

# 次世代校務DXガイドブックへの対応

2026年9月

NEC プラットフォームテクノロジーサービス事業部門

# 目次

1. 次世代校務DXガイドブック セキュリティ要素技術のご紹介
2. アクセスの真正性に関する要素技術
  - ー多要素認証・リスクベース認証・SSO
3. 端末・サーバ・通信の安全性に関する要素技術
  - ーデータ暗号化

# 1.次世代校務DXガイドブック セキュリティ要素技術のご紹介

次世代校務 DXガイドブックに記載されたセキュリティ要素技術の導入が必要です。

## 強固なアクセス制御による対策に関わる要素技術

### ①アクセスの真正性に関する要素技術

- |     |                        |                                                                                                                                                                                                                          |
|-----|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ①-1 | <b>多要素認証</b>           | 知識認証（ID及びパスワード等）、生体認証（指紋、静脈、顔、声紋等）、物理認証（ICカード、USBトークン、トークン型ワンタイムパスワード等）のうち、異なる認証方式2要素以上を組み合わせる認証方法。なりすましや不正アクセスを防ぐ。<br>※強固なアクセス制御による対策を講じるに当たっては、学校現場の実態や特徴を踏まえ、端末の電子証明書等を用いた端末認証と、知識認証・生体認証のいずれかを組み合わせて利用者認証を行うことも考えられる |
| ①-2 | <b>リスクベース認証</b>        | 端末のIPアドレスや位置情報、使用されているWebブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める認証方法。なりすましや不正アクセスを防ぐ。                                                                                                                                    |
| ①-3 | <b>シングルサインオン (SSO)</b> | 一度の認証で複数のシステムへのアクセスが可能となる仕組み。利便性を向上させるとともに、認証の煩雑化によるセキュリティリスクの低減を図る。                                                                                                                                                     |

NeoFace Monitorクラウド版

Soliton OneGate ×  
Bio-IDiom 顔認証SSO連携

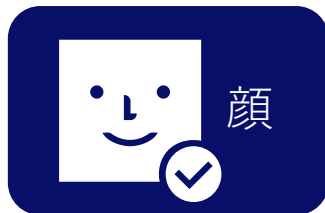
### ②端末・サーバ・通信の安全性に関する要素技術

- |     |                          |                                                                                                                                                                               |
|-----|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ②-1 | <b>通信の暗号化</b>            | 通信又は通信経路を暗号化し保護すること。第三者から通信内容を盗み見られることを防ぐ。                                                                                                                                    |
| ②-2 | <b>Webフィルタリング</b>        | インターネット上の特定のコンテンツやWebサイトへのアクセスを制限する機能。セキュリティリスクの高いWebサイトへのアクセスを防ぐ。                                                                                                            |
| ②-3 | <b>モバイル端末管理 (MDM)</b>    | 端末を一元的に監視・管理する機能。端末のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールが発生を防ぐとともに、紛失・盗難等の際に遠隔でデータ消去を行い情報漏洩を防ぐ。                                                      |
| ②-4 | <b>アンチウイルス</b>           | コンピュータウイルスやマルウェア感染への対策。既知のパターンファイル（マルウェア情報）からのマルウェアの検知・駆除や、不審な挙動をするプログラムの検知（ふるまい検知）・駆除等を行う。                                                                                   |
| ②-5 | <b>データ暗号化</b>            | 元データを変換し、第三者が簡単にデータの内容を解読できない状態にすること。アクセス権限が無い者の情報へのアクセスを制限する。                                                                                                                |
| ②-6 | <b>不正なアクセスを検知・遮断する技術</b> | 不正な通信を検知し、アクセスを遮断する等の制御を行う。<br>※不正なアクセスの検知（IDS）または遮断（IPS）による対策、エンドポイント対策（EDR等）、インターネットと繋がっているサーバ（Webサーバ）への外部からの攻撃を検知・防御する対策（WAF）、ネットワークとセキュリティを統合したクラウドサービスであるSASE等の活用が考えられる。 |

ActSecureクラウドセキュア  
ファイルサービス

出典：文部科学省「次世代の校務DXガイドブック」（令和7年3月）

## 顔認証(多要素認証)



### NeoFace Monitor クラウド版

- ・ PCログイン後も、**常時認証機能**により他者の不正利用を防止。
- ・ 多要素認証ガイドライン準拠
- ・ オンプレADに加え、Microsoft Entra ID (旧Azure AD)参加に対応。
- ・ 顔認証PCログイン製品の国内**シェアNo.1**。

## リスクベース認証/ SSO



### Soliton OneGate × Bio-IDiom 顔認証SSO連携

- ・ Soliton社のSoliton OneGateとNECのBio-IDiom 顔認証SSOを連携。
- ・ 校務システムや汎用クラウドサービスに対して、**顔認証を用いた多要素認証**が可能に。

## ファイル暗号化



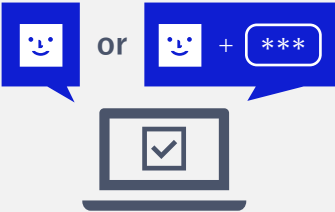
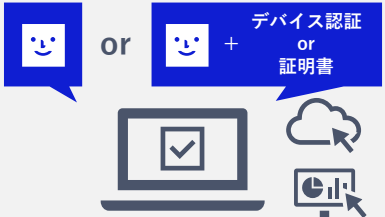
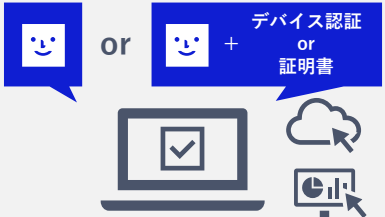
### ActSecureクラウドセキュア ファイルサービス

- ・ “**万一ファイルが流出しても安心!!**”
- ・ 自動でモレなくファイルを暗号化。
- ・ **導入後も利用者の操作は従来通り。**
- ・ 暗号化、解除の履歴が**ログに残り、追跡可能。**
- ・ 暗号化済みファイルを**簡単に視認**、拡張子も変更なし。
- ・ **サーバ構築不要**で簡単導入。

## 2.アクセスの真正性に関する要素技術 —多要素認証・リスクベース認証・SSO

# アクセスの真正性に関する3つの要素技術

アクセスの真正性には3つの要素技術がありますが、具体的に適用されるシーンは以下のようになります。  
ポイントとしては、**多要素認証**がリスクベース制御や、**シングルサインオン（SSO）**を実現するための手段としても利用される  
ということです。校務システムのクラウド化に際しては特に**SSOの多要素認証対応**が重要となります。

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                        |                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ガイドライン要件 ①-1<br/>多要素認証（なりすまし／不正アクセス防止技術含む）</p> <div><div><p>OSログオン</p><p>OSログオン時の認証</p></div><div><p>OSログオンにおける不正利用防止</p><div><p>離席時ロック</p><p>なりすまし防止</p></div></div></div> <td><p>ガイドライン要件①-2<br/>リスクベース認証</p><p>リスクベース制御</p><p>通常と異なる挙動を検知</p></td> <td><p>ガイドライン要件①-3<br/>シングルサインオン(SSO)</p><p>シングルサインオン</p><p>アプリログオン時の認証</p></td> | <p>ガイドライン要件①-2<br/>リスクベース認証</p> <p>リスクベース制御</p>  <p>通常と異なる挙動を検知</p> | <p>ガイドライン要件①-3<br/>シングルサインオン(SSO)</p> <p>シングルサインオン</p>  <p>アプリログオン時の認証</p> |
| <p>NECおすすめソリューション</p> <div><p>NeoFace Monitorクラウド版</p><ul style="list-style-type: none"><li>・生体認証を活用した<b>多要素認証利用</b>が可能</li><li>・画面ロック解除時の顔認証利用も可能</li><li>・利用者の<b>離席を検知</b>、画面ロックすることになりすまし利用を防止</li><li>・<b>未登録者は認証NG</b>から画面ロックになりすまし利用を防止</li></ul></div> <div><p>Soliton OneGate + Bio-IDiom 顔認証SSO</p><ul style="list-style-type: none"><li>・通常と異なるネットワークやデバイスの利用時に<b>追加の認証を要求</b></li><li>・生体認証を活用した<b>多要素認証利用</b>が可能</li><li>・<b>SAML/OIDCによるSSO</b>が可能</li></ul></div>                                                                                                                                                                                                                                                                                      |                                                                                                                                                        |                                                                                                                                                               |

以降のスライドで、ソリューションの詳細をご紹介します。

顔認証ならセキュリティと利便性の両立が可能です。  
慣れない端末の持ち出し運用でも安心を継続します。

## ログオン機能



カメラに顔を  
向けるとログオン

多要素認証に対応  
(パスワード+顔)

## 常時認証機能



一定間隔で  
ユーザを確認

※ 画面がロックされるタイミングは  
システム設定により変更可能

離席



画面  
ロック

離席時は本人検知エラー  
にて、画面をロック※

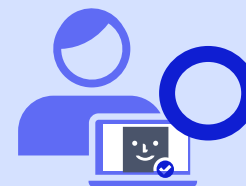
未登録ユーザ



画面  
ロック

ユーザ認証に失敗し  
画面をロック

## ロック解除機能

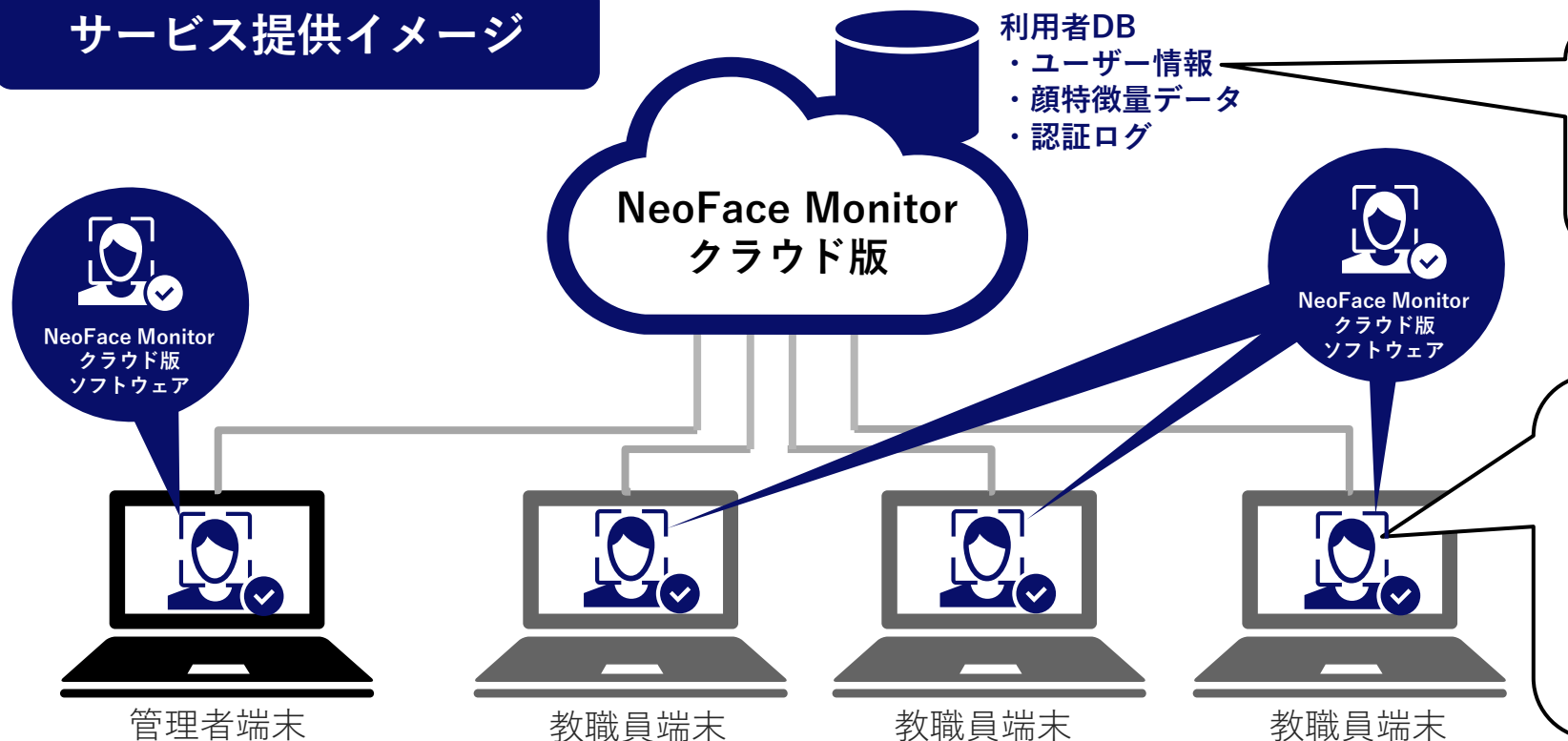


ロック解除もカメラ  
に顔を向けると完了

クラウドサービスのため**運用管理サーバが不要**です。

Point !

## サービス提供イメージ



クラウド提供の為、  
サーバ本体および  
構築・メンテナンス費用は不要！

Point !

PC(Windows)側は、顔認証に必要なクライアントソフトのインストールのみ！利用者様自身がクラウド上から必要なソフトウェアのダウンロードが可能！

「Windowsのローカルアカウント」「ドメインアカウント」「Microsoft Entra ID (旧Azure ADアカウント)」  
のログオン認証に対応

顔認証を含めた多要素認証によるPCセキュリティの導入は  
運用管理者様・教職員の皆さまに様々なメリットを提供いたします。

## 導入メリット

### ■ 情報漏洩リスクの軽減と生産性、セキュリティ意識の向上

- ・ 顔認証導入による不正抑止対策にて組織セキュリティを向上
- ・ 先進的なセキュリティ対策導入による従業員のセキュリティ意識の向上

### ■ 総合的なセキュリティ運用管理・調達コストの抑制

- ・ 利用者の認証強化とログ管理にて、統合的なセキュリティ管理を実現
- ・ パスワード忘れや、パスワード更新などの管理対応工数の削減
- ・ 指紋認証やICカード認証と比較した場合、専用装置の調達管理が不要

### ■ 教職員の利便性向上と業務効率化

- ・ カメラに顔を向けるだけでWindowsログオン認証できる利便性と快適性
- ・ Windowsログオン操作の簡易化による時間短縮で業務効率化

パスワード忘れ、  
更新の管理対応工数

**大幅削減**

POINT  
1

汎用のWebカメラで  
利用可能

- ・PC内蔵や外付けの汎用Webカメラを利用  
安価な導入や既存端末とのMIX運用など幅広いPC端末への適用が可能

Windows Helloは専用のIRカメラが必須

POINT  
2

認証速度や精度に優れ  
ストレスなく顔認証可能

- ・マスクを着けたままでも認証が可能
- ・斜めの顔向き(左右50度、上下30度)でもスムーズに認証

Windows Helloは左右15度まで

POINT  
3

PC利用中のなりすまし・  
共用端末不正利用を抑止

- ・常時認証機能およびなりすまし検知機能によりログオン後の不正利用リスクを低減
- ・アプリログイン代行機能やAPIオプションにて、特定業務アプリケーションへ顔認証ログインが可能
- ・共用端末利用時、1アカウントに対して複数のNeoFace Monitor利用者を設定可能

Windows Helloは1アカウント1利用者

POINT  
4

組織的なセキュリティ  
統合管理を実現

- ・顔+パスワードなど2要素ガイドラインに対応  
(Helloは顔のみで認証を行い、認証失敗時はPin入力に切り替わるため、生体認証の強制が不可)
- ・管理者にて利用者情報の登録を一元管理。不正な登録利用を防止するとともに、共有端末やPC交換時の顔画像再登録も不要
- ・全利用者の認証ログを一元管理することで、早期かつ確実なインシデントの把握が可能
- ・入退管理や認証印刷など他の顔認証製品との連携し統合的な顔認証ソリューション展開が可能

Windows Helloは利用者任せのセキュリティ運用

Soliton OneGateとNECのBio-IDiom 顔認証SSOを連携させることで、校務システムや汎用クラウドサービスに対して顔認証を用いた多要素認証が可能となります。



※ Windows、Android、iOSに対応。  
利用される構成によって、顔SSOの  
デバイス認証機能が利用できない場合  
があります。

校務DXとゼロトラストを支えるID基盤により、  
あらゆる認証をまとめて管理可能です。

クラウドもオンプレミスも  
認証を統合管理



- 多様化するIT環境（クラウド、社内システム、PC、ネットワーク）の認証を強化・統合
- 国産IDaaSとして、デジタル証明書を核とした多要素認証(MFA)を提供

3つの価値で  
DXとセキュリティを両立



セキュリティ強化

不正アクセス・情報漏えいから重要情報を保護



利便性の向上

パスワード管理の負担を軽減し、スムーズな業務アクセスを実現



運用負荷の軽減

ID管理や証明書運用を自動化・効率化

ポイント！

複雑化する認証の課題を、Soliton OneGateでシンプルに解決

学校に必要な認証を統合したオールインワンのID基盤であり、ネットワーク認証連携も可能です。

| 多要素認証                                                                                                                                            | シングルサインオン (SSO)                                                                                                                                | ネットワーク認証                                                                                                                             | ID管理・運用                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <p>デジタル証明書を核に、FIDO2、スマホ認証、ICカード、顔認証など多様な多要素認証（MFA）を柔軟に構成可能</p> |  <p>SAML対応クラウドサービスへのSSO、および代理認証アプリによるSAML非対応システムへのSSOを実現</p> |  <p>デジタル証明書を用いたWi-Fi/VPN認証で、不正な端末のネットワーク接続を防止</p> |  <p>AD/Entra ID連携やIDプロビジョニングでID管理を自動化。<br/>デジタル証明書の容易な発行・運用管理を実現</p> |

ポイント！

認証に関わる機能を幅広くカバー。統合的なセキュリティ基盤を構築

# Soliton OneGate × Bio-IDiom 顔認証SSOの連携 顔認証SSOでより簡単にシステムが利用可能に

BluStellar

## Before



多くのID/PWを管理（喪失・漏洩のリスクあり）

すべてのサービスでログイン操作が必要

第三者のなりすましが可能

## After



ID/PWの管理が不要

1度の顔認証で複数のサービスをすぐに利用できる

生体認証とデバイス認証の多要素認証のため、  
なりすましが困難

# (ご参考) 顔認証の位置づけ

顔認証は、生体認証の中でも特に  
**精度と利便性が両立**した認証方式



## 1 自然な認証

顔は、普段から人間が相手を判別する手段として利用している身近な認証方式であり、利用者の心理的負担が少ない

## 2 タッチレス(非接触)

タッチレス認証により高い利便性に加え、衛生面でも優れた認証方式

## 3 生体情報の登録が容易

スマホのカメラ等、身近な端末で利用者自身が自分で登録が可能

## 4 専用装置が不要

一般的なWebカメラも利用可能であり、登録用データとして既存の顔写真利用も可能なため、専用装置が不要

NEC調べ (2022/6)

●精度は本人拒否率/他人受入率、登録未対応率などから総合的に評価 ●利便性は認証速度、登録装置の要不要、非接触などから総合的に評価

### 3. 端末・サーバ・通信の安全性に関する要素技術 —データ暗号化—

データ  
自動保護



様々な形式の  
データを自動保護

- ファイル自動保護  
様々なファイルに対応
- ファイル操作ログ収集

利便性  
そのまま



利用者の負担にならない  
利便性/操作性

- 復号せずに閲覧/編集  
再暗号化が不要
- 日常のID/パスワードが  
利用可能（都度入力不要）
- 鍵アイコン付与で視認性向上

簡単導入  
+  
運用サポート



迅速な導入対応と  
負担とならない運用性

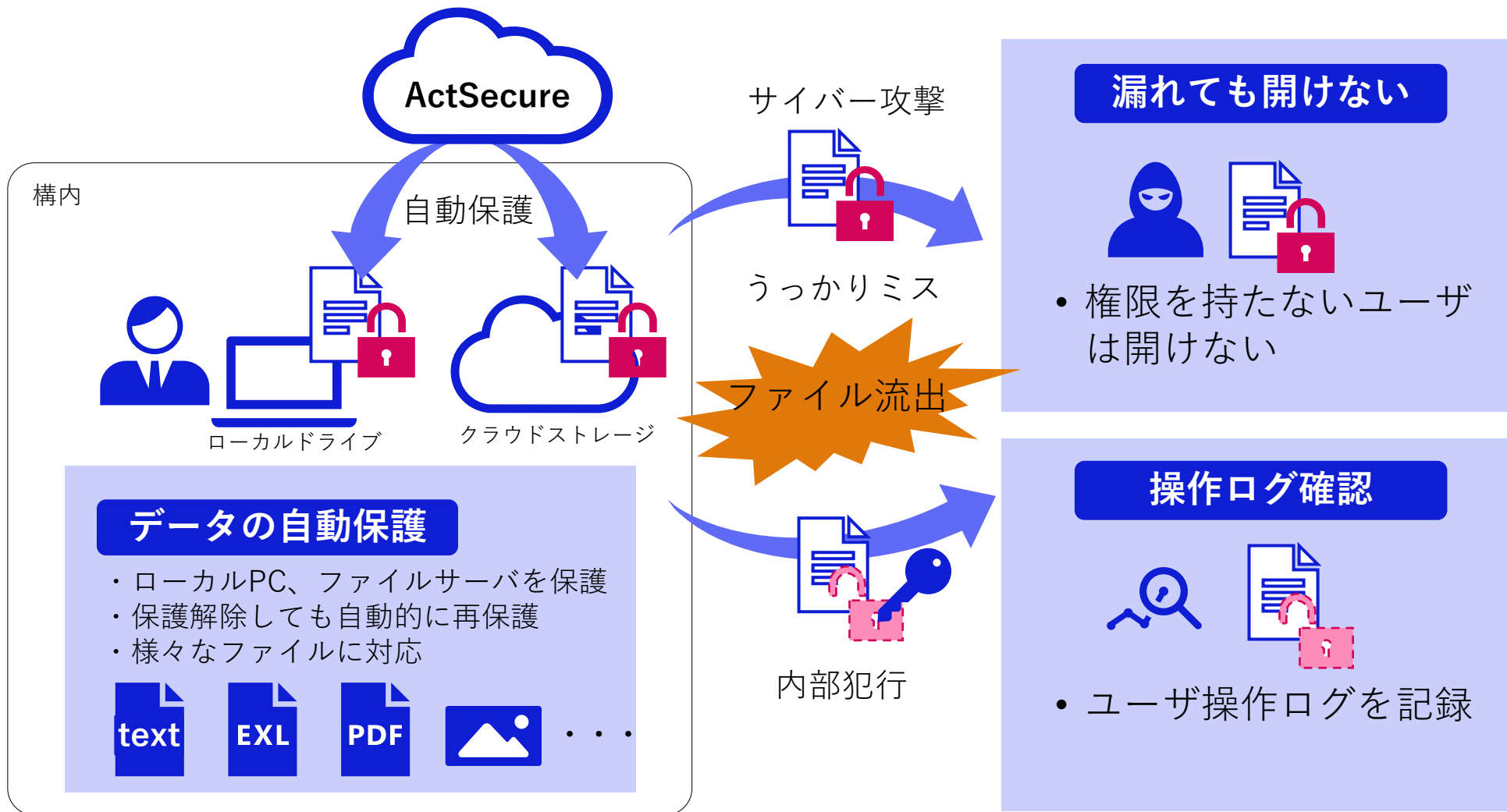
- 最短 5 営業日で利用開始  
（サービス申請書提出後）
- システム運用はサービスで実施

# ActSecureクラウドセキュアファイルサービス 様々な形式のデータを自動保護

BluStellar

データ  
自動保護

様々な形式のデータを自動的に保護



利便性  
そのまま

セキュリティを高めつつ、操作性・視認性を確保



従来と変わらぬ  
操作性・視認性

保護済みファイル  
アイコン



既存のアイコンに  
鍵マーク付与

## 操作性

- ・アイコンクリックでアプリケーション起動
- ・ID/パスワードの入力は不要
- ・保護したまま閲覧・編集



- ◎煩わしい保護解除が不要
- ◎ファイル利用中の安全性を維持
- ◎再暗号化し忘れのリスクが無い

## 視認性

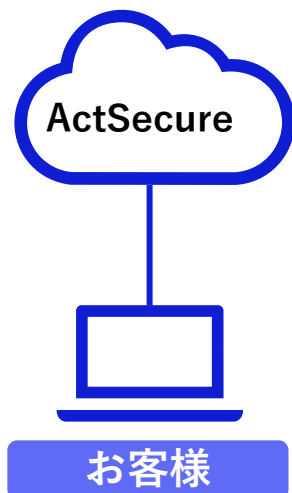
- ・アイコンはアプリケーションイメージを維持
- ・鍵マーク付与で保護状態を簡単に視認
- ・ファイル名、拡張子名も変わらない

# ActSecureクラウドセキュアファイルサービス 迅速な導入対応と負担とならない運用性

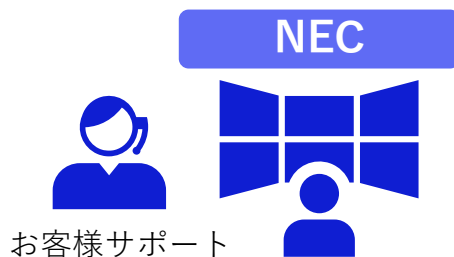
BluStellar



クラウドサービスによるファイル保護環境の提供



[ActSecure サービスデスク]



## スピード導入

- ActSecureでファイル保護機能をご提供（最短 5 営業日）
- お客様環境に必要なもの
  - ・ クライアントソフトウェア
  - ・ 本サービスへ接続するInternet環境

※RMS版を利用する場合はお客様自身でEntra IDなどの事前設定が必要です。

## 保守

- サーバ構築不要、保守の手間を軽減

## サポート

- お客様サポート窓口を開設
- ファイル保護ルール変更、運用設定変更、調査など、NECが支援

**NEC**

\Orchestrating a brighter world