

リモートワーク時代の 中小企業のための認証セキュリティ

A close-up photograph of a person's hands typing on a laptop keyboard. Overlaid on the image is a semi-transparent login form with three input fields: 'Username' with a person icon, 'Password' with a lock icon, and a 'LOGIN' button. A large white padlock icon is also centered over the keyboard area.

Username

Password

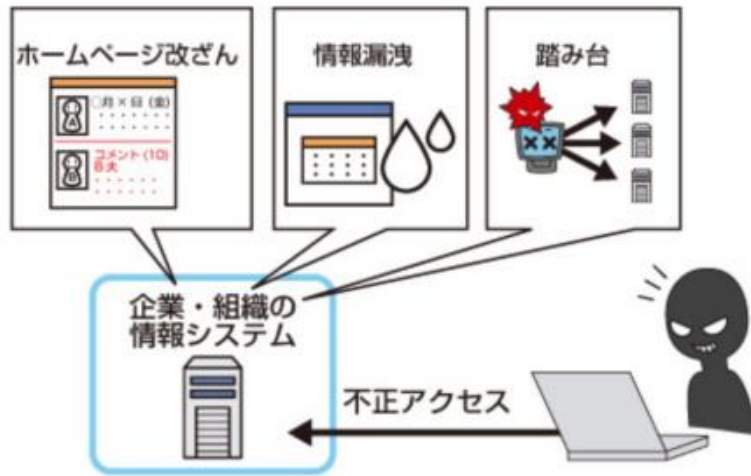
LOGIN

不正アクセス・不正ログインの脅威とは？

不正アクセスとは？

「本来アクセス権限を持たない者が、サーバや情報システムの内部へ侵入を行う行為」
(総務省「国民のための情報セキュリティサイト」より)

不正アクセスの内容は情報漏洩、情報の改ざん、踏み台など多岐にわたります。



出典：総務省「国民のための情報セキュリティサイト」

・世界のIT不正行為の被害額

約 6,000 億ドル

・原因の主要因

81%がログイン情報の盗難

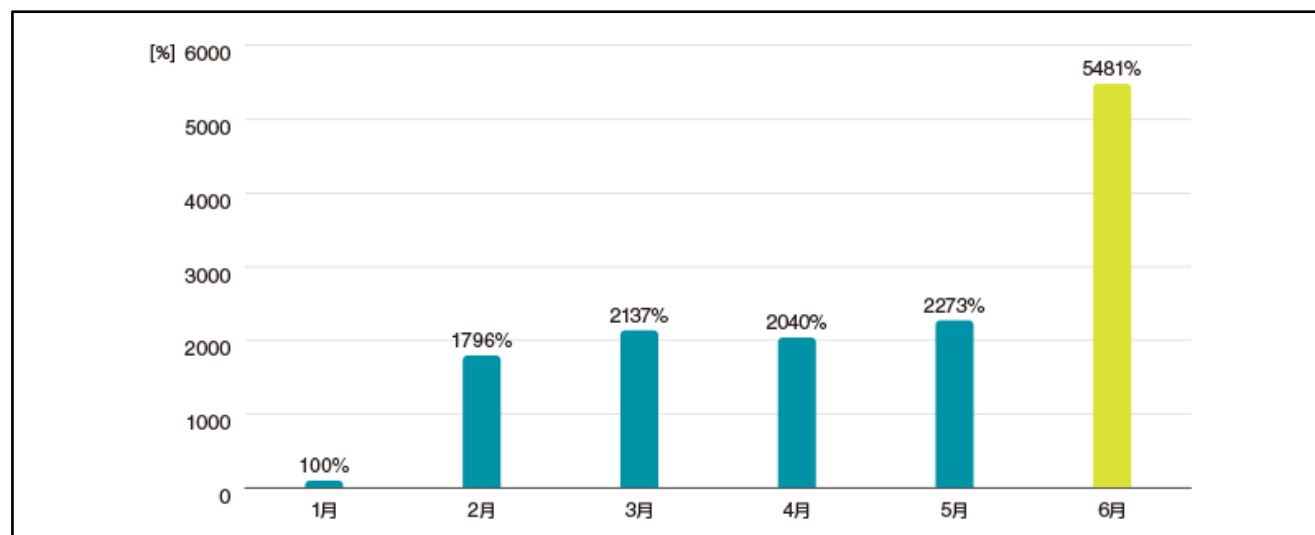
・情報漏洩が発覚するまでの期間

平均 200 日

リモートログイン認証への攻撃の増加

グラフは、Windowsのリモートデスクトップへの攻撃数をグラフ化したものです。
2020年の上半期、新型コロナウイルスによる緊急事態宣言の発令からWindowsのリモートログインへの攻撃が急激に増加しています。

2020年1月の検出数を100%とすると、**5481%**と**50倍**以上。
現在も、ログイン認証への攻撃は増加、複雑化しておりそれに対する対応が急務です。



RDPを狙った脅威の月別推移グラフ(2020年上半期・国内)

2020年1月の検出数を100%として設定

出典：https://eset-info.canon-its.jp/files/user/malware_info/images/ranking/pdf/MalwareReport_2020FirstHalf.pdf

不正アクセスによる被害

2022年2月

トヨタ自動車(株)がサプライチェーン攻撃により、**日本国内の全14工場28ラインの稼働を3月1日に停止**。また、小会社の日野自動車(株)、ダイハツ工業(株)も同じく一部工場の稼働を停止。

原因は主要取引先である小島プレス工業(株)が**サイバー攻撃（ラムサムウェア）**を検知したため。

小島プレス工業(株)は社内サーバの障害を検知後に被害拡大を防ぐために全てのネットワークを遮断。

これにより、業務継続に必要不可欠な「部品の受発注システム」が使用不能となった。

2022年6月

図書館運営会社が、勤怠・人事給与システムの認証が総当たり攻撃によって突破され、**従業員や退職者など6,886人分の個人情報や勤怠履歴、給与データがき損**。

・サプライチェーン攻撃：

ターゲット企業のグループ会社、業務委託先、発注先、仕入れ先などを攻撃し、それを足がかりにターゲット企業に侵入する攻撃。

・ラムサムウェア：

感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭や暗号資産）を要求する不正プログラム。

・総当たり攻撃：

ユーザID、パスワードに入力可能なパターンを全て入力して認証を突破する攻撃。

不正ログインの増加からSalesforceが多要素認証を必須化

コロナの影響などによるリモートワークの増加、それに伴う不正ログインの増加から、2022年2月1日から、Salesforceのログイン認証において**多要素認証が必須化**。
ログインするためには、ユーザ名・パスワード以外の第三要素が必要になりました。

※必須化の期限は延長されています。

変更前

ユーザ名

パスワード



変更後

ユーザ名

パスワード

下記のいずれかの使用が必須

- ・ 認証用アプリケーション
 - ・ セキュリティキー
- ・ 組み込み Authenticator

The image shows the Salesforce login page. At the top is the Salesforce logo. Below it are input fields for 'ユーザ名' (Username) and 'パスワード' (Password). A blue 'ログイン' (Login) button is positioned below the password field. Under the button is a checkbox labeled 'ログイン情報を保存する' (Save login information). At the bottom, there is a link that says 'パスワードをお忘れですか?' (Forgot your password?).

どの多要素認証が良いのか？

IDやパスワードのログイン情報は、人為的ミスからどうしても漏洩してしまう。
かといって、社員のITリテラシー向上の教育も複雑で長いパスワードの設定も実施しづらい。
そこで、シンプルな**物理的対策**が有効性を発揮します。

特におすすめ！

	SMS・自動電話	アプリ	モバイルプッシュ通知	トークン
メリット	• アプリのインストールが不要で、電話番号があればすぐ使える • SMSに送られたコードを入力するだけで認証できる • フィーチャーフォンでも使える	• アプリをインストールするだけですぐに利用できる • 物理的なデバイスが必要なので、不正アクセスのリスクを抑えられる • ネットワークに接続しなくても利用可能	• プッシュ通知を侵害するのは非常に難しく、安全性が高い • スマホ等に届いた通知を承認するだけで認証できる	• 特定のトークンが必要なため、安全性がかなり高い • トークン自体が不正アクセスを受けるリスクが無い • 初期設定が簡単で、利用も挿してタッチするだけでOK • インターネット環境やバッテリーが不要
デメリット	• 自分の電話番号を特定のサイトやプラットフォームに開示しなければならない • SMS受信可能なSIMカードと環境でないと使えない • 「SMSへのアクセス権限」を取られるとハッカーに筒抜け	• 認証デバイスを変更した時の移行手続きが面倒になる • 認証コードをアプリで読み取り、手で入力する手間が発生する • 複数デバイスから認証できるため、物理的な侵害や紛失のリスクが比較的高くなる	• インターネットへのアクセス環境が必要 • プッシュ認証をサポートする限られたサービスでのみ利用可能	• トークンの紛失リスクがある • 持ち運ぶ端末が増える

セキュリティキーで低コストかつ強固なセキュリティを実現する

セキュリティキーの特徴

- ・使用するPCに依存せずに導入することができる。
※既存のPCにそのまま使用可能。
PC入れ替え時も継続して利用可能。
- ・PC紛失時も高いセキュリティが保てる
- ・導入コストが安い。
※1つあたり数千円から導入可能。
- ・インターネット環境がなくても使用可能。



情報端末の紛失について

2012年に調査を開始以降、個人情報の漏えい・紛失事故を年別にみると、2021年の事故件数は**137件（前年比33.0%増）**で過去最多。

社数も120社（同36.3%増）で、これまで最多だった2020年（88社）を32社上回りました。

2021年は情報端末の紛失により、**100万件以上**の個人情報流出した事件が2件発生しています。



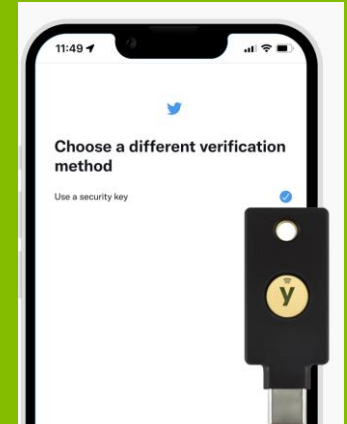
代表的なセキュリティキー製品

YubiKey

【YubiKey】シリーズは、2007年にスウェーデンで設立、2011年よりシリコンバレーにも拠点を置く認証セキュリティのパイオニア「Yubico社」が開発するセキュリティキー。

Yubico社の製品はGoogle社・Facebook社・Salesforce社など世界の大手企業の社内セキュリティツールとして大々的に採用されています。

こんな企業におすすめ：『外国の取引先から多要素認証導入を要求されている』



ATKey

台湾のEgis Technology傘下のAuthenTrendによって開発されたセキュリティキー。

最新の製品ラインナップ全てに特許取得のスタンドアロン指紋認証を取り入れるなど、先進的な技術を積極的に取り入れた製品ラインナップが特徴です。

こんな企業におすすめ：『指紋認証を安価で導入したい』



セキュリティキー認証が可能な主なサービス

PC



メール



クラウドストレージ



開発ツール



パスワード管理



SNS



セールスフォース



これら以外のサービスも認証可能なサービス多数あり。
カスタマイズすることで自社の独自のサービスにおいても
認証が可能。

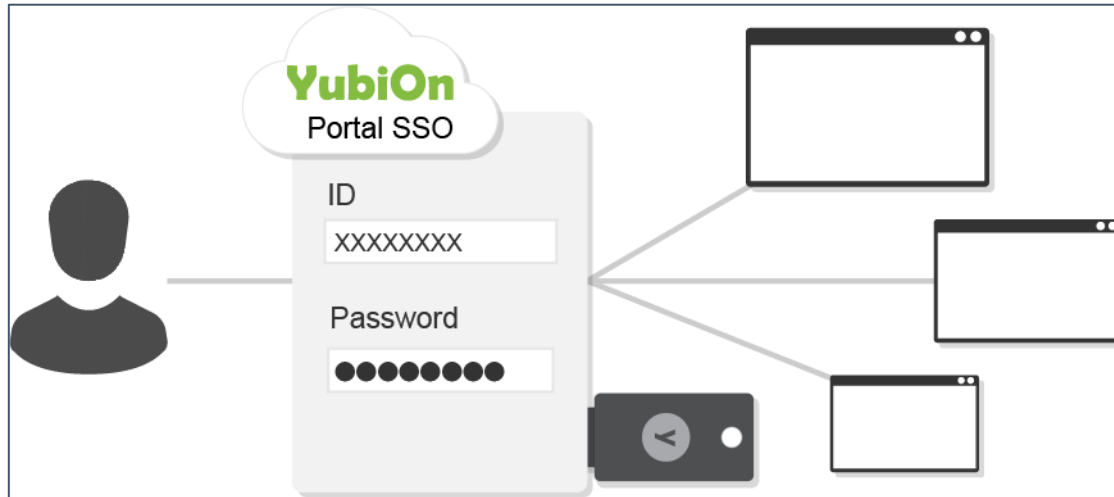


セキュリティキーを使用したソリューション



シングルサインオンを可能にするソリューション

PCログイン以外のWebサービスへのログインを一括管理するYubiOn



キーワード

#SSO
#リモートアクセス
#SalesforceのMFA
#指紋認証
#認証管理

YubiOn Portal にログインすることで、SalesforceやGoogle Workspaceなどの
Webサービスでのログインが全て不要に。

PCのログインもセキュリティキーで管理することができるため、セキュリティキーの設定のみで全てのアクセス管理が可能になります。

YubiOn

会社 : <https://sgk.co.jp/>

サービス : <https://www.yubion.com/>

Windowsのリモートワークを実現するソリューション

セキュリティキーを使用して認証することで安全なリモートワークを実現する**Yubi Plus**



キーワード

- #Windowsログイン
- #リモートワーク
- #SalesforceのMFA
- #指紋認証
- #認証管理

スタンドアロン版は持ち出しPCなどの保護に最適。
リモートワークの実現に最適なネットワーク版では、
管理サーバでログの取得および
USBセキュリティ鍵の一元管理も可能です。

ラインアップ	スタンドアロン版 認証サーバ不要 持ち出しPCなど特定のPC保護に最適 ミニマムスタートに適しています	ネットワーク版 PCの台数に関係なく認証サーバで一元管理 テレワークに最適なリモートアクセスが可能
二要素認証	可能	可能
リモートアクセスの利用	—	可能
認証サーバ	不要	必要
ワークグループ環境での利用	可能	可能
Active Directory環境での利用	可能	可能
ログの取得	可能(自パソコン内に保存)	可能(認証サーバ内に保存)

Yubi Plus

会社 : <https://www.njs-net.co.jp/>

サービス : <https://www.njs-net.co.jp/product/service/yubiplus/>

人材紹介会社での導入事例

コロナ禍で従業員が事業所に集まらない中で、セキュリティを強化するためにセキュリティキーを導入。
PCのログインから使用しているWebサービスのログインをセキュリティキーを使用した多要素認証に切り替えた。
1週間で切り替えが完了し、セキュリティ強化以外にも以下のメリットがありました。

- #Windows□グオン
- #リモートワーク
- #指紋認証
- #認証管理
- #労務管理



「弊社は人材紹介会社ですが、数万人の求職者の方々からお預かりした個人情報をSalesforceで管理しており、絶対に不正ログインされるわけにはいきません。リモートワークでセキュリティ保護の運用が弱まってしまうおそれがあったためYubiKeyを導入しました。」

株式会社Sociarise 代表取締役 中村 拓海氏

	ログインに関する問い合わせ	パスワード変更の管理	PCのセットアップ	労務管理が正確に
導入前	月に1回程度発生	四半期に1度実施	各PCにセットアップが必要	従業員の申告のみ
導入後	導入後は 0件	セキュリティキー導入後は 不要	セキュリティキーにログイン情報があるため、PCのセットアップが 簡略化	ログイン時のログが簡単に収集できるため 労務実態の把握が可能に

会社概要・お問い合わせ

ABOUT-CONTACT

サービスに関するご相談・ご不明点などが御座いましたら、お気軽にご相談ください

- | | |
|--------|--------------------------------|
| ■ 社名 | PJ-T&C合同会社（ピージェーティーシー） |
| ■ 設立 | 2019年6月 |
| ■ 代表者 | 藤本 篤志（FUJIMOTO Atsushi） |
| ■ 事業内容 | 中小企業デジタル化支援、及びセキュリティソリューションの提供 |
| ■ 所在地 | 東京都中野区 |

グループ会社

株式会社PILOT-JAPAN

株式会社Sociarise

■ 企業情報

主要取引金融機関

巢鴨信用金庫中野支店

東京商工会議所会員（会員番号：C2838036）



PJ-T&C合同会社

Technology & Consulting

WEBサイトはこちら

<https://pj-tc.com/>



03-4400-6707

平日10時～17時



info@pj-tc.com