

① 重要なファイルへのアクセスを監視・制限することができます。

② PCの利用履歴、インストールソフト、利用機器を把握できます。



③ メールの宛先、メールの内容添付ファイルをチェックすることができます。

ヨドックのオススメ構成

以下大手企業様でよくある基本的なセキュリティ構成です。

CheckPoint

①VPN接続時間・接続範囲の制限
（不正アクセス防止、社員労働状況の確認）
②WEB閲覧制限
（内部漏洩対策）
③ログの監視強化
（社員労働状況の確認、内部不正の検知・抑制）

SkySea

①ログ監査による操作履歴の確認
（社員労働状況の確認、内部不正の検知・抑制）
②DVD,USB等の外付けデバイスの使用制限
（内部不正の検知・抑制）
③セキュリティポリシーに違反する行為の検知・注意喚起
（内部漏洩対策）
④インストールアプリケーションの監視と削除
（内部漏洩対策）

ActiveDirectory

①ファイルアクセス権限の厳密化
（内部漏洩対策）
②パスワードポリシーの設定
（内部漏洩対策）

※一度に纏めて構築を実施した場合、
・運用の変更に社員の方が対応できない
・制限の増加により、既存システムの一部が障害を起こす
などが頻発する可能性があるため、順次導入をおすすめします。

※SkySea、ActiveDirectoryを導入する為にはオンプレサーバ、クラウドサーバが必要になります。

※SkySea、ActiveDirectory、VPNClientのクライアントPCへの導入作業については代表的な1台を設定し、その他のクライアントへのインストール作業は御社で実施していただくことを想定しています。この作業の為の手順マニュアル作成はお見積りに含まれます。全PCへの導入についてもご依頼ある場合は別途お見積りさせていただきます。

※ActiveDirectory導入においてファイルサーバの権限設定を行う必要がありますが、環境内容が不明の為見積には含まれていません。

らくらんセキュリティサポート の特徴

対応範囲が広い

- ネットワーク、サーバ、システム、ホームページと様々な要件に応えられる。
- ワンストップ対応の為、色々な業者を経由することがない。
- 様々なスキルをもった技術者が対応。

迅速な対応

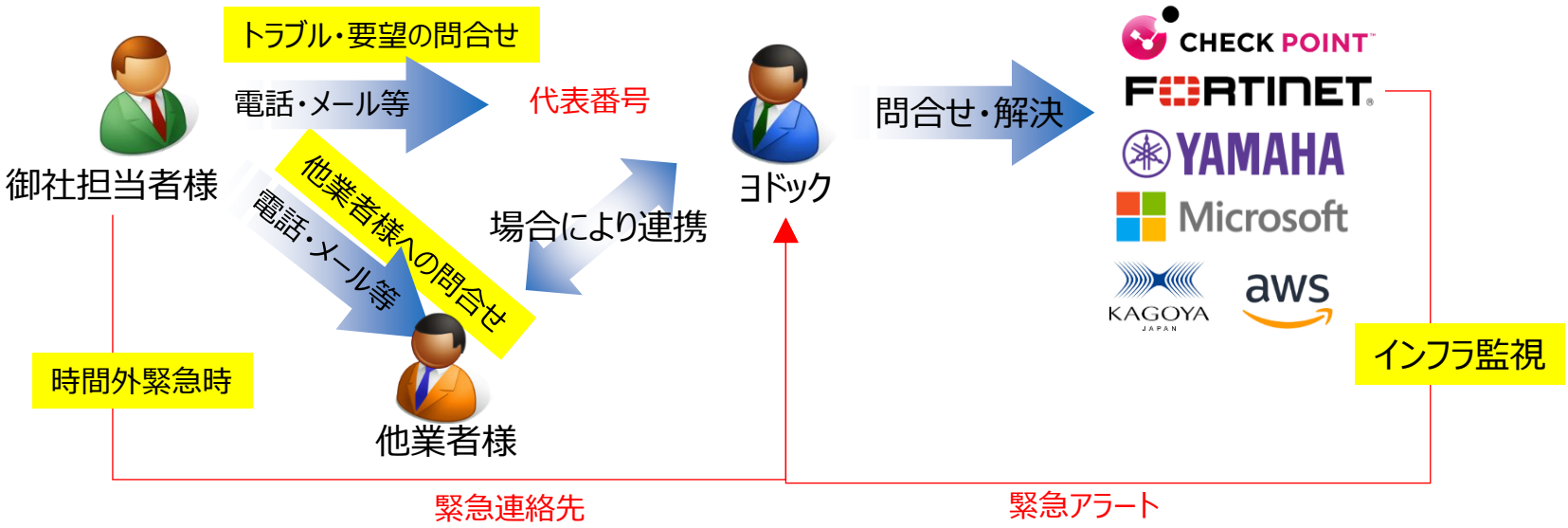
- 障害検知を自動化できるところは自動化しているので対応が早い。
- 有人対応時間範囲にて60分以内で初動対応。
- 24時間365日監視対応（監視プログラムが導入できる場合）

低コスト

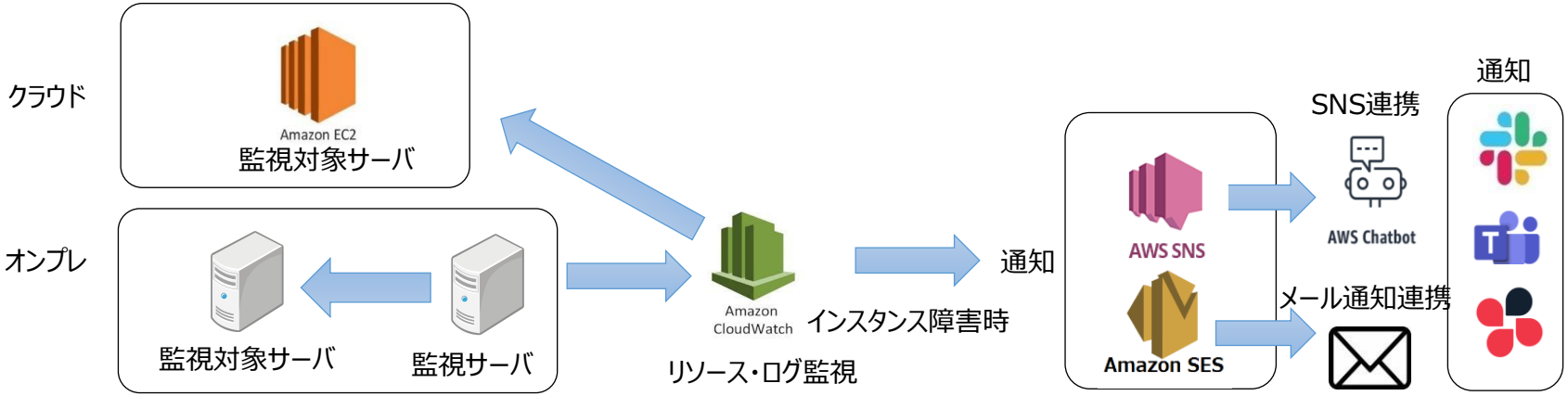
- 弊社の他の顧客と技術者をシェアする形式により価格を抑える。
- 対応範囲・規模感を決めることで価格を抑える。
- 様々な対応実績・構築実績により対応コストを抑える。

保守サービス提供イメージ

対応フロー



監視フロー



運用・保守内容

サービス時間条件

- 障害対応時間：有人対応時間範囲にて障害検知・お問合せ後、対応開始するまでを60分以内といたします。
  対応時間外については緊急通知・緊急ダイヤルに対してベストエフォートでの対応とします。
- 定期保守作業：計画的に停止する場合は御社相談のもと実施いたします。

支援内容

- 受付方法：電話問い合わせ、メールでの受付を実施いたします。
- 有人対応時間：月～金 ９：３０～１７：３０（土日祝除く）
- 実施方法：原則リモートでの対応とします。
- 実施内容：下記項目を自動又は手動にて対応します。

インフラ運用・保守内容例

Ping死活監視	バックアップ運用	各種設定変更	ログチェック	リソース監視による 問題発見・改善提案

システム運用・保守内容例

システム稼働チェック	利用に関わる お問合せ対応	ドメイン設定更新	SSL証明書更新	システムログチェック
システム調査作業	データパッチ作業	システムトラブル対応	バグ・不具合対応	

Total Solution Provider

YODOQ

We keep chasing our dream

株式会社ヨドック

【大阪本社】〒532-0011　大阪府淀川区西中島5-14-10 新大阪トヨタビル10F
TEL：06-6305-2278 （代表） FAX：06-6305-2279
【東京支店】〒101-0044　東京都千代田区鍛冶町1-6-15 井門神田駅前ビル4F
TEL：03-5843-7983
URL：https://www.yodoq.com/
e-mail：contact-hosyu@yodoq.com