障害点（Point-of-Fail）：店舗システムがセキュリティの弱点になる理由

リテールは、最もサイバーセキュリティ攻撃の標的にされている業界[1]。

4社に3社
の小売事業者が過去にセキュリティ侵害を受けており、
そのうち**50%**の侵害は過去1年間に起きています[1]。

大きな損害をもたらすPOSのセキュリティ侵害。

- ブランドの評判の失墜
- ダウンタイムと生産性の低下
- 法務、コンプライアンス、ITのコスト

ある多国籍ホスピタリティ チェーンは、
2018年に起きた顧客データの漏えいから復旧するために、
合計約**10億ドル**[2]を費やしたと推定されています。

HPとインテルのソリューションがエンドポイントの回復性を強化

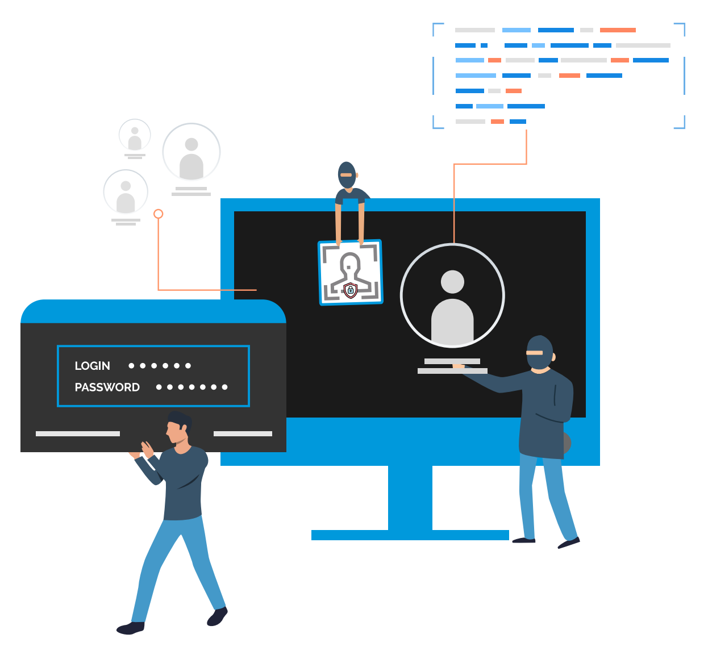
保護、検出、復旧の総合的なアプローチで、
小売事業者の回復性を確保できます。


包括的な保護

迅速な自己回復

インテリジェントな検出

あらゆる方向から脅威が迫る状況では、すべてのデバイスを網羅する階層的セキュリティが不可欠。



10件に1件
のWebリクエストがマルウェアに
つながっています。店舗スタッフは、
競合相手の価格、陳列レイアウト、
プロモーションを検索します[3]。

81%
のハッキング関連
セキュリティ侵害に、
安全性に疑問があるか脆弱な
資格情報が関わっていました[4]。

既知の攻撃と未知の攻撃をリアルタイムに検出。

2018年に成功した組織の
エンドポイントに対する攻撃のうち、
76%が
ゼロデイでした[5]。

従来のウィルス対策
ソリューションで阻止できる
ゼロデイ 攻撃は
43%に過ぎません[5]。

攻撃から速やかに復旧し、最悪なシナリオの影響を最小限に。

ある大手総合小売
事業者は、2019年に
2日間にわたって
10時間続いた
POS停止の間に、
推定**1億1,000万ドル**の
売上を損失しました[6]。

HPのPOSソリューションは業界をリードするセキュリティ機能を
備えており、セキュリティ侵害の対策、検出、復旧を支援し、
POSが障害点とならないようにします。

詳細について

レポートで詳細をご確認ください。

Three Key Imperatives for Enhanced Endpoint Resilience（エンドポイントの回復性強化に必要な3つの課題）

レポート全文を読む

HPは幅広いPOSデバイスのポートフォリオで、小売事業者とホスピタリティ事業者がお客様のニーズにいつでもどこでも応えられるよう支援します。従来式POSからモバイルPOSまで、HPは従業員を支援し、お客様のエンゲージメントを促進するテクノロジー ソリューションで、カスタマー エクスペリエンスに変革をもたらします。HPはデバイス設計からセキュリティを組み込みます。詳細をご覧ください。

www.hp.com/go/retail

Intel® AMTを搭載したIntel vPro®プラットフォームにより、ソフトウェアのリモート更新、ソフトウェアに関連した問題の発見と解決、さまざまな修理に伴う高額な電話および出張サービスの解消、既存のHPセキュリティ ソリューションを補完するハードウェア ベースのセキュリティ層の追加が可能になります。HPのリテールとホスピタリティのお客様に、複雑なデバイス管理を必要とする新しいエクスペリエンスを提供できます。

https://www.intel.com

出典：

1. Thales『Data Threat Report, 2019』（2019年データ脅威レポート）
2. Bloomberg Intelligence
3. Symantec『Internet Security Threat Report, 2019』（2019年インターネット セキュリティ脅威レポート）
4. Verizon『Data Breach Investigations Report, 2019』（2019年データ侵害調査レポート）
5. Ponemon Instituteの『State of Endpoint Security Risk Report, 2018』（2018年エンドポイント セキュリティ リスク状況レポート）
6. 2019年CNBC

4AA7-6633JPN 、2020年12月