概要資料

applippli-key

「パスワードレス × 2段階認証 × ランサムウェア対策」
Windowsログインの“防波堤”を、もっと身近に。

株式会社アプリップリ

20260728

会社概要

会社名	株式会社アプリップリ(applippli Co., Ltd.)
所在地	〒820-0202　福岡県嘉麻市山野875-2
事業内容	クラウドプラットフォーマー API・アプリ・モジュール開発 フィンテック(地域通貨事業)
資本金	1,300万円
創業 / 設立	1980年5月5日 /　2000年9月14日
グループ会社	applippli Myanmar Co., Ltd.(ミャンマー現地法人)
包括連携協定	嘉麻市デジタル推進に関する包括連携協定締結(福岡県嘉麻市)

会社概要

パートナー資格

Microsoft AI Cloud Partner

弥生 販売 パートナー / 弥生 教育 パートナー / 弥生 開発 パートナー

＜弥生株式会社＞

DCP GOLD Daijin Certified Partner

＜応研株式会社＞

Sorimachi Official Sales Partner SOSP
ソリマチ認定セールスパートナー

＜ソリマチ株式会社＞

各種認定

経済産業省認定 Smart SME Supporter 第46号-25020008（19）

＜経済産業省認定＞
スマートSMEサポーター
認定番号：第46号-25020008(19)

ISO 27001:2022 CERTIFICATION intertek UKAS MANAGEMENT SYSTEMS 014

ISO 27001:2022　認証取得

＜国際規格＞
情報セキュリティマネジメント
システム
（ISO/IEC27001:2022）

2026 健康経営優良法人 KENKO Investment for Health 中小規模法人部門

＜日本健康会議認定＞
健康経営優良法人2026

経営理念

お役立ちと安心をまじめに提供する

私たちの会社は、社員の成長を通じて、お客様に「お役立ち」と「安心」をお届けするために存在しています。社員一人ひとりが成長し、前向きで幸せな気持ちで働くことで、質の高いサービスを提供することができます。その結果、お客様には安心して任せられる信頼感と、満足いただける価値を実感していただけます。

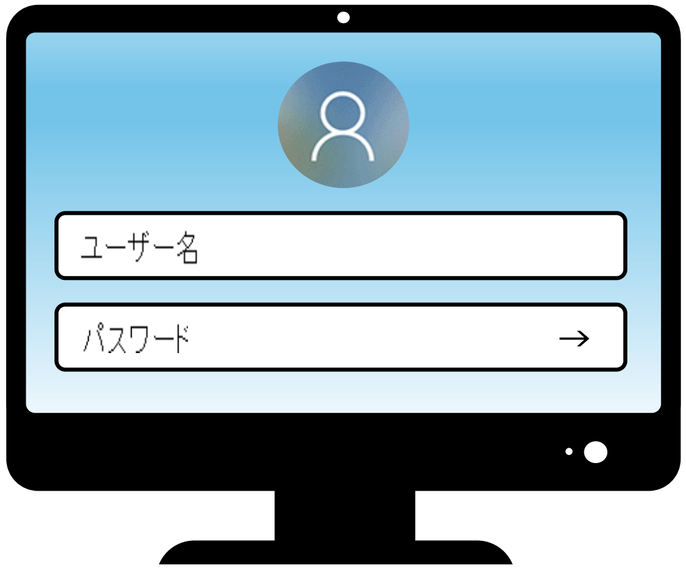
こんなセキュリティのお悩みはありませんか？

- 取引先からセキュリティ強化の要請
- 従業員の異動や退職によるデータ保持
- 同じパスワードを使いまわしている
- 安価でセキュリティ対策を実現したい

その悩み、applippli-key で解決します！

サービス概要

いままでのログイン



applippli-keyでのログイン

自社アプリ「applippli Authenticator」で、①②どちらの方法でもログインできます。
Microsoft/GoogleのAuthenticatorもご利用いただけます。

Ver.2.0 主要新機能

認証だけでなく「検知・自動防御・通知」まで。認証×検知のハイブリッド防御へ進化しました。

ワンタッチログイン

01

スマホをワンタップ
するだけでログオン。
OTP認証にも対応。

ログ・検知・自動IPブロック

02

12種の攻撃パターンを
リアルタイム検知し、
数秒で自動IPブロック。

LINE通知

03

脅威検知の瞬間に
管理者のLINEへ通知。
初動を数秒に短縮。

applippli-key のアプローチ ― 3つの壁で守る

認証の壁
不正ログインをブロック

➡

検知の壁
ランサムウェアを早期発見

➡

即時通知
管理者がすぐに動ける

ゼロトラスト原則で多層防御 ―「決して信頼せず、常に検証する」

新機能① ログ・検知・自動IPブロック

認証イベントと脅威を自動記録。不審なアクセスを検知し、自動でIPブロック／LINE通知します。

12
種類の攻撃パターンを
検知ポイントで網羅

侵入を試みた段階から数秒で
自動IPブロック／LINE通知

侵入	ブルートフォース攻撃 / RDP不正侵入 / 不正ログオン試行
拡散	横展開（ラテラルムーブ） / プロセス偽装実行
窃取	認証情報の窃取（lsass.exe へのアクセス）
妨害	シャドウコピー削除 / セキュリティ機能の無効化
永続化	サービス偽装登録 / 管理者権限の不正取得
実行	ファイル大量暗号化 / ネットワーク不正アクセス

認証・脅威イベントログ（管理コンソール画面イメージ）

日時	イベント	結果	ユーザー	IPアドレス
2026/07/08 07:42:26	2段階認証ログオン	成功	owner	—
2026/07/06 09:32:01	ネットワーク不正アクセス	脅威	admin	91.202.233.79
2026/07/06 09:31:00	ネットワーク不正アクセス	脅威	admin	91.202.233.79

※ 画面はイメージです。検知した脅威は同時に管理者のLINEへ通知されます。

新機能② 一画面でPCセキュリティ状況を把握

認証ログ・脅威検知・LINE通知設定をひとつの管理コンソールで。サーバー不要、設定は約5分です。

※ 画面はイメージです。表示している数値はデモ環境のサンプルです。

認証ログの記録・可視化

誰が・いつ・どの端末から
ログオンしたかを自動記録

脅威のリアルタイム検知

12種の攻撃パターンを
OS深部で常時監視

自動IPブロック・LINE通知

検知から数秒で遮断し、
管理者へ即時通知

新機能③ LINE通知で初動を「数秒」に

LINEに届いたその瞬間、PC名・ユーザー・IPアドレスが分かる。管理者は即断できます。

従来（メール通知・目視）

T+0	数時間後	翌朝	+数日後
攻撃開始・潜伏	ログに記録	メールで確認	対応完了

対応開始まで最短でも半日～数日。

applippli-key（LINE直接通知）

T+0	～数秒	即時	～数秒
侵入を試みる	自動で検知	IP自動ブロック	LINEへ通知

不正ログイン「前」に防ぐ認証セキュリティ。

初動対応時間を 最大99% 削減

applippli-key 公式アカウント

● 不正アクセス検知 09:35

【DESKTOP-A01】ログオン失敗が5分間に10回を超過。攻撃元IPを自動ブロックしました。

● プロセス偽装検知 09:36

【DESKTOP-B02】svchost.exe がシステムパス外から起動。署名検証に失敗。

● 認証情報窃取の疑い 09:37

【DESKTOP-C03】lsass.exe への不審なアクセスを検知しました。

● 自動対応完了 09:40

【自動対応】ファイアウォールで不審な接続を遮断済みです。

製品ラインナップ（全3種・デバイスライセンス）

守りたいPCの「台数」で導入。PC1台ごとの購入で、そのPCを使う従業員は全員が利用できます。

スタンドアロン版
PC用デバイスライセンス

- 単体PCにインストール
- Windows 10 / 11 に対応
- 1台から契約・運用が可能

サーバー版
サーバー用デバイスライセンス

- Windows Server 2016以降
- オンプレ・クラウド・仮想
- 複数ユーザー環境に最適

ふるさと納税版
スタンドアロン版

- ふるさと納税の返礼品
- ふるさとチョイスで申込
- 楽天ふるさと納税でも申込

「デバイスライセンス」とは？

✓ コスト最適化
交代制のPCもPC1台分の費用だけ

✓ 人数課金なし
利用者が増減しても追加購入は不要

✓ 管理がシンプル
守りたい端末の数だけ用意すればよい

対応OS	対応環境	導入時間	課金単位
Windows 10 / 11 Server 2016以降	オンプレ・仮想 クラウド	設定画面から約5分 サーバー構築不要	PC1台ごと 人数課金なし

生体認証との違い

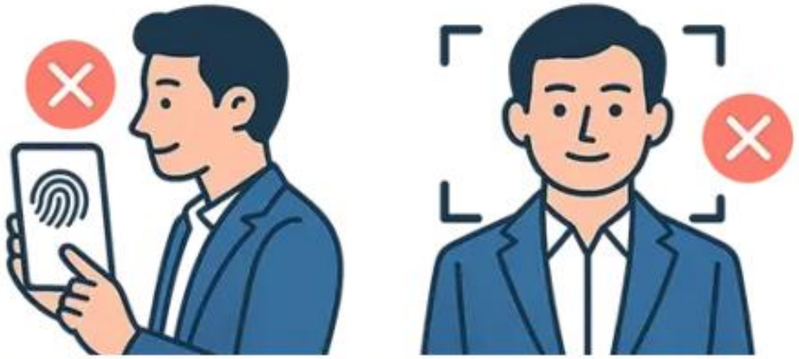
【重要】指紋・顔認証では不正アクセスは防げません

なぜか？

現在の指紋・顔認証は、単に**「Windowsパスワードを指紋や顔に置き換えているだけ」**だからです。
内部的にはパスワードでログインしているのと全く同じ仕組みであり、強固な壁にはなっていません。

「生体認証 ＝ 2段階認証（2FA）」という勘違い。
そこをランサムウェアに狙われています。

● 指紋・顔認証の実態



パスワードの入力代行に過ぎません。
これは2段階認証ではありません。

● 真の2段階認証（2FA）

物理的に別のデバイス（鍵）を使い、
30秒ごとに変わるワンタイムパスワードによって初めて成り立ちます。

物理的に切り離された「別のもの」による認証。これこそが不正アクセスを遮断する唯一の手段です。

導入効果①

applippli-keyの導入により、パスワード依存の弱い防御から、
本人確認を組み合わせた強固なセキュリティへ進化します。

BEFORE	AFTER
パスワードのみの守りは、 盗まれると簡単に突破 されてしまう状態	「知識情報（パスワード）」 ＋ 「所持情報（認証コード）」 により「突破されにくい」状態 を作ります

導入効果②

applippli-key の導入により、次のような追加効果も得られます。

サイバー攻撃を重要な場所へ「侵入させない」仕組みの構築

サイバー攻撃を**100%防ぐことは不可能**です。しかし、重要なデータがある
PCやサーバーに“侵入されない状態”を作ることはできます。
applippli-keyは、その**“最後の防御壁（ゼロトラストの入り口）”**を担います。

「守る仕組み」を整えることが、企業の信頼につながる

フィッシングサイトやメールからの感染については、社員がどんなに注意しても、
ヒューマンエラーとして発生する可能性があります。
applippli-keyの導入により**「ミスが起きても守れる仕組み」**を作れます。
小額で情報資産を守り企業の信頼向上につながります。

ランサムウェアには多要素認証(MFA)が有効

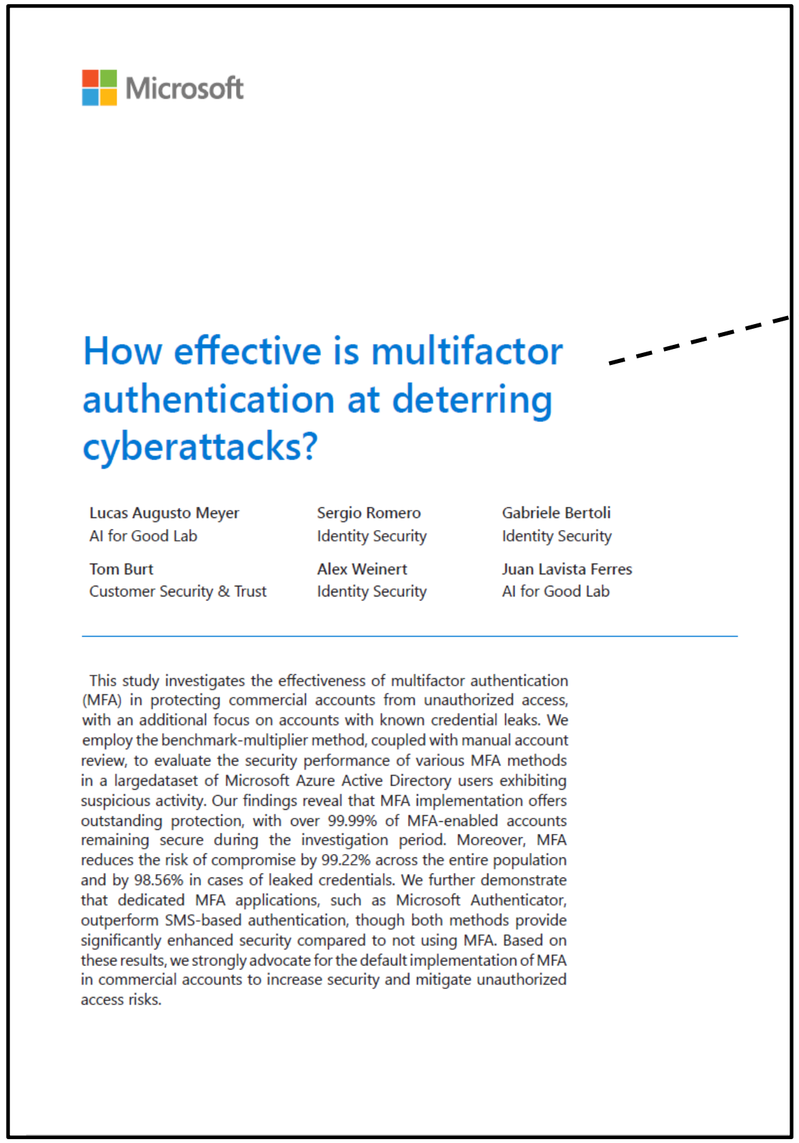
攻撃防止効果

98.56%

Microsoftの調査によると、多要素認証(MFA)は、ユーザー名・パスワードなどの資格情報漏洩時の**攻撃成功率をわずか1.44%に抑え、リスクを98.56%削減**します。約12.8万件の漏洩アカウント分析で、MFAは実証済みの防御策であり、認証専用アプリを使うとさらに効果が高まります。

出典:Lucas Augusto Meyer et al., ”How effective is multifactor authentication at deterring cyberattacks?”, arXiv:2305.00945, CC BY 4.0

エビデンスについて



Microsoft

How effective is multifactor authentication at deterring cyberattacks?

Lucas Augusto Meyer
AI for Good Lab

Sergio Romero
Identity Security

Gabriele Bertoli
Identity Security

Tom Burt
Customer Security & Trust

Alex Weinert
Identity Security

Juan Lavista Ferres
AI for Good Lab

This study investigates the effectiveness of multifactor authentication (MFA) in protecting commercial accounts from unauthorized access, with an additional focus on accounts with known credential leaks. We employ the benchmark-multiplier method, coupled with manual account review, to evaluate the security performance of various MFA methods in a largedataset of Microsoft Azure Active Directory users exhibiting suspicious activity. Our findings reveal that MFA implementation offers outstanding protection, with over 99.99% of MFA-enabled accounts remaining secure during the investigation period. Moreover, MFA reduces the risk of compromise by 99.22% across the entire population and by 98.56% in cases of leaked credentials. We further demonstrate that dedicated MFA applications, such as Microsoft Authenticator, outperform SMS-based authentication, though both methods provide significantly enhanced security compared to not using MFA. Based on these results, we strongly advocate for the default implementation of MFA in commercial accounts to increase security and mitigate unauthorized access risks.

Microsoftの研究結果

多要素認証は、サイバー攻撃の防止に、どれほど効果があるのか？

結論1

MFAを使っているアカウントの

99.99% が攻撃を受けても無事

結論2

MFA未使用の場合と比較すると、

侵害されるリスクが**99.22%**減る

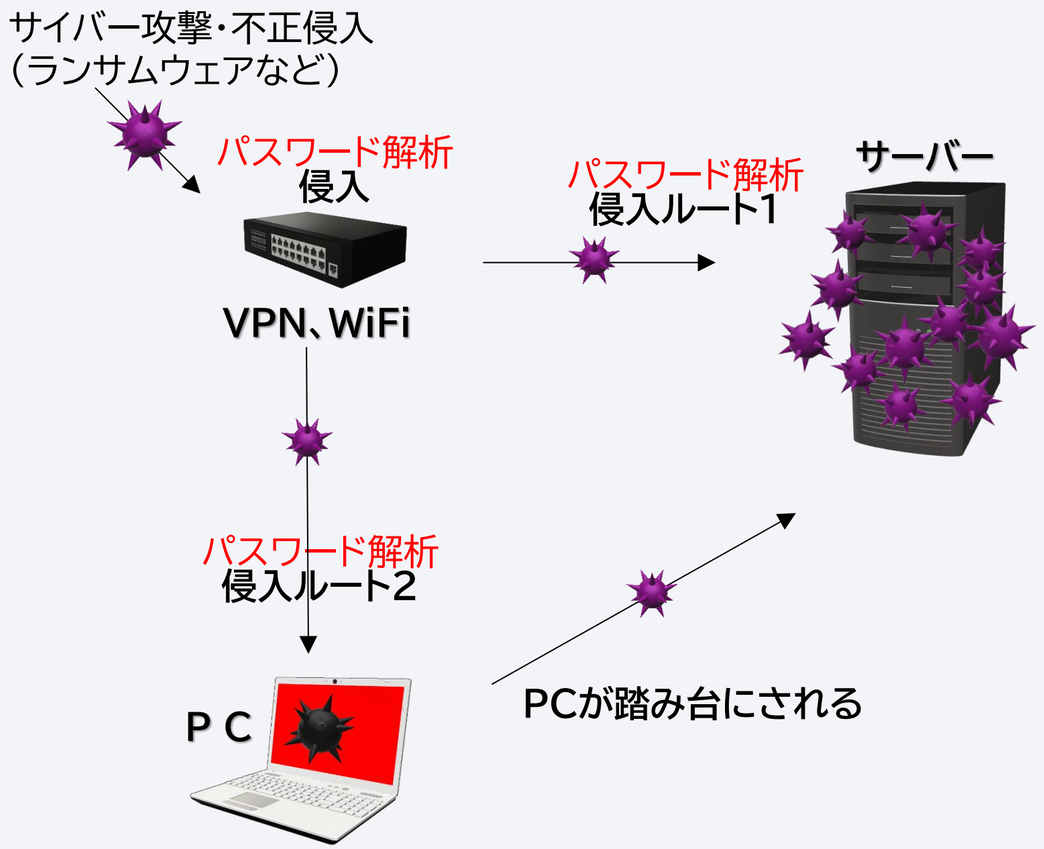
結論3

パスワードが漏えいした最悪のケースでも、

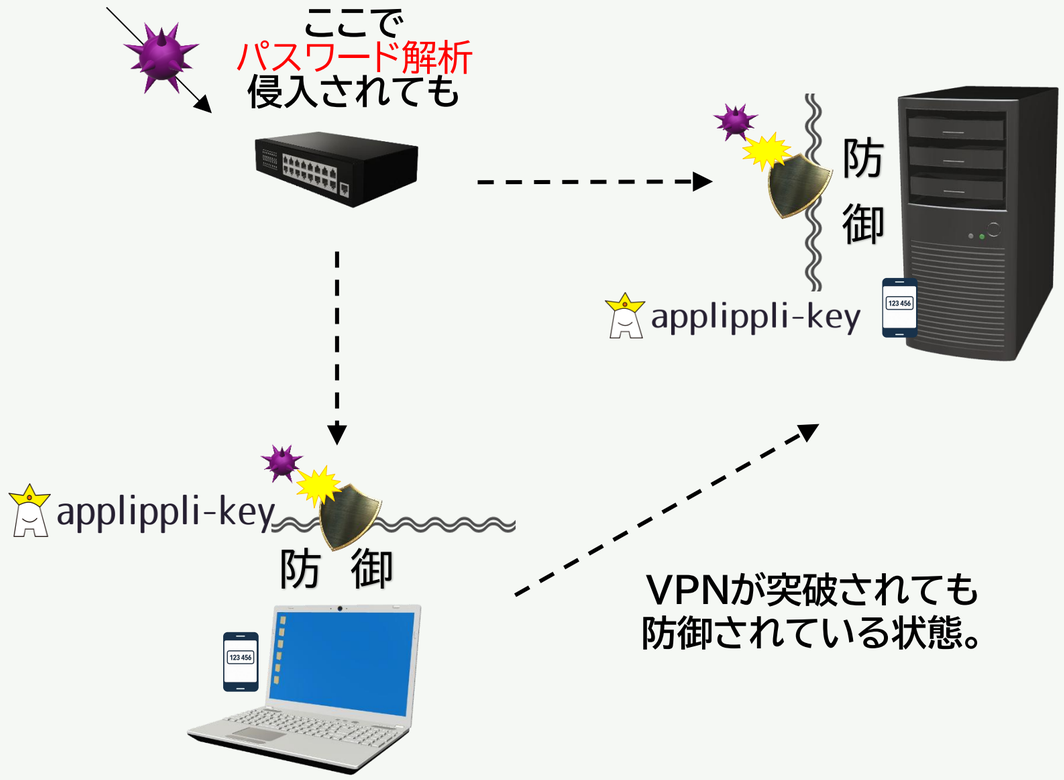
MFAがあれば**98.56%**の攻撃を防ぐ

なぜサイバー攻撃(ランサムウェアなど)が防御できるのか？

導入前の状態



applippli-key導入後



サイバー攻撃は、ID・パスワードの解析・突破 ⇒ サーバーへの侵入を防ぐことが重要です。

applippli-keyはVPNを突破されても、PCやサーバーからの侵入経路を、MFA認証で防御します。

日本のサイバー攻撃の現状

★データが示すサイバー攻撃の実態

出展元	データ内容	数値
警察庁「不正アクセス行為の発生状況」（2023年）	不正アクセス認知件数	年間 5,673件 うちPW解析起因 約87%
Verizon DBIR 2023（世界標準レポート）	侵害のうちPW関連の割合	全侵害の 約81%
NICT（情報通信研究機構）「NICTER観測レポート2023」	国内IPへの攻撃パケット観測数	年間 約2,454億パケット （1日約6.7億）
推計（337万社） ※法人IPアドレス比率 約40%	企業1社あたりの推計攻撃数	約100回/日 （月3,000回）

※不正アクセス認知件数は被害届が提出された件数のため、実際は数倍～10倍程度発生してます。

日本のサイバー攻撃の現状

★突破率から見る被害率

シナリオ	想定される状況	突破率	年間侵害回数
対策なし	パスワードのみ・使い回し	約0.1%	約36回
標準対策	パスワード管理ツール使用	約0.01%	約3.6回
MFA導入	Applippli-key導入	約0.001%以下	約0.3回以下

・大半は不正アクセスやサイバー攻撃を受けたことに気づいていない

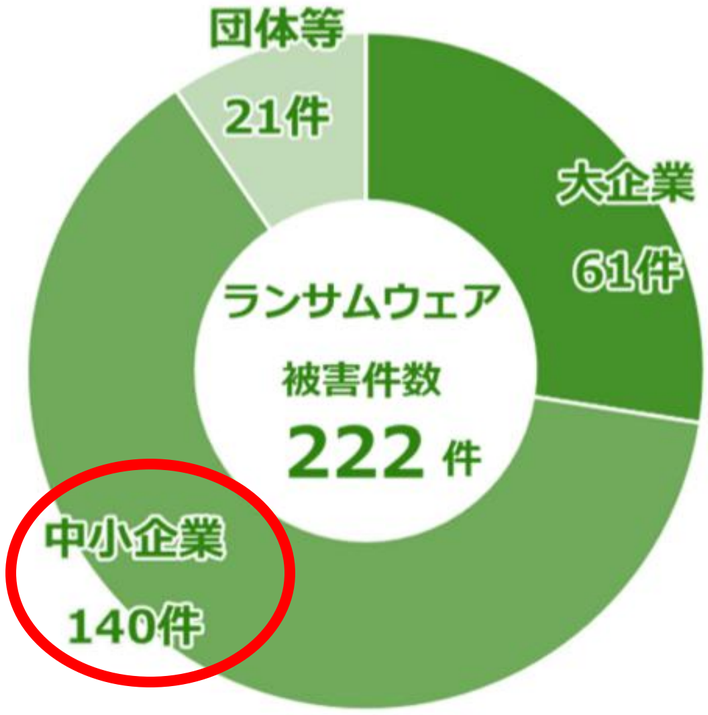
・すでに起きている事象に対して対策を行う必要がある

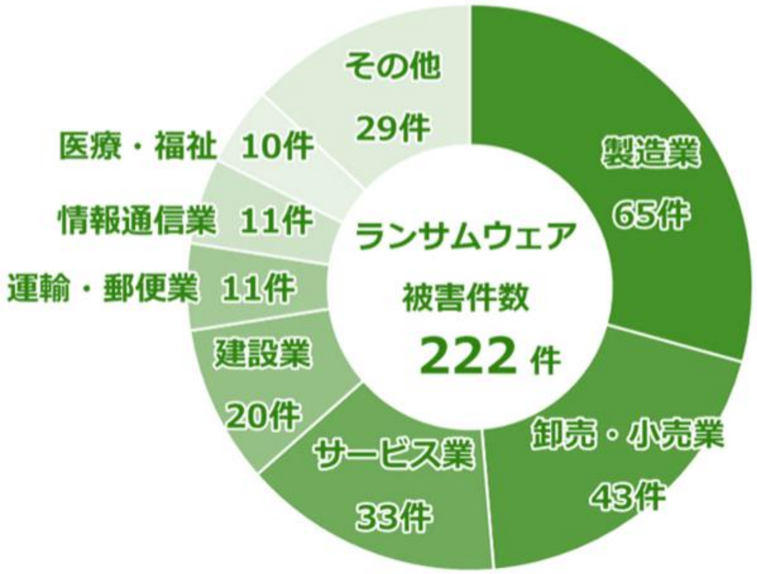
サイバー攻撃は大企業だけの問題ではない

むしろ、中小企業はサイバー攻撃から狙われている

■ ランサムウェアの被害に関する統計

― 警察庁『令和6年サイバー空間をめぐる脅威の情勢』より抜粋





問題となっているランサムウェアの被害の多くは、中小企業(63%)となっている。 被害業種は多岐にわたり、且つ氷山の一角の状況である。

中小企業のセキュリティ対策の現実

【結論】中小企業の情報セキュリティ対策は深刻に遅れている

■ 中小企業の情報セキュリティの体制について

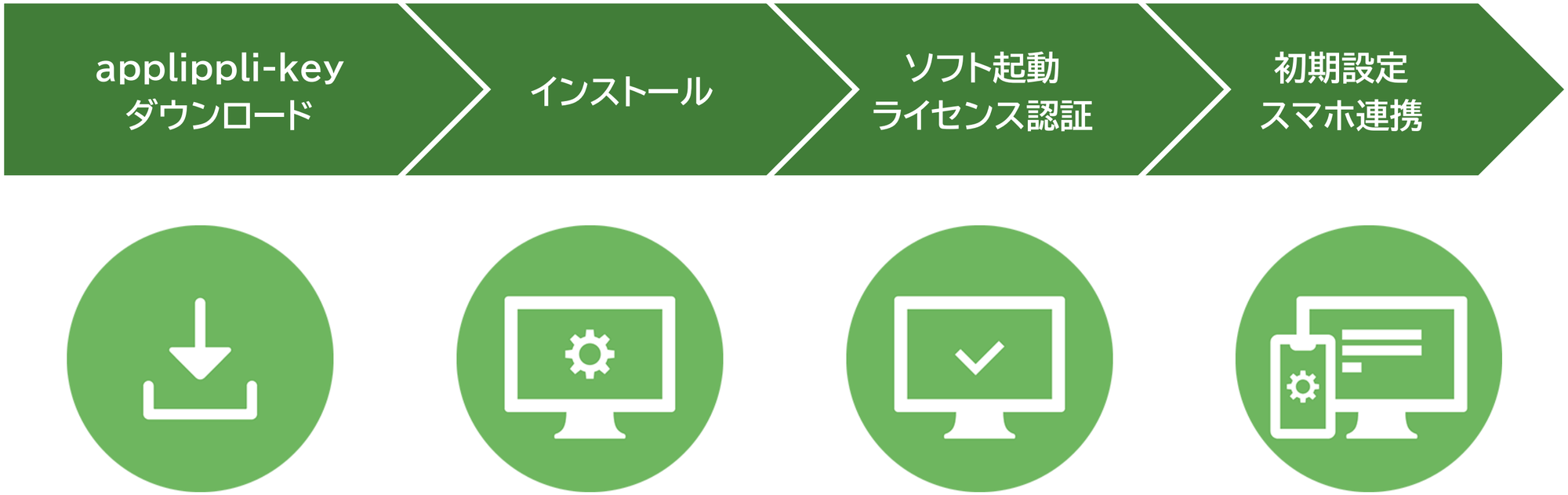
― IPA『2024年度中小企業等実態調査結果』より作図

中小企業の 約**1割**のみしか、情報セキュリティ専門部署が無く、

約**7割** が情報セキュリティ対策を組織的に行っていない

利用開始方法について

applippli-keyは、お申し込み後 すぐに導入が可能 です



補足事項

※ お申し込み後、ご入金・決済確認後にセットアップファイル、ライセンス情報がメールにて通知されます。

※ applippli-keyのインストール中に端末の管理者権限が必要です。事前にご確認ください。

サービス仕様概要

- **WindowsOS（ServerOS含む）各種対応しています。**
  スタンドアロン版：Windows10 / 11
  サーバー版：Windows Server 2016 / 2019 / 2022 / 2025

- **ご利用のスマートフォンへのワンタイムパスワード発行アプリのインストールが必要です。**
  Google Authenticator / Microsoft Authenticator など

- **ライセンスを有効にする際は、インターネット接続が必要です。**

- **ライセンスの再利用はできません。再申込が必要です。**
  インストールしたPCを入れ替える時など、ライセンスの引継ぎはできません。
  別途、新規にサービスの申し込みが必要です。

※ 認証アプリは自社製「applippli Authenticator」に対応。Google／Microsoft Authenticatorも利用可能です。
※ スタンドアロン・オンプレのほか「仮想」「クラウド」環境にも対応しています（現在 iOS には非対応）。

よくある質問

スマホが手元にないとPCにログインできないのか？

万が一スマホが手元になくても、緊急ログオンにてログインが可能です。
緊急ログオンの回数制限以内にスマホをご用意いただきますようお願いします。

インターネット環境に接続されてないスマホ、PCでも使えるか？

Microsoft やGoogleのワンタイムパスワード発行アプリは、オフライン利用が可能です。
ただし、applippli-keyのダウンロード、ライセンス認証時および、
ワンタイムパスワード発行アプリのインストール時にはインターネット回線が必要です。

MacOSも対応しているか？

現在はWindows OSのみとなっております。今後、Mac OS対応もリリース予定です。

どこにもなかった新しい「お役立ち」を。

applippli
アプリップリ