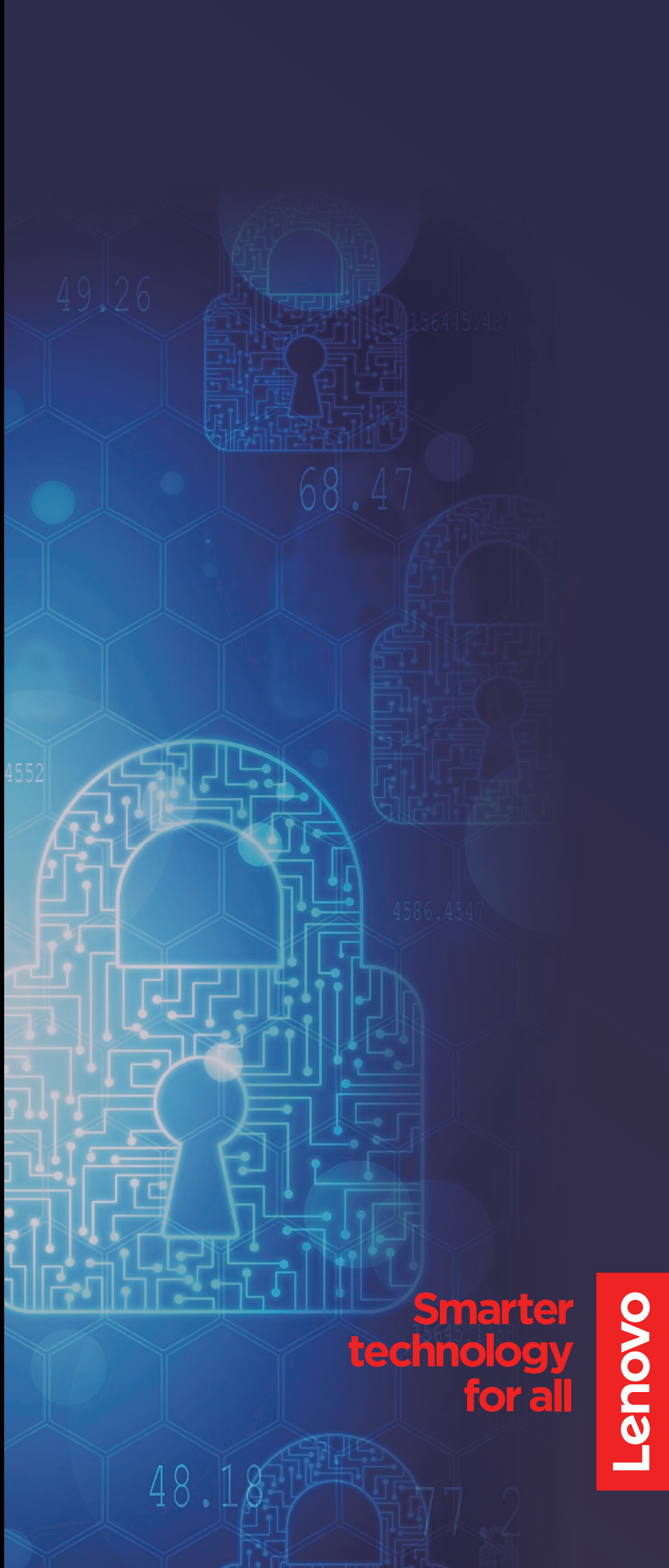
ThinkShield

ハードウェアベンダーならではの
セキュリティ・ソリューション

- 開発製造
- ファームウェア
- 盗難紛失
- ソーシャルハッキング
- サイバー攻撃



Windows 10

Smarter technology for all

Lenovo

ThinkShield

SECURITY = DATA

時代の変化と共に、ようやく真の意味で
“場所と時間を問わない働き方”の普及がはじまっています。
その一方、PCを持ち運ぶが故に高まる
セキュリティリスクに対する対策の重要性も強まるばかりです。
特に情報漏洩対策、すなわち“データ”保護の観点では、
従来からのエンドポイントセキュリティはもちろんのこと、
ハードウェア、そしてファームウェアの観点でも対策を
検討することが必要になってきています。
レノボのThinkShieldソリューションは
ハードウェアを製造しているメーカーならではの観点で
お客さまのセキュリティ対策に貢献します。

THE DATA SECURITY

情報セキュリティにおいて、何よりも守るべきなのはお客さまの大切な“情報”です。
ThinkShieldはハードウェアベンダーならではの観点で、お客さまの情報漏洩対策を強力にサポートします。

“Data”
情報の漏洩

開発製造

開発～製造～納品段階で
混入する潜在的な脅威に対応

- Trusted Supplier プログラム
- 信頼されたサプライチェーン
- パッケージングセキュリティー
- 独立したセキュリティオフィス

ファームウェア

ファームウェア以下の
レイヤーでの脅威に対応

- 自己回復BIOS
- クリーンなプリロードイメージ
- RTPプリロードイメージ
- Thunderbolt セキュリティー
- System Update
- 脆弱性対応
- ThinkShield Secure Wipe
- 物理ポートコントロール
- SecureDoc
- dTPM & BitLocker

盗難紛失

盗難紛失時に発生する
脅威に対応

- セキュアドッキング
- アセットタグ
- 自己暗号化ドライブ
- ドライブ暗号化サービス
- セキュア ハードドライブ
- ディスク返却不要サービス
- Absolute
- BIOSアセット情報エリア

ソーシャルハッキング

ソーシャルハッキングに対応

- ThinkPad Privacy Guard
- ThinkPad Privacy Alert
- Windows Hello
  - Match-on-Chip 指紋認証
  - IRカメラによる顔認証
  - 指紋認証マウス
  - NFC Tap-to-Login
- Smart USB Protection
- Tamper Detection
- ThinkShutter

サイバー攻撃

サイバー攻撃に対応

- SentinelOne（センチネルワン）
- Lenovo WiFi セキュリティー

NIST Cyber Security Frameworkへの対応

“企業”として準拠が求められる可能性のあるNIST SP800-171をはじめとするセキュリティ基準に対して、
ThinkShieldソリューションは保護のために必要なハードウェア・ファームウェアレベルでのコンポーネントを提供します。

ID 識別

- Trusted Supplier プログラム
- 信頼されたサプライチェーン
- パッケージングセキュリティー
- 独立したセキュリティオフィス

PR 防御

- 自己回復BIOS
- Match-on-Chip指紋認証
- IRカメラ
- スマートカードリーダー/ NFC
- ThinkShutter
- 自己暗号化ドライブ
- ThinkPad Privacy Guard
- ThinkPad Privacy Alert
- Lenovo WiFi セキュリティー
- LTE対応
- セキュアドッキング
- アセットタグ/BIOS情報エリア
- Lenovo EaaS with Blancco
- SentinelOne（センチネルワン）

DE 検知

- 自己回復BIOS
- Secure Boot
- Tamper Detection
- Lenovo Vantage
- System Update
- Lenovo PSIRT
- MACアドレスパススルー
- SentinelOne（センチネルワン）

RS 対応

- 自己回復BIOS
- Secure Boot
- ThinkShield Secure Wipe
- Tamper Detection
- 独立したセキュリティオフィス
- SentinelOne（センチネルワン）

RC 復旧

- 自己回復BIOS
- Secure Boot
- SentinelOne（センチネルワン）

Windows 10

Windows 10 Pro を搭載した世界トップ クラスのデバイス

ThinkShield × 働き方改革

時間と場所を問わない働き方の普及により、PCに求められるセキュリティ要件も変化を遂げています。
ThinkShieldソリューションを搭載したThinkPadは、テレワーク先でも高いレベルのセキュリティを提供します。

テレワークセキュリティガイドラインへの対応

システム管理者が実施すべき対策

情報セキュリティ保全対策の大枠

- 情報のレベル分けに応じて、電子データに対するアクセス制御、暗号化の要否や印刷可否などの設定を行う
  ➡ Windows Information Protection

悪意のソフトウェアに対する対策

- フィルタリング等を用いて、テレワーク勤務者が危険なサイトにアクセスしないように設定する
  ➡ Lenovo WiFiセキュリティー、Windows Defender SmartScreen
- テレワーク勤務者がテレワーク端末にアプリケーションをインストールする際は申請させ、情報セキュリティ上の問題がないことを確認した上で認める
  ➡ Windows Defender Application Control
- 貸与用のテレワーク端末にウイルス対策ソフトをインストールし、最新の定義ファイルが適用されているようにする
  ➡ Windows Defender ウイルス対策
- 貸与用のテレワーク端末のOSおよびソフトウェアについて、アップデートを行い最新の状態に保つ
  ➡ Lenovo Vantage、サポートサイト上でのドライバ公開
- ランサムウェアの感染に備え、重要な電子データのバックアップを社内システムから切り離した状態で保存する
  ➡ Windows Defender Exploit Guard

重要情報の盗聴に対する対策

- テレワーク端末において無線LANの脆弱性対策が適切に講じられるようにする
  ➡ Lenovo WiFiセキュリティー、LTE内蔵ノートブック

不正侵入・踏み台に対する対策

- 社外から社内システムへアクセスするための利用者認証について、技術的基準を明確に定め、適正に管理・運用する
  ➡ Match-on-Chip指紋認証、IRカメラ、FIDO対応スマートカードリーダー

参照情報: 総務省 テレワークセキュリティガイドライン（第4版）
http://www.soumu.go.jp/main_content/000545372.pdf

テレワーク勤務者が実施すべき対策

悪意のソフトウェアに対する対策

- アプリケーションをインストールする際は、システム管理者にその旨を申請し、許可を受けたアプリケーションのみをインストールする
  ➡ Windows Defender Application Control
- 作業開始前に、テレワーク端末にウイルス対策ソフトがインストールされ、最新の定義ファイルが適用され最新の状態であることを確認する
  ➡ Windows Defender ウイルス対策
- 作業開始前に、テレワーク端末のOSおよびソフトウェアについて、アップデートが適用され最新の状態であることを確認する
  ➡ Lenovo Vantage
- テレワークにはルールに定められた情報セキュリティ対策が適用されているものを使用し、スマートフォン、タブレット等に関しては不正な改造（脱獄、root化等）を施さない
  ➡ Tamper Detection、自己回復BIOS

端末の紛失、盗難に対する対策

- 機密性が求められている電子データを極力管理する必要が無いように業務の方法を工夫する。やむを得ない場合は必ず暗号化して保存するとともに、端末や電子データの入った記憶媒体（USBメモリ等）等の盗難に留意する
  ➡ BitLocker、WinMagic、Absolute

重要情報の盗聴に対する対策

- 無線LAN利用に伴うリスクを理解し、テレワークで利用する場合は確保すべきセキュリティレベルに応じた対策が可能な範囲で利用する
  ➡ Lenovo WiFiセキュリティー、LTE内蔵ノートブック
- 第三者と共有する環境で作業を行う場合端末の画面にプライバシーフィルターを装着したり、作業場所を選ぶ等により、画面の覗き見防止に努める
  ➡ ThinkPad Privacy Guard、ThinkPad Privacy Alert、専用プライバシーフィルター

不正侵入・踏み台に対する対策

- 社外から社内システムにアクセスするための利用者認証情報（パスワード、ICカード等）を適正に管理する
  ➡ Match-on-Chip指紋認証、顔認証用のIRカメラ、スマートカードリーダー、FIDO対応

Windows 10

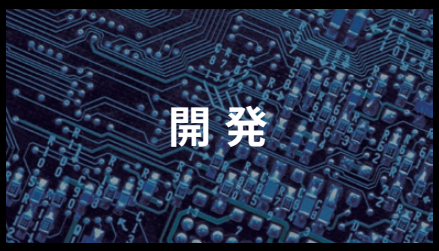
Windows 10 Pro を搭載した世界トップ クラスのデバイス

Security by Design

開発・製造段階での取り組み

セキュリティありきのプロダクトライフサイクルマネジメント

レノボでは製品開発段階にはじまり部品の調達、製造、そしてお客さまのお手元に届くまで、
包括的なプロダクトセキュリティを念頭に置いてライフサイクルマネジメントを行っています。
製品がお客さまのビジネスの保護に寄与することが、私たちの優先事項です。



- ハードウェア/ファームウェアレベルでのセキュリティ機能の実装
- 製品セキュリティポリシー開発ガイドの標準化
- 独立したProduct Security Officeによるセキュリティ レビュー

- Trusted Supplier Program
- 工場に対する物理アクセスの管理
- 安全な製造プロセス
- ソフトウェアイメージング及びBIOSの安全な配布

- 不正開封防止包装の実装
- 安全な物流サプライヤーとの連携
- 追跡、監査可能な体制

- PSIRTチーム
- ソフトウェア脆弱性への対応
- 信頼された交換要部品の調達
- ドライブ消去を含むプロセスを経た安全な廃棄/リサイクルプロセス

Windows 10

Windows 10 Pro を搭載した世界トップ クラスのデバイス

脆弱性への対応

レノボでは、お客さまとそのデータを保護するために、脆弱性対応に対するプロセスを整えています。セキュリティ研究者、学者、および広域なセキュリティ・コミュニティその他の方々からの脆弱性に関する情報を歓迎します。

脆弱性対応プロセス

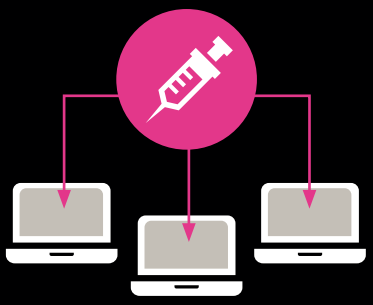
1. CVE番号の割当

レノボのPSIRTは脆弱性をご指摘くださる方々と連携すると共に、関連するすべてのご提案/お問い合わせに2営業日以内に返答します。当社のCVE Number Authority Information Sharing and Embargo Policyに従ってCVE識別子を割り当てる場合があります。

2. 修正プログラムの開発と公開

PSIRTによる問題の調査の後、修正プログラムを開発または調達し、お客さまにできる限り迅速に提供します。レノボでは、常にプラットフォーム ソフトウェアの最新バージョンを実行することを強く推奨しています。そのため、support.lenovo.comで入手可能な最新バージョンに対してのみ、セキュリティ脆弱性を評価します。

※オペレーティングシステムのセキュリティ脆弱性については、ご使用のOSベンダーに連絡することをお勧めします



レノボ セキュリティ アドバイザリ

最新の脆弱性情報をご確認いただけるポータルサイトをご用意しています。
https://support.lenovo.com/au/ja/product_security/home

独立した Product Security Office（PSO）

PSOでは、ソフトウェアコーディングとセキュリティ、ネットワーク、ハードウェア、サプライチェーンロジスティクス、脆弱性テスト、業務管理、サプライヤへの対応、社外とのインシデントコミュニケーションなどさまざまなスキルを持った人材を集めています。

主なセキュリティ上の役割	成果物
セキュリティ標準	● 製品アーキテクチャーのサポート ● 認定 ● 品質、標準、ツール
PSIRT	● すべてのセキュリティインシデントのリスク最小化 ● 顧客および社内とのコミュニケーション ● ポリシーと手順の維持
サプライチェーン	● Trusted Supplier Program ● BIOSおよびファームウェアビルドプロセス ● 安全な製造、梱包、出荷、配送 ● ポリシーと手順の維持
ガバナンスとコンプライアンス	● ガバナンス/ポリシー/手順 ● トレーニングとコミュニケーション ● 監査（社内監査および第三者監査） ● コードの保証とコンプライアンス

Security on Firmware

ファームウェアレイヤーでのセキュリティ

自己回復BIOS

ThinkPad 2020年*モデルに搭載された自己回復BIOSにより、ファームウェアレベルでのサイバー攻撃に対して自動的に正常なBIOS / UEFIへのリカバリーを実施する機能が搭載されています。

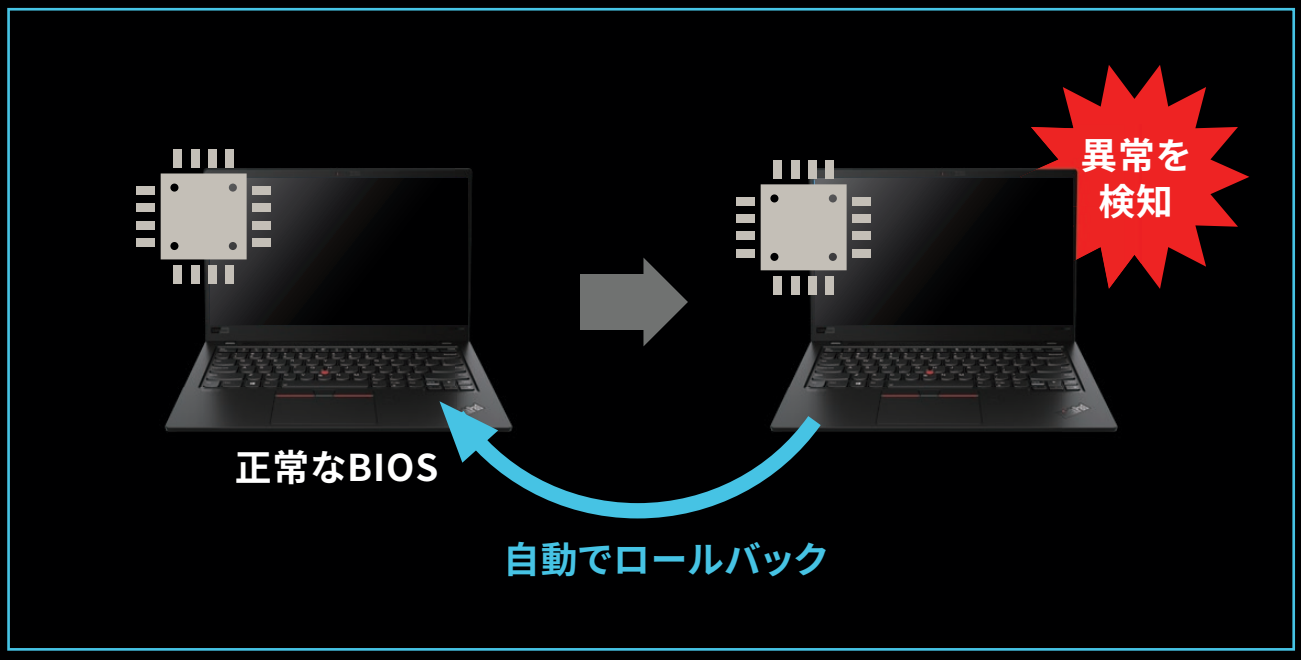
* ThinkPad Eシリーズ、ThinkPad Lシリーズ（13インチ）およびAMD製APUを搭載したモデルは対象外

どのような脅威に対して対応するのか

- BIOSなどのファームウェアレイヤーを狙う攻撃者からの潜在的な攻撃に対する保護
  - OSより上位のレイヤーからアクセスができないことから既存のエンドポイントセキュリティでは検出できない可能性
  - 感染後、リカバリを実施するためにはシステムボードの交換等が必要なため困難
- BIOSアップデートに万が一失敗した場合、ハードウェアレベルでの対処が必要となる可能性があり、回復が困難

どのように保護されるのか

1. 正常な状態でBIOS / UEFIのバックアップを保存
2. BIOS / UEFIに対する改ざんが検知された場合、自動的にロールバックを実施
3. BIOSアップデートが正常に終了しなかった場合にも、自動的にロールバックを実施



Windows 10

Windows 10 Pro を搭載した世界トップ クラスのデバイス

物理ポートコントロール

ThinkPad、ThinkCentre、およびThinkStationにはBIOS / UEFI上の設定変更により本体に内蔵されたI/Oポートのアクセス制御が可能です。さらに、ThinkCentreに搭載されたSmart USB Protectionでは、USBポート経由の通信の制御も設定可能です。

どのような脅威に対して対応するのか

- USBポートなど経由での不正侵入や情報漏洩は、ネットワークレイヤーでの監視では防ぐことができない脅威
- サードパーティーの資産管理アプリケーションやMDM経由での制御の場合、追加のコストや工数が課題
- セキュリティ上の理由でマイクやカメラからの潜在的な盗撮/盗聴リスクが発生するケース

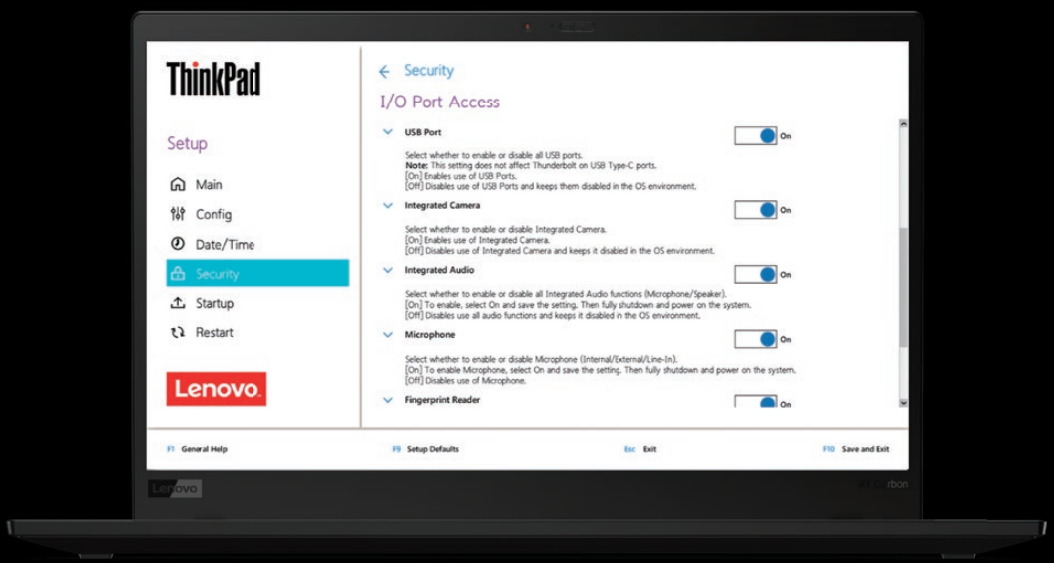
どのように保護されるのか

- I/Oポートの有効化、無効化をBIOS / UEFI上で設定可能
- OSよりも下のレイヤーで無効化されるため、アプリケーションレイヤーでの誤用を事前に防止
- ThinkCentreに関しては、USBポート経由の通信をRead Only / データ転送禁止に設定可能
- PC使用期間中にポリシーが変わった場合でも、BIOS / UEFIの設定により柔軟に対応可能
  （例: オンライン会議の利用を開始したため、Webカメラの使用禁止を解除したい）
- スーパーバイザーパスワードにより、エンドユーザーが変更できない設定とすることが可能

制御可能なI/Oポートアクセスの例

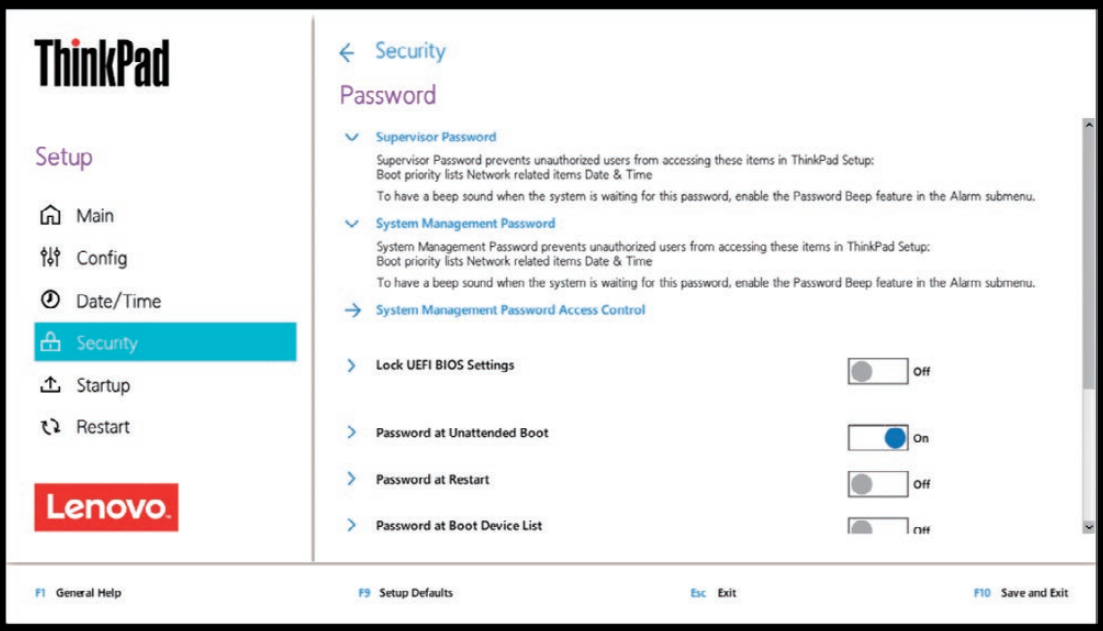
- ☑ Ethernet LAN
- ☑ Wireless LAN
- ☑ Wireless WAN
- ☑ Bluetooth
- ☑ USB Port
- ☑ Memory Card Slot
- ☑ Integrated Camera
- ☑ Integrated Audio
- ☑ Microphone
- ☑ Fingerprint Reader
- ☑ Thunderbolt™ 3

※モデルによって設定可能な項目は異なります



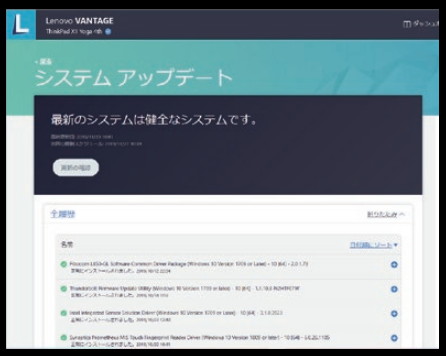
バックドアのない スーパーバイザーパスワード

レノボの提供するUEFI/BIOSにはスーパーバイザーパスワードをリセットするためのバックドアがありません。これにより、意図しない操作や設定変更によるリスクを最小限に留めます。



Lenovo Vantage System Update

プリインストールされた純正ユーティリティ“Lenovo Vantage”にはファームウェアの自動更新をサポートするSystem Updateが実装されています。また、アップデートはWebサイト上でも公開しています。



セキュアなアップデート/パッチ提供

Think製品が提供するBIOSアップデートはSHA 256/RSA 2048を利用した署名により安全性が担保されます。また、ドライバーのアップデートについても同様にデジタル署名を行っています。

Windows 10

Windows 10 Pro を搭載した世界トップ クラスのデバイス

Tamper Detection

ThinkPadに搭載されたTamper Detectionは、PC内部への不正な侵入に対する保護を提供します。裏蓋が開けられたことをセンサーによって検知し、起動時にスーパーバイザーパスワードの入力を求めることで、物理的なセキュリティインシデントのリスクを最小化します。

どのような脅威に対して対応するのか

- ハードウェアレベルでの改竄 / 不正なモジュール取り付け等の潜在的なリスク
  アプリケーションレイヤーで検知できない場合、リスクが継続的なものとなる場合も
- 知らない間にストレージの一時取り外しがあった場合にも気付くことができない

どのように保護されるのか

- 裏蓋の開閉を独立したコントロールチップであるThinkEngineとの連携で検知
- 裏蓋の開閉を検知した場合、次回PCの起動時にスーパーバイザーパスワードの入力が必須。
  エンドユーザーが起動できなくなるため、IT部門が不正なハードウェアコンポーネントへの侵入に気付くことが可能

プリロードされたクリーンなOSイメージ

ThinkPadにプリインストールされているWindows 10 Proのイメージに搭載されているアプリケーションは
Windows標準で搭載されているアプリを除くと、ドライバ、純正ユーティリティのみの最小限な構成です。

* 一部モデルを除きます

どのような脅威に対して対応するのか

- 普段使用されていないプリインストールアプリケーションがアップデートされていないことにより、脆弱性への対応が行われないまま放置されてしまうリスクが存在
- 意図しないアプリケーションがプリインストールされることにより、そこからの情報漏洩リスクが存在

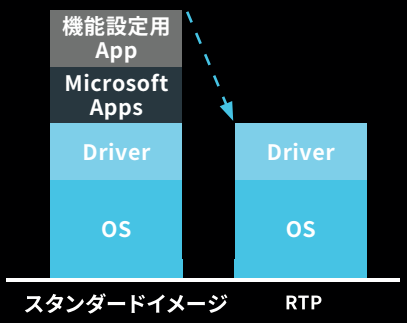
どのように保護されるのか

1. お客さまが本当に必要となる（PCの動作に必要な）最小限のアプリケーションのみを導入
   ※ Windows 10標準のApp + ドライバー + Lenovo Vantage等のユーティリティ
2. 独立したProduct Security Officeによるプリインストールアプリケーションへの厳しいレビュー

Ready to Provision

Modern ITデプロイメントに最適なカスタムプリロードイメージ

OS標準の基幹アプリ、そして動作に必要な最小限のドライバー以外を削除することによりModern ITデプロイメントを実施する際のプロビジョニングのベースとしても最適なクリーンなOSイメージです。ファクトリーサービスとして提供しています。



Windows 10

Windows 10 Pro を搭載した世界トップ クラスのデバイス

ThinkShield Secure Wipe

2020年*モデルのThinkPad*に組み込まれた、ファームウェアレベルで起動可能な内蔵ドライブのデータ消去のためのソリューション。GUIベースで直感的に利用可能、また機能の有効化や無効化はBIOS / UEFI上から設定可能。

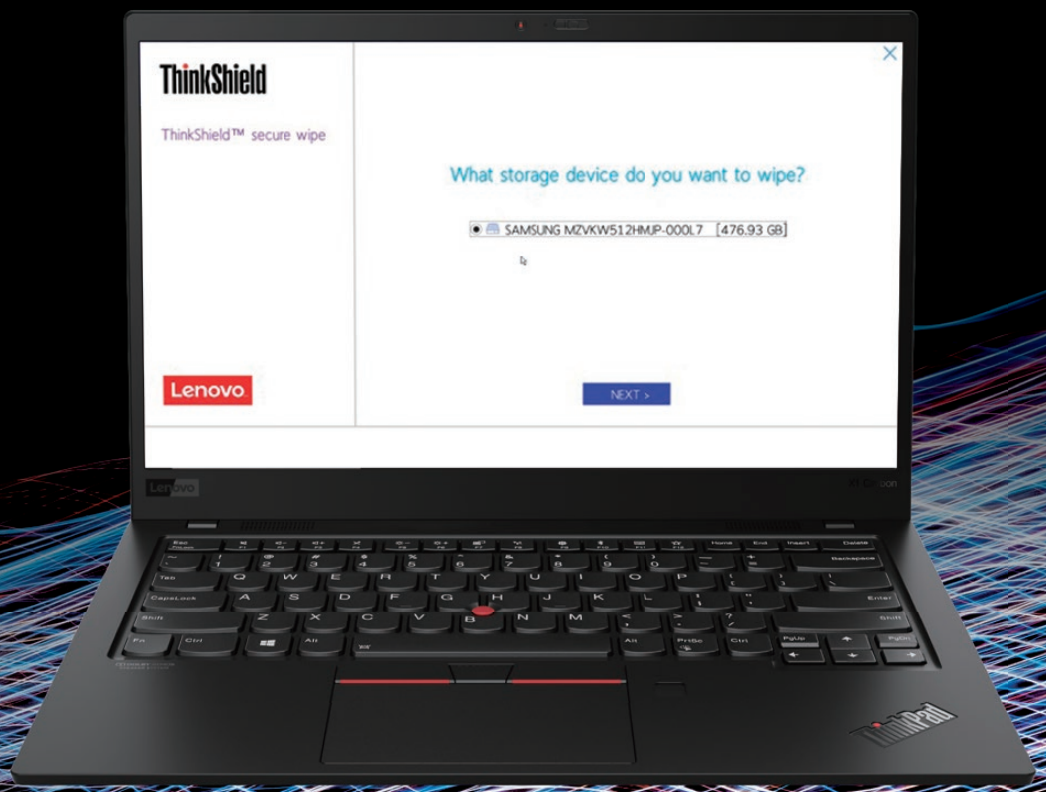
* ThinkPad Eシリーズは対象外
* ストレージの種類によっては対応しない場合があります

どのような脅威に対して対応するのか

- PCの廃棄や売却時に適切なかたちでデータ消去を実施しないと後から第三者に重要データを復元される潜在的なリスクが存在
- サードパーティー製のデータソフトウェアやクラウドソリューションの場合、管理工数、導入費用面等など、追加のコストが発生

どのように保護されるのか

1. ファームウェアレイヤーに出荷段階から組み込まれている機能で起動時にF12を押下することでThinkShield Secure WipeをOSレイヤーより下で起動することが可能
2. データ消去コマンドを実行した場合、データ消去コマンドを選ぶことで標準的なデータ消去メソッドに沿うかたちでデータ読み出し不可状態に



Windows 10

Windows 10 Pro を搭載した世界トップ クラスのデバイス

Lenovo

Security for Lost Device Prevention

盗難紛失対策

Absolute

Absolute Data & Device Security（Absolute）はThinkPadのBIOS / UEFIにエージェントが組み込まれた盗難、紛失時の情報漏洩対策と資産保護のためのソリューションです。

どのような脅威に対して対応するのか

- テレワークの普及などによりPCの持ち出しが増えると、比例してデバイスの盗難紛失のリスクが増大
- 盗難紛失後、PC内のデータが漏洩する“情報漏洩事故”の危険性が極めて高い
- 悪意のある攻撃者が管理用のMDMエージェントを削除することで追跡を逃れる可能性も

どのように保護されるのか

- 位置情報トラッキング機能によるデバイス位置の特定
- 遠隔デバイスロック / データ消去によるリスクの低減
- BIOS / UEFIにエージェントが組み込まれており
  万が一エージェントが削除された場合でも自動的に再インストールが可能
- 盗難デバイスの発見・回収サービスも提供

Windows 10

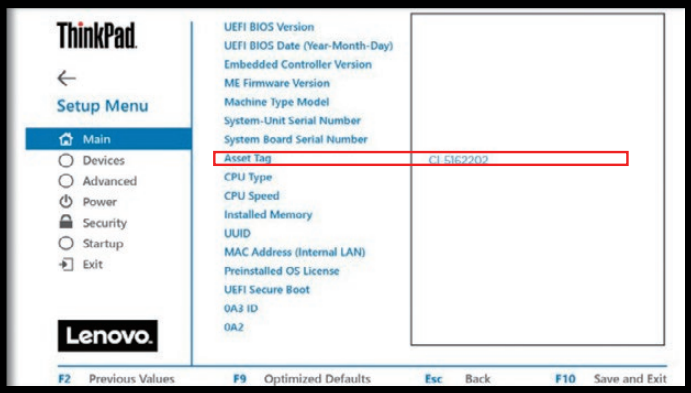
Windows 10 Pro を搭載した世界トップ クラスのデバイス

Lenovo

BIOSアセット情報エリア

ThinkPadのファクトリーサービス（工場出荷時サービス）の一環として、お客さま組織内の管理番号（例: 資産番号）をUEFI / BIOSに埋め込んだかたちで出荷することが可能です。万が一の紛失 → 再発見時も、アセット情報をUEFI / BIOS上で確認してデバイスを特定することが可能です。

資産管理用ラベルを製造工場でPC筐体に貼付することも可能。貼り忘れによる資産管理上のリスクを最小化。



セキュアドッキング

離席時の盗難リスクを最小化する目的で、ThinkPad本体のみならず、例えばドッキングステーションやモニターなど、各種純正周辺機器にもセキュリティスロットを搭載しています。また、専用の鍵で本体との間を施錠することが可能なタイプのドッキングステーションもご用意しています。

どのような脅威に対して対応するのか

- 事業所の内外にかかわらず、離席時にはPCが盗難されるリスクが存在
- 特にドッキングステーションについては着脱が多く行われるため、PCの盗難紛失対策と利便性、という2面を同時にカバーすることが必要

どのように保護されるのか

1. セキュリティスロット

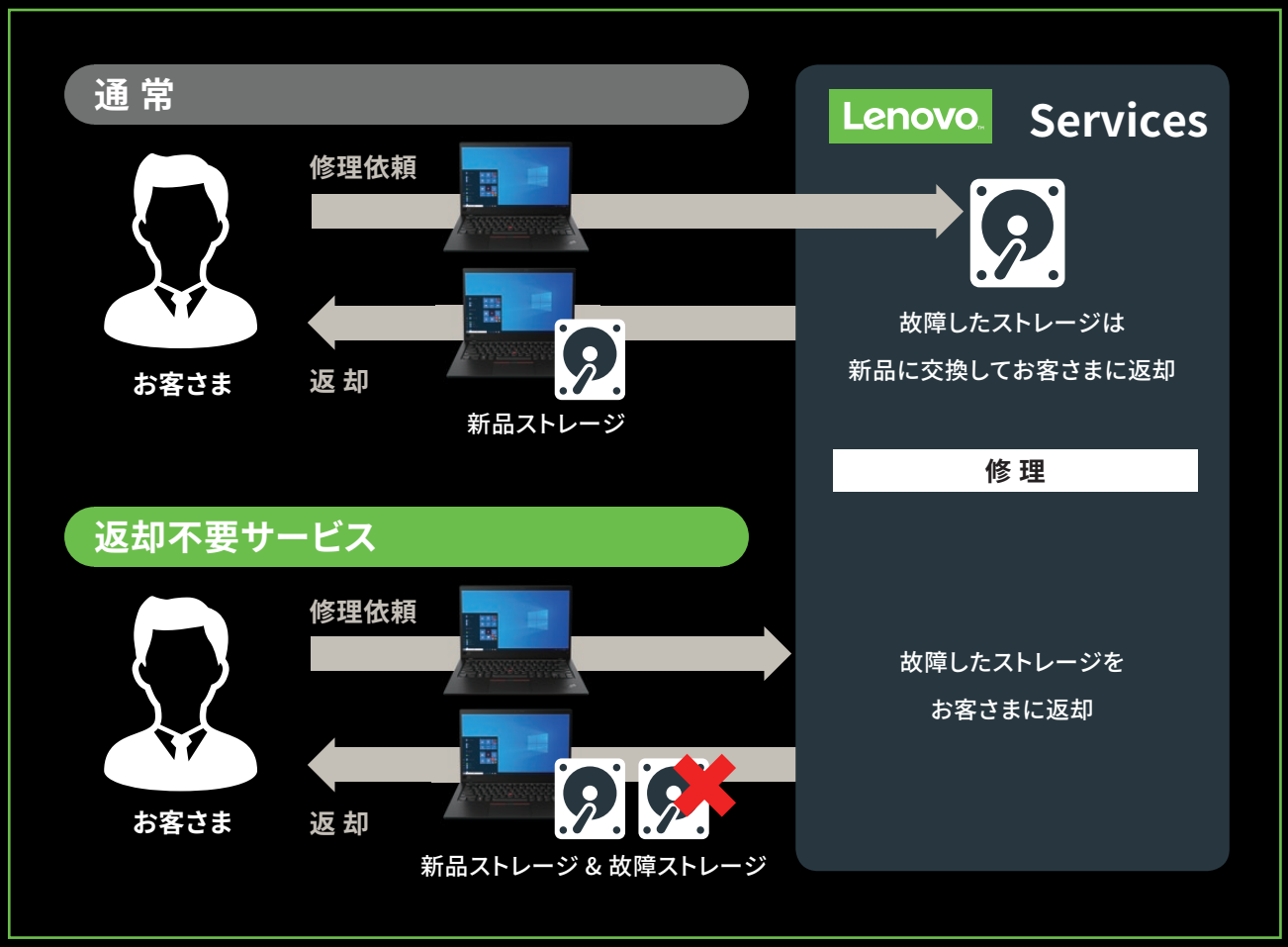
セキュリティケーブル（ワイヤー）と組み合わせて使用することにより、PCや周辺機器を机などのオフィス什器に固定することが可能

2. システムロックキー

専用の物理キーをシステムロックキースロットに差して、鍵をロック位置にかけるとThinkPadがドッキングステーションにロックされ、分離不可となる。ドッキングステーション側のセキュリティロックスロットからセキュリティケーブルで固定することにより、利便性と安全性を高い次元で両立することが可能

ディスク返却不要サービス

通常修理対応の際には、故障し交換された古いストレージの所有権はレノボに属しますが、
レノボがこれを放棄し、壊れたHDDをお客様のお手元に残すことで、情報をお客さまの手元に残します。



Windows 10

Windows 10 Pro を搭載した世界トップ クラスのデバイス

Security for Social Hacking

ソーシャルハッキングに対するセキュリティ

ThinkPad Privacy Guard

ThinkPad Privacy Guardはディスプレイ内に内蔵されたプライバシーフィルターです。
ワンタッチで有効化⇔無効化の切替が可能で、作業時とプレゼンテーション時の使い分け等が可能です。

どのような脅威に対して対応するのか

- テレワークの普及も進む今日、オフィスや自宅だけに限らず、コワーキングスペースなどで働くケースが増えている
  不特定多数の人と近接することから、覗き見からの情報漏洩のリスクも
- プライバシーフィルターを外付けした場合、閉じられた空間での利用時⇔オープンスペースでの利用時で着脱することが難しいという課題あり。また、プライバシーフィルター紛失のリスクも
- 特に2-in-1においてはプライバシーフィルターの装着でタッチ/ペン利用時のユーザビリティが悪化

どのように保護されるのか

1. ディスプレイモジュール内に電子的なフィルターを埋め込むことにより任意のタイミングで視野角制限（プライバシーフィルター機能）を有効化、無効化可能
2. 切替はF12キー、もしくはFn＋Dキーのコンビネーションを押下するだけのワンステップ
3. 有効化時は側面から見た際には画面がブラックアウトして見えづらくなる

ThinkPad Privacy Alert

ThinkPad Privacy Guard内蔵モデル（IRカメラ搭載）で利用可能なのぞき見による個人情報や認証情報の漏洩を未然に防ぐ保護機能です。

どのような脅威に対して対応するのか

- PC利用中の画面の背後からののぞき見による入力/表示中の内容漏洩
- ThinkPad Privacy GuardのONし忘れによる表示内容の漏洩

どのように保護されるのか

1. パスワードなどの認証情報入力時に自動的にThinkPad Privacy Guardを有効化、利用していたアプリケーションを閉じると無効化する挙動を設定可能（Lenovo Vantageより設定可能）
2. 内蔵のIRカメラによる視線トラッキング技術を活用した

- 背後から人が画面を見ている時に画面上に警告を出すことが可能な機能
- 視覚的に左から覗かれているのか、右から覗かれているのかも確認可能
- のぞき見検知時に自動的にThinkPad Privacy Guardを有効化する機能（Glanceアプリケーションより設定可能）

* 本機能の利用時にはIRカメラが常に有効化されます
* Webカメラ利用時に併用することはできません

Windows 10 Windows 10 Pro を搭載した世界トップ クラスのデバイス

ThinkShutter

不正なカメラ利用を防止する目的で、レノボでは3段階のセキュリティ機構を内蔵Webカメラに実装しています。

どのような脅威に対して対応するのか

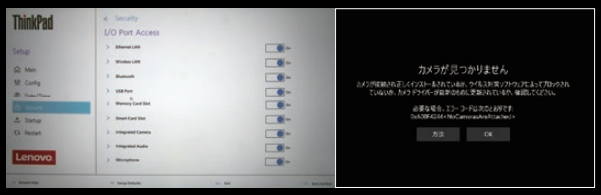
- 不正にWebカメラからの映像を取得するマルウェアの脅威
- Webカメラの利用による機密情報漏洩防止と、増え続けるオンライン会議への参加のニーズの両立
- カメラが露出することによる利用者の“見られている”感覚の払拭

どのように保護されるのか

ファームウェア

BIOS / UEFI上での有効化・無効化

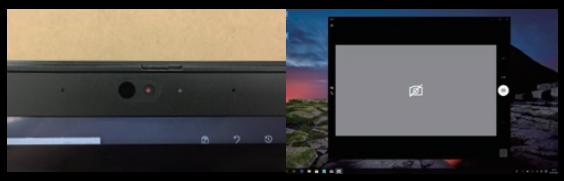
スーパーバイザーパスワードによって従業員が
設定値を変更することを未然に防ぐことも可能



ハードウェア

ThinkShutter

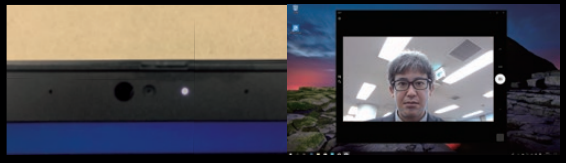
物理的なカメラシャッターにより非利用時の
盗撮を未然に防ぐ



ソフトウェア

LEDインジケーター

カメラ動作時にLEDインジケーターが点灯、
不正なカメラ利用を視覚的に発見可能



安全性の高い指紋認証モジュール

ThinkPadは高いレベルのセキュリティを実現した指紋認証ソリューションを実装することで
大切な生体認証情報の保護と、パスワードレスによる利便性、ショルダーハッキング防止に貢献します。

どのような脅威に対して対応するのか

- 安全性の高いパスワードの設定のためには複雑、かつ他の認証情報と被らないユニークな文字列が求められるが実際にはかんたんで覚えやすいものを設定されてしまうリスクが存在
- クラウドベースのソリューションの普及が進む中で、パスワードの重要性はかつてないほど高まっているがパブリックスペースでのパスワード入力により、覗き見によって認証情報を盗まれてしまう可能性も

どのように保護されるのか

Match-on-Chip指紋認証

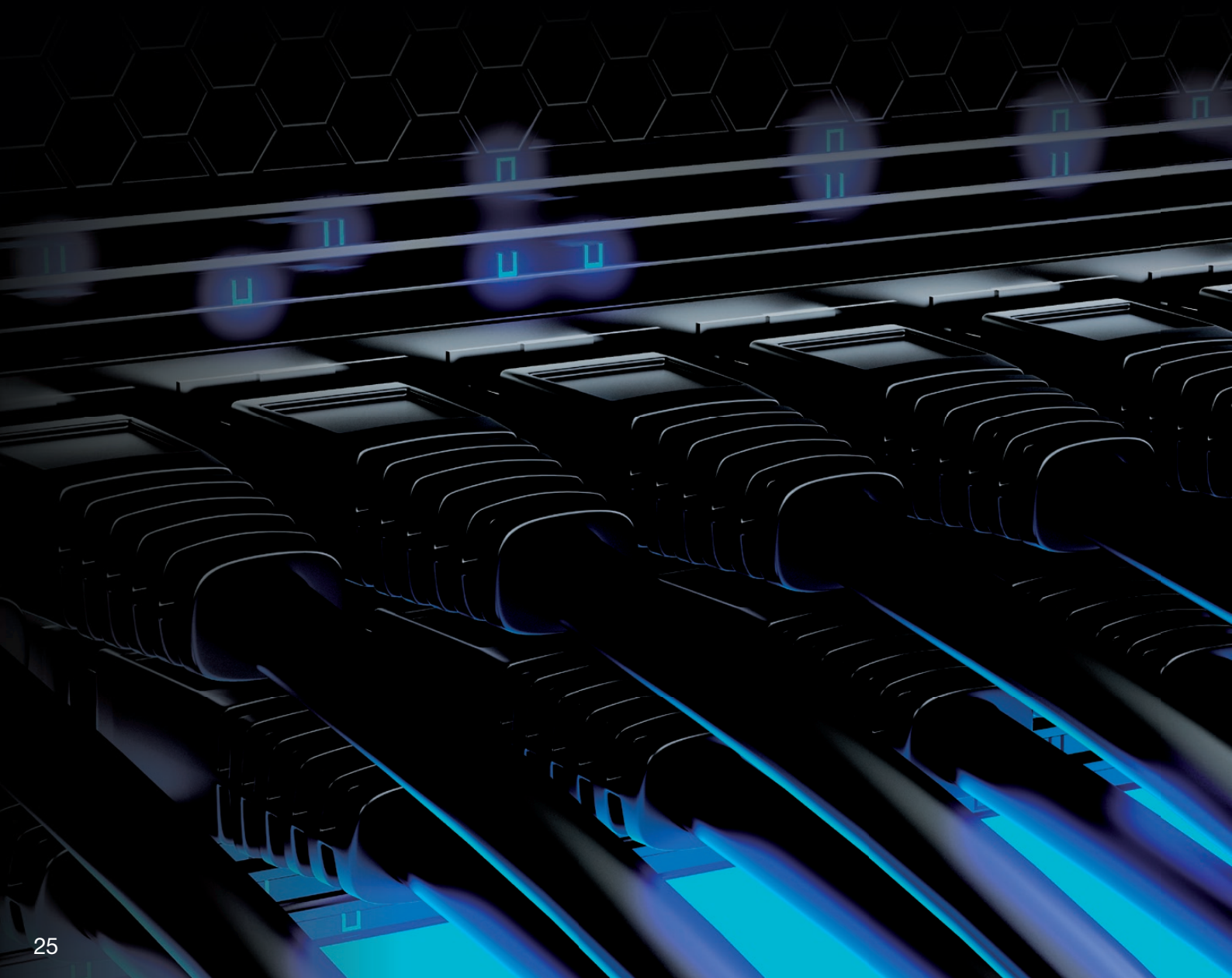
指紋データを指紋認証モジュール内にある独立したセキュアな領域に保存することで大切な生体データの漏洩防止に貢献。大切な生体データは専用チップ内に保持した上でOS/ファームウェア側には認証結果のみ通知

耐偽装指紋性能の高い認識メカニズム

Windows 10 Pro を搭載した世界トップ クラスのデバイス

Security for Cyber Protection

サイバー攻撃対策



Lenovo WiFi セキュリティー

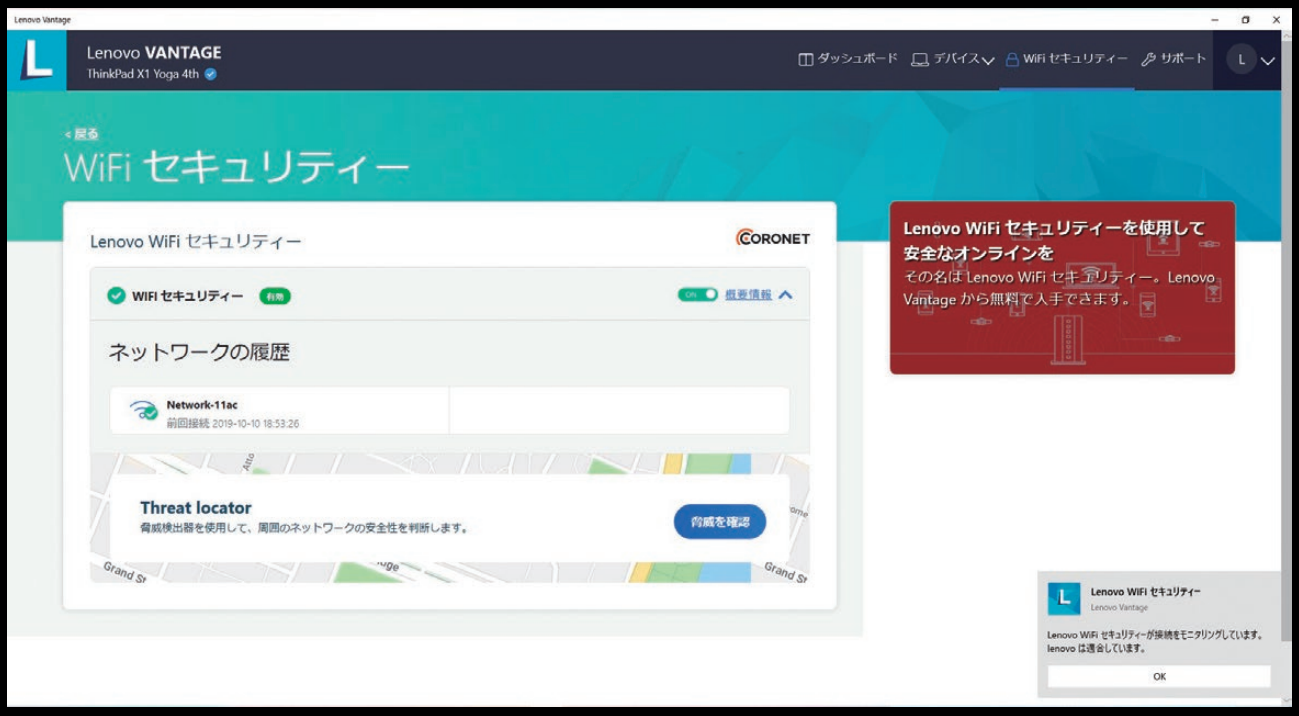
Lenovo WiFi セキュリティーは、プリインストールアプリケーションである
Lenovo Vantageに統合されたワイヤレス・ネットワークの安全性を評価する機能です。

どのような脅威に対して対応するのか

- 現代のデバイスはそのほとんどが常に無線LANをONにして様々な場所で利用されるが、空港のターミナルや街中のカフェなどから見えるSSIDのうちのいくつかは悪意のあるワイヤレス・ネットワークである可能性がある
- 使用感は正規の（安全な）ワイヤレス・ネットワークと同じで見分けが付かないが、実際には悪意のある攻撃者が通信の傍受、認証情報を含むデータの収集、デバイスの乗っ取りなどを秘密裏に行う可能性がある

どのように保護されるのか

1. Lenovo WiFi セキュリティーを有効化することで、使用可能なネットワークの安全性を自動的に評価
2. ユーザー自身がどの公共ネットワークが安全で、どの公共ネットワークが危険かを判断することが可能。アラートは自動的にToast POP-UPのかたちでユーザーに通知
3. プライバシーを尊重し、実行中のアクティビティや接続先ではなく、ネットワークがデータ転送プロセスを処理する方法のみを評価対象とする設計



Windows 10

Windows 10 Pro を搭載した世界トップ クラスのデバイス

●このカタログで使用されている製品の写真は、出荷時のものと一部異なる場合があります。また、仕様は事前の予告なしに変更する場合があります。●表示画面および印刷帳票の出力例のうち、特に断り書きのない出力例のデータ部分はすべて架空のものです。●画面ははめ込み合成で実際の表示とは異なります。●このカタログの情報は2020年9月現在のものです。●製品、サービス等詳細については、弊社もしくはビジネス・パートナーの営業担当員にご相談ください。●このカタログに掲載されている標準価格および料金は、2020年9月現在のもので事前の予告なしに変更する場合があります。最新の価格に関しては、弊社ホームページ をご参照ください。●「ダイレクト価格」は、直販による提供価格であり、ビジネス・パートナーなど再販者の販売価格を拘束するものではありません。弊社ホームページでは供給状況などの事情により一部の製品を掲載しており、「ダイレクト価格」製品すべてが弊社ホームページで購入できることを意味するものではありません。●当カタログ記載の製品にプリインストールあるいは添付されているソフトウェア製品につきましては、その梱包方法および内容物に関し、市販されているものとは異なる場合があります。

Lenovo
レノボ・ジャパン株式会社
NEC レノボ・ジャパン グループ

法人のお客様向け情報サイト
http://www.lenovojp.com/business/

お問い合わせフォーム
https://www.lenovojp.com/business/estimate/form/

20-09 Printed in Japan