セキュリティ
アップデートサービス

脆弱性とは

01.脆弱性とは

脆弱性とは、コンピュータのOSやソフトウェアにおいて、プログラムの不具合や
設計上のミスが原因となって発生した**「情報セキュリティ上の欠陥」**のことを言います。
脆弱性は、**セキュリティホール**とも呼ばれます。

脆弱性が放置されていると、**外部から攻撃を受けたり、ウィルスの感染**に利用されたり
する危険性があるため、インターネットに接続しているコンピュータにおける
情報セキュリティ上の大きな問題のひとつとなっています。

脆弱性が発見されると、多くの場合、ソフトウェアを開発したメーカーが更新プログラムを
作成し提供します。

脆弱性を防ぐには、**OSやソフトウェアのアップデートが必要**となります。
一度対応したOSやソフトウェアでも、新たな脆弱性が発見されるたびに
アップデートの対応が必要となるため、コンピュータを利用する限り
脆弱性に対して継続的な対策が可能な体制を構築する必要があります。

02.IPA情報セキュリティ10大脅威

セキュリティ被害の多くの要因がOSやソフトウェアの脆弱性となっています

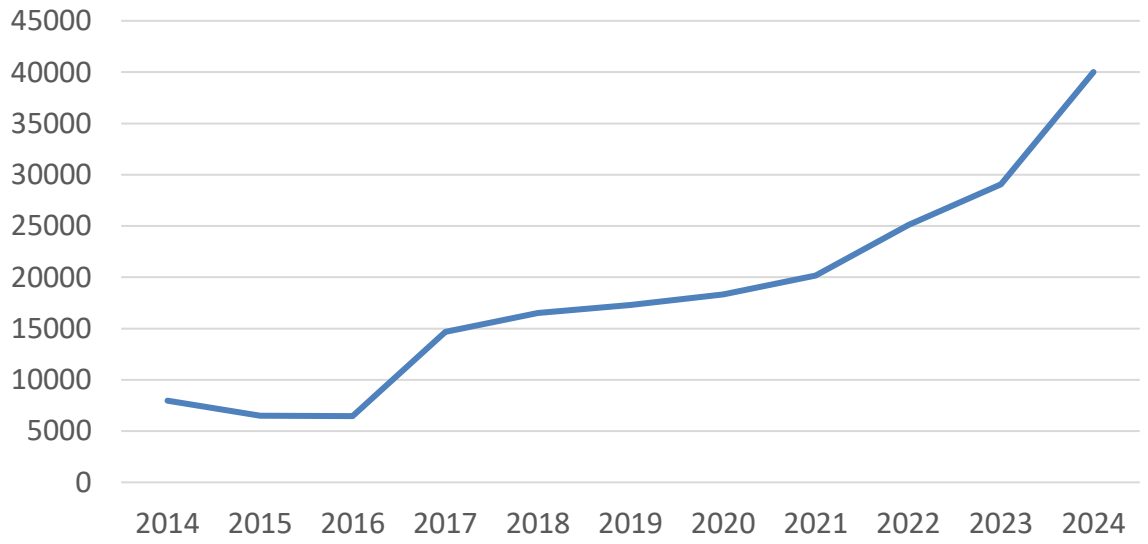
順位	情報セキュリティの脅威	インシデント発生要因
1位	ランサムウェアによる被害	OS・ソフトウェアの脆弱性／注意の欠落
2位	サプライチェーンや委託先を狙った攻撃	OS・ソフトウェアの脆弱性／セキュリティ対策レベルの格差
3位	システムの脆弱性を突いた攻撃	OS・ソフトウェアの脆弱性／セキュリティ対策レベルの格差
4位	内部不正による情報漏えい	情報管理の不足
5位	機密情報等を狙った標的型攻撃	監視・社内連携の不備
6位	リモートワーク等の環境や仕組みを狙った攻撃	監視・社内連携の不備
7位	地政学的リスクに起因するサイバー攻撃	情報管理の不足
8位	分散型サービス妨害攻撃（DDoS攻撃）	OS・ソフトウェアの脆弱性／対応の遅れ
9位	ビジネスメール詐欺	注意の欠落
10位	不注意による情報漏えい等	社内体制の不備／注意の欠落

出典:IPA 情報処理推進機構　情報セキュリティ10大脅威2025：https://www.ipa.go.jp/security/10threats/10threats2025.html

03.日々発見される脆弱性

年々脆弱性の報告件数は右肩上がりに上昇

年	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
CVE 登録件数	7949	6494	6458	14658	16521	17305	18323	20153	25084	29066	40009



2017年から急激に上昇
1日に平均約100件もの
脆弱性が報告されている

CVE:情報セキュリティにおける脆弱性について
それぞれ固有の名前や番号を付与したもの

04.脆弱性対策の課題

脆弱性は日々報告されるため、利用しているOSやソフトウェアに関する情報を
正確に把握し、アップデートの必要性や優先順位を決め
最終的な対処の判断を行う日々の運用が必要となります。

脆弱性対策フェーズ	課題
情報収集	JPCERTやJVNの情報を日々チェックするのが辛い 最適なパッチを探すのが大変
影響する情報の特定	どれが自分たちに必要な情報なのかわからない 利用しているOSやソフトウェアのメンテナンスが難しい
評価・優先順位づけ	パッチ適用は後回しになってしまう 属人化してしまっている
対処・管理	実際にどれほど対処されているかわからない 対策状況に関して確認する方法がわからない

サービス概要

05.セキュリティアップデートサービス

脆弱性情報の収集・評価・通知からアップデートまで行うセキュリティオプションサービス

① 脆弱性情報の収集

最新の脆弱性情報を収集・管理画面にて確認可能

② 脆弱性情報の配信

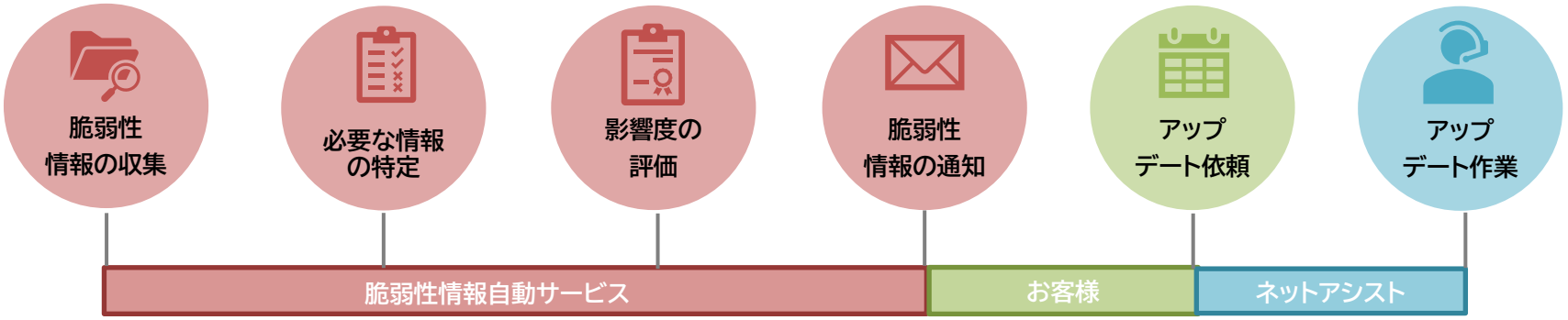
関連するOS・ミドルウェアの脆弱性情報を配信

③ 影響度の評価

関連する脆弱性の影響度を「数値」で判断できる

④ セキュリティパッチ

セキュリティアップデートでの脆弱性対応を実施



06.導入のメリット

セキュリティアップデートサービスは対象サーバに必要な脆弱性情報を自動で収集し
影響度をご案内。「重大」な脆弱性は、メール通知からセキュリティアップデートまで対応いたします

導入前の課題

**対象サーバに必要な脆弱性情報の提供や
脆弱性に対しての管理・運用はなし**

- 日々発見される脆弱性情報の収集が面倒・・・
- 自社サーバに現存する脆弱性が把握できない…
- セキュリティアップデートを実施する
タイミングが分からない…

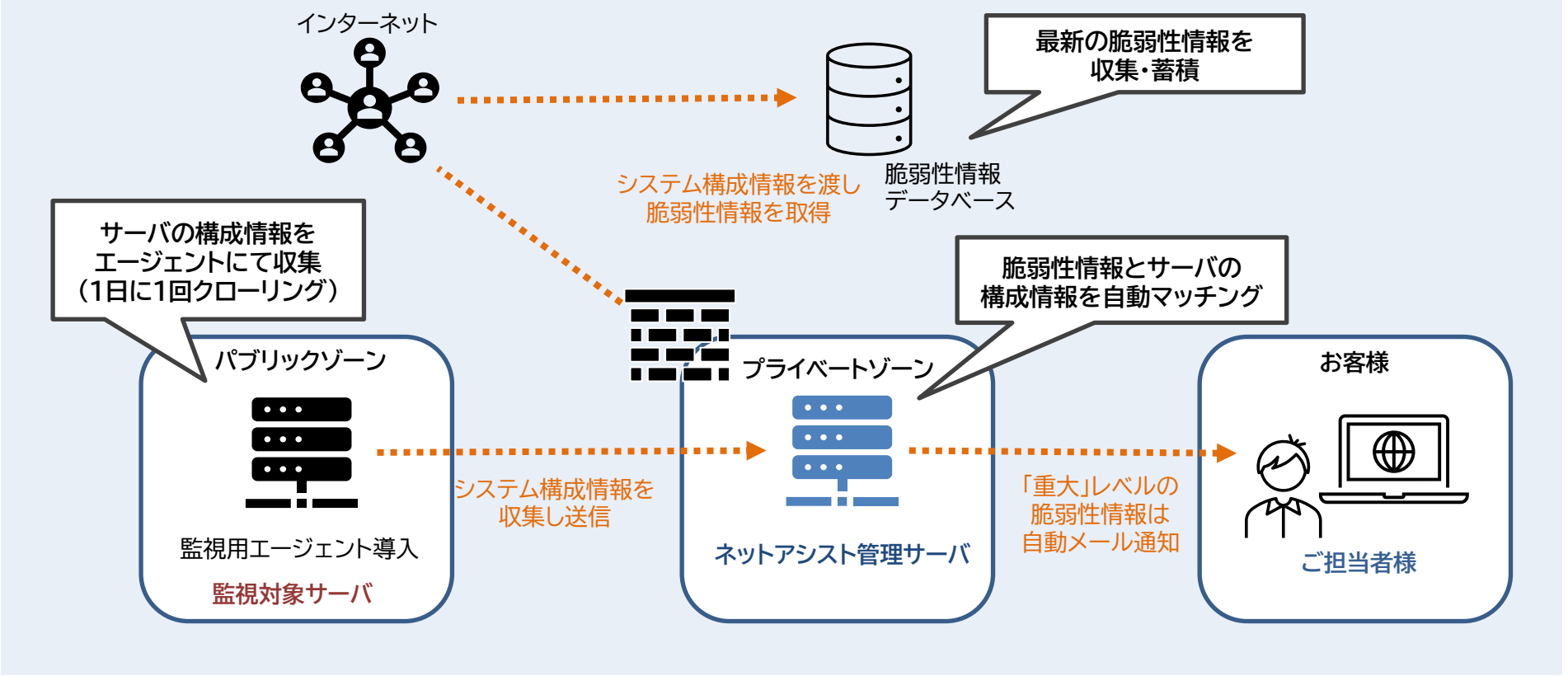
導入のメリット

**対象のサーバに対し適切な
脆弱性の情報提供や管理運用ができる**

- 重要な脆弱性情報を見過ごすことがない！
- 自社サーバに存在する脆弱性を把握できる！
- 脆弱性情報が来たら、アップデートを
依頼するだけでなので簡単！

07.脆弱性情報の管理の仕組み

脆弱性情報配信サービスシェア国内No.1の「SIDfm VM」を利用しサービスをご提供いたします
お客様に必要な脆弱性情報を日本語で提供する「脆弱性情報収集・管理ツール」です



- Linuxサーバへエージェントをインストールする際、Ruby/OpenSSL/unzipのインストールが必要です。
- Windowsサーバへエージェントをインストールする際、7zip等の解凍ソフトウェアのインストールが必要です。

08.SIDfm管理画面

管理画面にログインいただくことで、お客様サーバに現存する脆弱性情報を確認できます。
脆弱性情報の詳細や対処方法も管理画面上から確認が可能です。

脆弱性情報の詳細や対処方法などのお問合せは、原則対応いたしません

09.セキュリティアップデートサービス料金表

MSPアシスト/AWSアシストのオプションサービスとしてご提供いたします

初期費用／1台あたり（税抜き）
30,000円～　※すでにご契約頂いているお客様の場合は無償

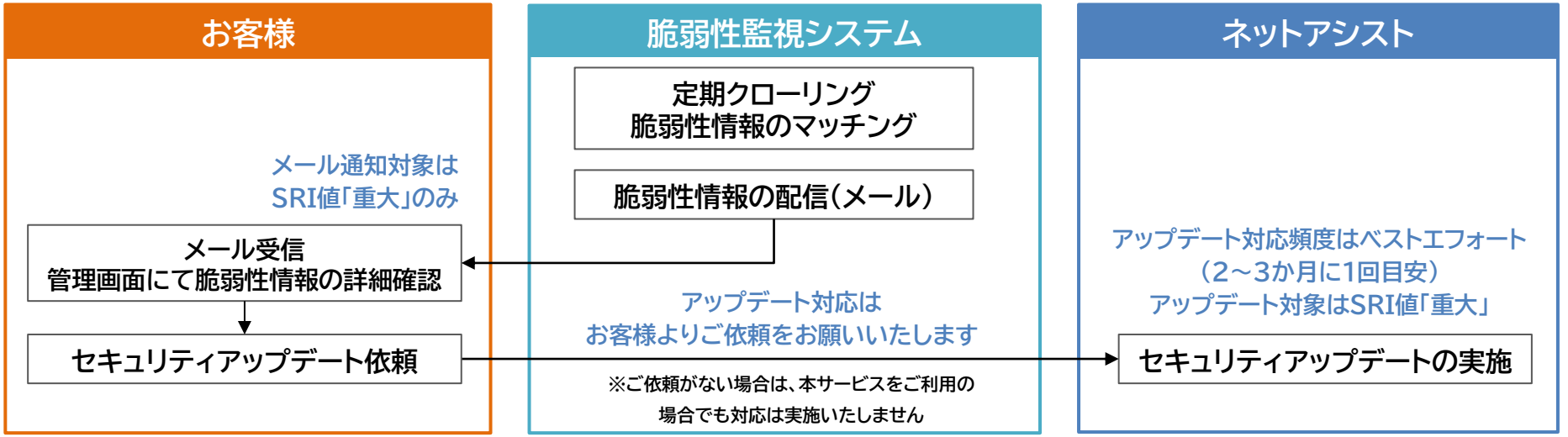
月額費用／1台あたり（税抜き）		
シルバープランご利用	ゴールドプランご利用	ゴールドプラスご利用
対象外	+20,000円～	+10,000円～

注意事項

セキュリティアップデートの際にスナップショットの取得や切り戻し作業、手順書の対応などをご希望の場合は対応内容によって初期費用・月額費用が増額になります。

本サービスをご契約いただいたお客様からのご依頼を優先して対応いたします。本サービスのご契約がないサーバのセキュリティアップデート対応（別途有償作業）は実施までお時間を頂きます。

10.脆弱性対応フロー



注意事項

- アップデート作業時に特別対応（切り戻しや手順書の対応）が必要な場合は日程調整に時間がかかります
- 新規の脆弱性が発見されてから、メール配信まで数営業日かかる可能性がございます
- セキュリティパッチの適用は公式よりパッチが配布されてからの対応になります