業界のガイドラインを読み解く、

多要素認証の要点とは？ - エンドポイント編 -

近年の脅威動向

IPA

情報セキュリティ10大脅威 2023

(組織編)

セキュリティ水準の底上げが必要、
業界のセキュリティガイドライン強化に繋がっている

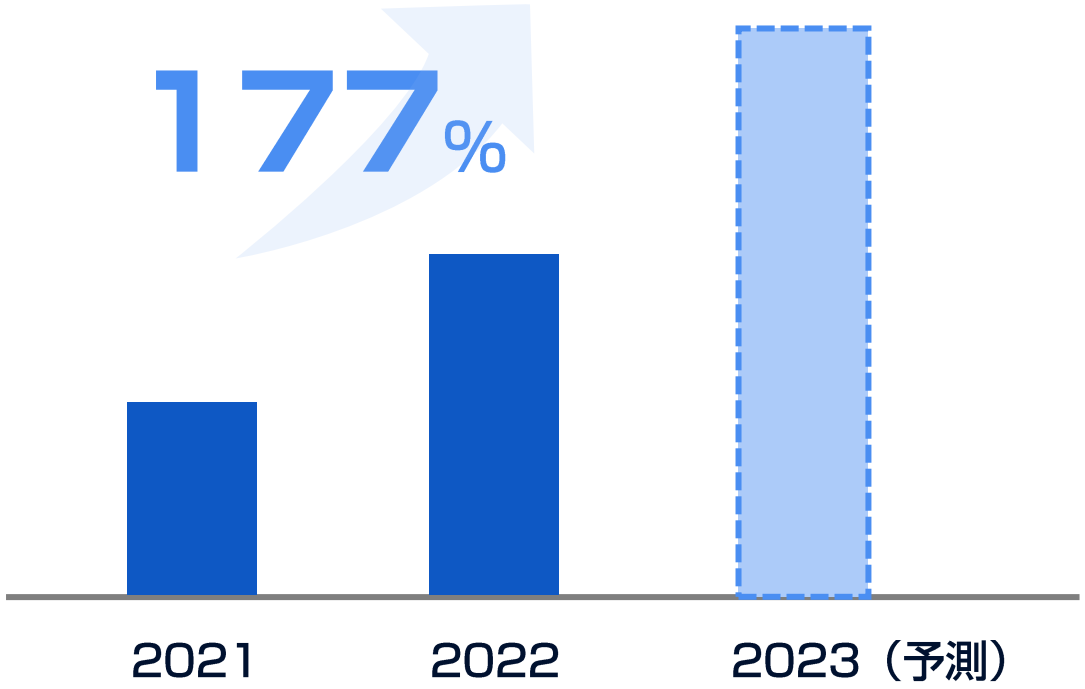
被害の増大に、
デジタル化や働き方改革の影響が見られる

10大脅威	順位	
ランサムウェアによる被害	1位	
サプライチェーンの弱点を悪用した攻撃	2位	↑
標的型攻撃による機密情報の窃取	3位	
内部不正による情報漏えい	4位	↑
テレワーク等の ニューノーマルな働き方を狙った攻撃	5位	
修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）	6位	
ビジネスメール詐欺による金銭被害	7位	
脆弱性対策情報の公開に伴う悪用増加	8位	
不注意による情報漏えい等の被害	9位	
犯罪のビジネス化 （アンダーグラウンドサービス）	10位	

https://www.ipa.go.jp/security/vuln/10threats2023.html

多要素認証のニーズが変化

- 多要素認証ソフト 「SmartOn」 新規出荷の推移



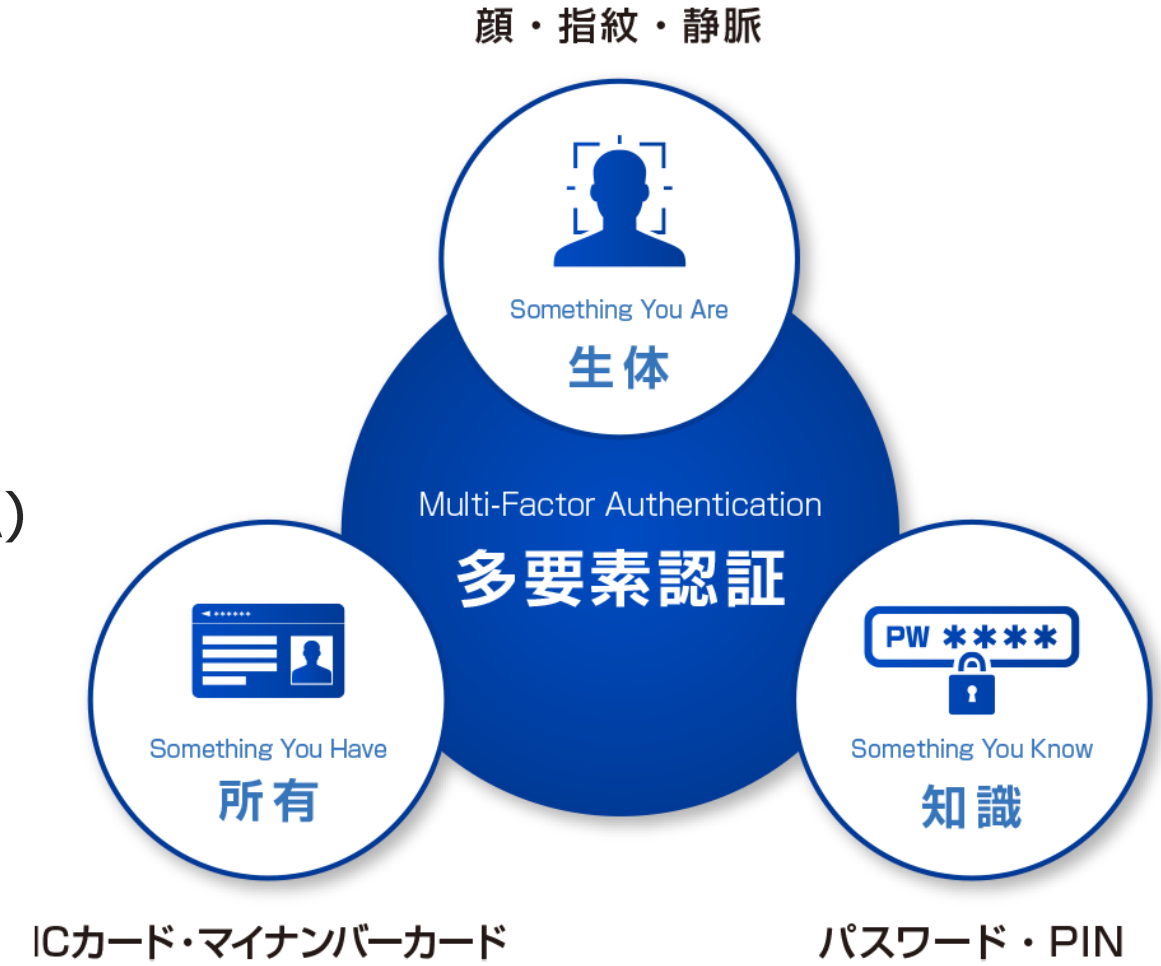
導入が明らかに**活発化**

一般的な対策 になりつつある

多要素認証とは？

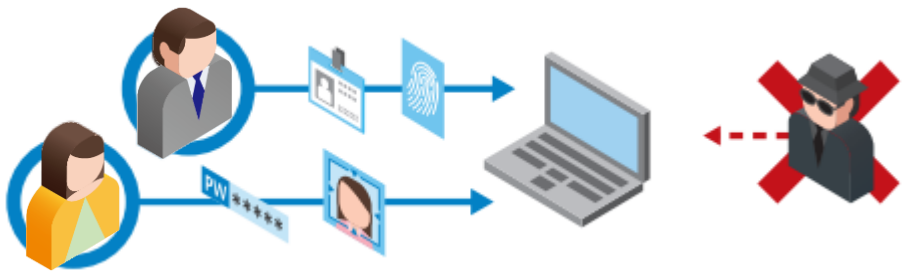
複数の要素を組み合わせて行う認証方法

Multi-Factor Authentication（MFA）



多要素認証の利用場面

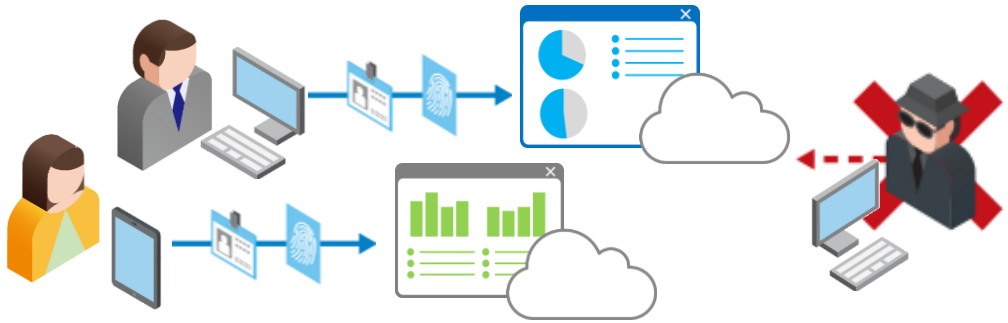
PC自体へのログイン



- PCなどの業務端末を利用する時の認証
- 主に法規制の遵守、ガイドライン対応で導入しなければならないことが多い

↑今回はこちら

クラウドサービスのログイン



- クラウドサービスを利用する時のアプリ認証
- サービス提供ベンダーの利用者規定により、導入・対応が必要となる場合がある

Soliton OneGate

多要素認証が導入される理由

1 業務のデジタル化

- 守るべき情報資産が急増
- PCに適切な鍵をかけて、秘匿情報として扱えるようにする必要がある

2 セキュリティガイドライン整備

- 経済安全保障の観点から、サプライチェーンリスク対策として、各業界のセキュリティガイドラインが強化され、その準拠に迫られている。

業務のデジタル化による変化

入り口であるPCを守る

近年における法律の改訂

法律	対象	近年行われた違反時罰則強化	近年の改訂ポイント（一部）
個人情報の 保護に関する法律	個人情報	行為者：1年以下の懲役又は50万円以下の罰金 法人：50万円→**1億円**以下の罰金 ※不正な利益を図る目的の提供・盗用の場合	• 利用目的明確化 • 開示・利用停止等への対応 • 個人関連情報の新設 • 外国への提供など • 個人情報保護委員会・本人への報告義務
不正競争 防止法	営業秘密	行為者：10年以下の懲役又は1000万円 →**2000万円**以下の罰金（併科あり。海外重罰併科時は3000万円以下） 法人：3億円→**5億円**以下の罰金（海外重罰併科時は10億円以下）	• 営業秘密の**保護範囲拡大**（刑事・民事上） • 罰則強化による抑止力向上 • 立証責任の転換、除斥期間延長

情報漏えいは企業経営の観点だけでなく、
国家の経済安全保障の観点でも大きな課題

導入される理由

1 業務のデジタル化

- 守るべき情報資産が急増
- PCに適切な鍵をかけて、秘匿情報として扱えるようにする必要がある

2 セキュリティガイドライン整備

- 経済安全保障の観点から、サプライチェーンリスク対策として、各業界のセキュリティガイドラインが強化され、その準拠に迫られている。

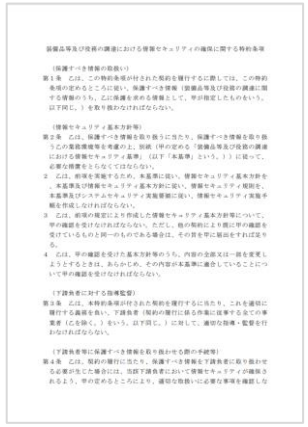
多要素認証が明記されているガイドラインの例

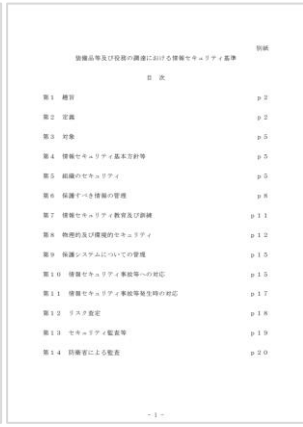
名称	業界
政府機関等のサイバーセキュリティ対策のための統一基準群	**官公庁・独法**
防衛産業サイバーセキュリティ基準 ：保護システムへアクセスする場合には必須。2023年以降の契約に適用	**防衛産業**
地方公共団体における情報セキュリティポリシーに関するガイドライン ：導入を推奨。マイナンバー端末には必須	**自治体**
教育情報セキュリティポリシーに関するガイドライン ：2021年5月の改訂で教育情報システムへの接続に関し多要素認証の導入を明記	**教育**
医療情報システムの安全管理に関するガイドライン ：古くから推奨され続けてきたが、昨年のV5.2でついに必須化	**医療**
FISC 安全対策基準	**金融**
PCI DSS ：昨年のV4.0から更に強化、範囲拡大。クレジットカード会員情報を扱う場合には必須	**金融**

防衛産業サイバーセキュリティ基準

- リリース　：2022年4月1日
- 米国の取り組み(NIST SP800-171等)を参考にした厳格な情報セキュリティ基準
- 対象　：防衛省との契約に基づき保護すべき情報等を扱っている企業全て
- 適用時期　：令和5年度(2023年度)の契約から適用

※ システム換装等を考慮し一定の移行期間(最長5年間)を設定するも、
サイバー情勢も踏まえ、できるだけ早期の導入が推奨される





防衛産業サイバーセキュリティ基準の整備について(防衛装備庁)
https://www.mod.go.jp/atla/cybersecurity.html

第6 識別及び認証

1 識別及び認証等の実施

（2） 認証の実施

PCログオン時は多要素認証

ア　保護システム管理者は、保護システム利用者が第5第2項第1号の規定により付与されたアカウントで 保護システムにログオンする場合は、本人だけが知る要素（以下「知識要素」という。）、本人だけが所有する要素（以下「所持要素」という。）及び本人の持つ生体的要素（以下「生体要素」という。）のうち 複数の異なる要素を保持すると認められた者のみを許可（以下「多要素認証」という。）するものとする。

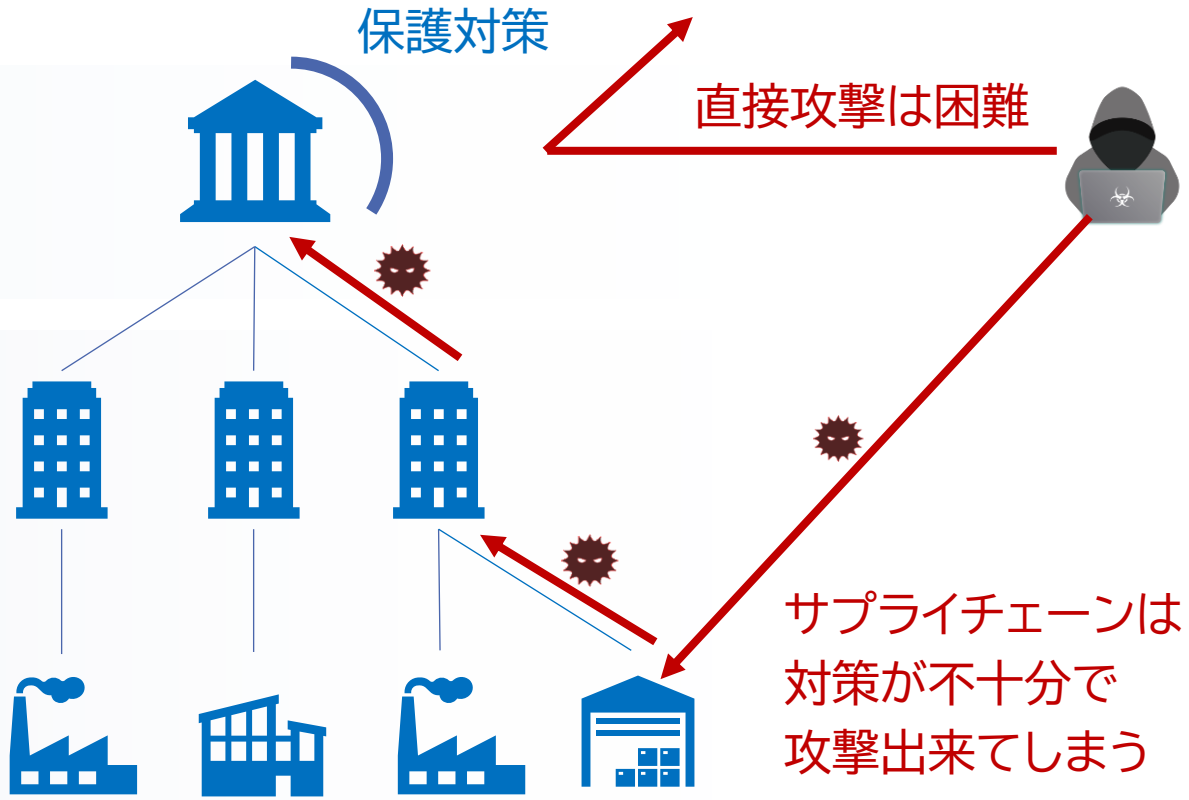
イ　保護システム利用者が保護システムに対し、リモートアクセスによりログオンする場合は、アに規定する 多要素認証をリプレイ攻撃に耐性のある方式で行う ものとする。

特にリモートアクセスでのログオンでは、攻撃耐性の強い方式を求めている

➤ Tier2/Tier3 からの問い合わせも多い

NIST SP800-171 ← サプライチェーンリスク対策

NIST規格	対象情報	対象組織
SP800-53	機密情報(CI) Classified Information	政府機関
SP800-171	保全が必要な情報(CUI) Controlled Unclassified Information	防衛産業
		下請企業



国内でも、サプライチェーン全体のセキュリティ向上を目指す動きが進む

経済安全保障とセキュリティガイドライン

- 2015年6月 NIST SP800-171 初版
- 2020年2月 NIST SP800-171 Rev2公開
  - 米国の国防調達においては、保全が必要な情報（CUI）を取り扱うすべての調達先企業に対し、NIST SP800-171の要求事項を満たすことが義務化。2017年末以降、米国国防産業に適用。

▼

- 2022年4月　防衛装備庁**「防衛産業サイバーセキュリティ基準」**を整備
  - 2023年度の調達から適用開始
  - システム換装等を考慮し一定の移行期間（最長5年間）が設定されるも、早期対応が求められる

- 2022年5月**「経済安全保障 推進法」**が成立・公布
  - 各業界でサプライチェーンリスク対策のガイドラインや基準などの策定が進む

『重要技術の保全』と
『基幹インフラなどの保護』

経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）（令和4年法律第43号）
https://www.cao.go.jp/keizai_anzen_hosho/index.html

経済安全保障を背景に強化されるガイドライン

名称	業界
政府機関等のサイバーセキュリティ対策のための統一基準群	**官公庁・独法**
防衛産業サイバーセキュリティ基準 ：保護システムへアクセスする場合には必須。2023年以降の契約に適用	**防衛産業**
地方公共団体における情報セキュリティポリシーに関するガイドライン ：導入を推奨。マイナンバー端末には必須	**自治体**
教育情報セキュリティポリシーに関するガイドライン ：2021年5月の改訂で教育情報システムへの接続に関し多要素認証の導入を明記	**教育**
医療情報システムの安全管理に関するガイドライン ：古くから推奨され続けてきたが、昨年のV5.2でついに必須化	**医療**
FISC 安全対策基準	**金融**
PCI DSS ：昨年のV4.0から更に強化、範囲拡大。クレジットカード会員情報を扱う場合には必須	**金融**

ガイドライン要件に加え、
自組織の運用に沿った導入検討が大切

医療情報システムの安全管理に関するガイドライン 第5.2版

6. 医療情報システムの基本的な安全管理
6.5. 技術的安全対策 「利用者の識別・認証」

(1) 利用者の識別・認証

医療情報システムへのアクセスを正当な利用者のみに限定するために、医療情報システムは利用者の識別・認証を行う機能を持たなければならない。

小規模な医療機関等で医療情報システムの利用者が限定される場合には、日常の業務の際に必ずしも識別・認証が必須とは考えられないケースが想定されることもあるが、一般的にこの機能は必須である。

認証を実施するためには、医療情報システムへのアクセスを行う全ての職員及び関係

得ない状態を保つ必要がある。

認証強度の考え方として、現状において、医療情報システムにアクセスする端末ごとに二要素認証を追加実装することは、医療機関等の負担が増加すると考えられる。このような技術は、本来システムにあらかじめ実装されているべきであり、今後、認証に係る技術の端末への実装状況等を考慮し、できるだけ早期に対応することが求められる（※）。

※ 二要素認証技術の端末等への実装を促してきたが、さらに強く推し進めるため、令和 9 年度時点で稼働していることが想定される医療情報システムを、今後、導入又は更新する場合、原則として二要素認証を採用することが求められる。

（これまで）二要素認証技術の端末等への実装を促してきたが、さらに強く推し進めるため

C. 最低限のガイドライン

1. 医療情報システムへのアクセスにおける利用者の識別・認証を行うこと。
2. 利用者の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合、それらの情報を、本人しか知り得ない状態に保つよう対策を実施すること。
3. 利用者
の破
よる
4. 利用者
の者による入力のおそれがある場合には、クリアスクリーン等の対策を実施させること。
13. 令和 9 年度時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新に際しては、二要素認証を採用するシステムの導入、又はこれに相当する対応を行うこと。

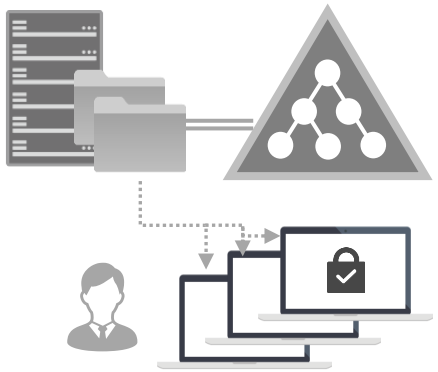
D. 推奨されるガイドライン

5. 利用者認証には、ID・パスワード＋バイオメトリクス又は IC カード等のセキュリティ・デバイス＋パスワード若しくはバイオメトリクスのように、2 つの独立した要素を用いて行う方式（二要素認証）等、より認証強度が高い方式を採用すること。ただし、医療情報システムを利用する端末に二要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め二要素以上（記憶・生体計測・物理媒体のいずれか 2 つ以上）の認証がなされていれば、二要素認証に相当すると考えてよい。
6. 許可された者以外の無線 LAN の利用を防止するため、例えば 802.1x や電子証明書を組み合わせるなどして、無線 LAN のセキュリティを強化すること。

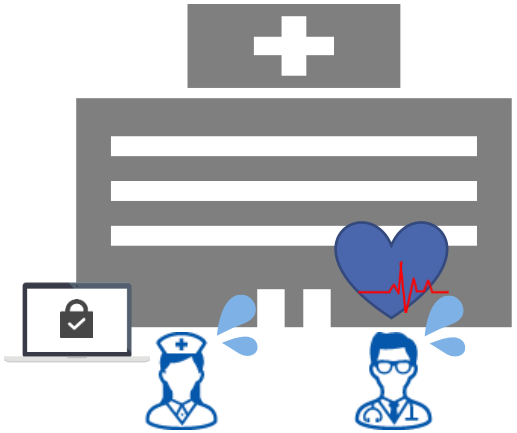
ICカード＋生体認証のように、より認証強度が高い方式を採用すること

2027年に稼働していると想定されるシステムの利用時には必須

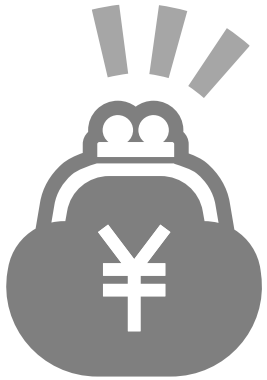
多要素（二要素）認証導入の課題



新規システム
導入のハードル



現場業務に
対する影響



コスト

『新規システム導入のハードル』を解消する

- 中心にあるのは
  電子カルテシステム
- 導入に負荷を掛けない
- 長期的に使う

**新規システム
導入のハードル**

選定のポイント

- **病院での導入実績がある**
- **構築・展開・切り替えが容易**
- **柔軟な運用ができ、使い続けられる**

『現場医療業務に対する影響』を解消する

- 現場業務への支障
- 医療現場では、
  手袋やマスクを着用
- 共有PCの運用

現場医療業務に対する影響

選定のポイント

- **認証 →ログオンがスムーズ**
- **マスク着用のまま認証できる**
- **共有PC環境に対応可能な仕組み**

『コスト』の課題を解決する

- 投資は最小限にしたい

コスト

選定のポイント

- **導入・運用コストが抑えられる**
- **高額な外付けデバイスが不要**
- **安心して、長く使える**

例えば、ソリトンの SmartOn

18年連続

SmartOn® は 国内シェアNo.1 の PCログオン認証製品です

安心と信頼の実績

- 累計4,500社、350万ライセンス
- 豊富な機能、柔軟な設計
- 実績十分な構築パートナー様が多数

※ 出展「2004～2021ネットワークセキュリティビジネス調査総覧デバイス認証ツール」 富士キメラ総研

導入・運用を支援する、様々な機能

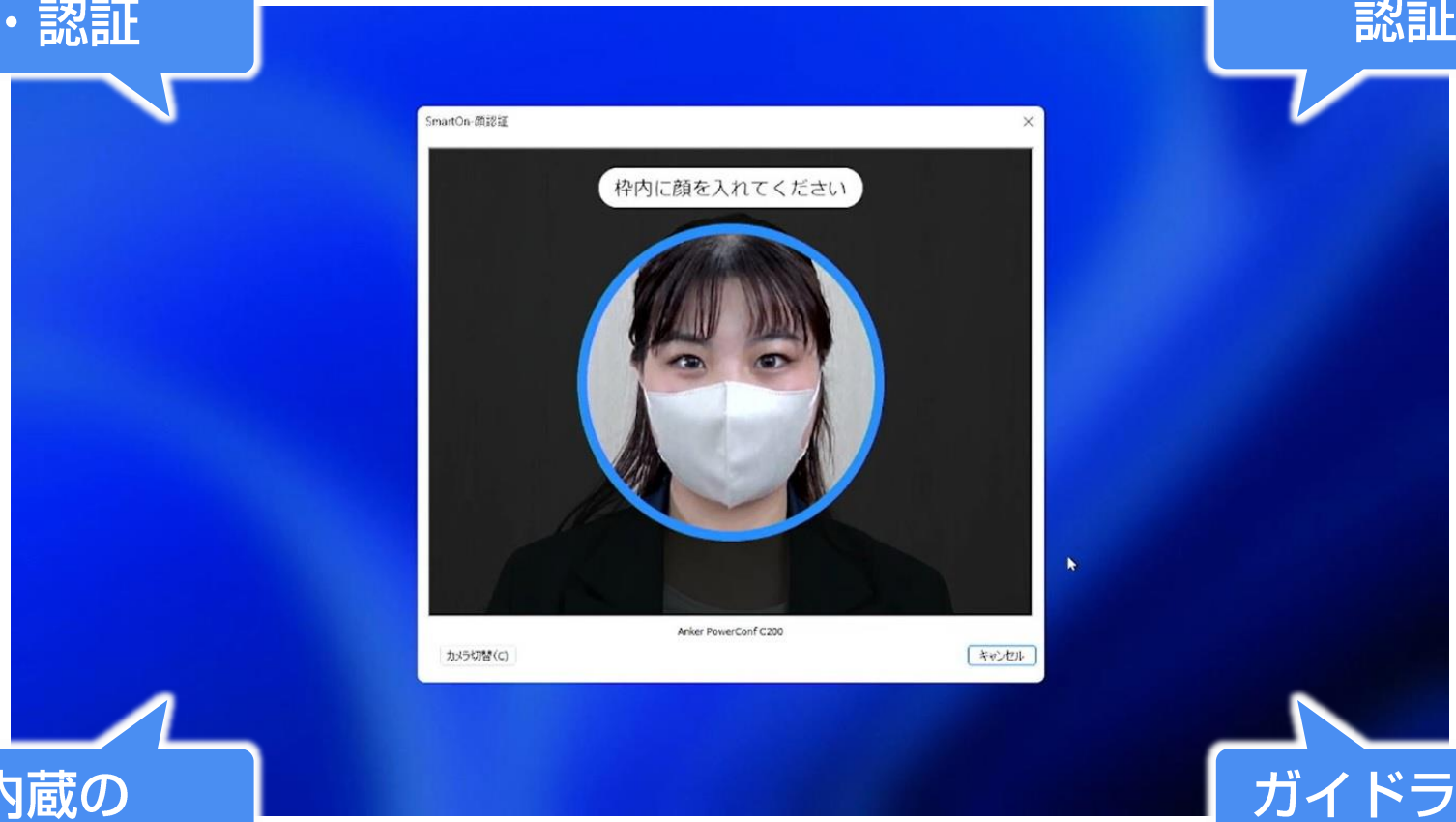
- Agentのサイレントインストール
- 選べるトークン
- 認証情報の一括登録
  or 初回ログオン時の自動登録
- Agentの自動バージョンアップ
- 代用コード発行
- 生体情報を安全に保管

etc.

現場に負担をかけない認証技術

スムーズな
登録・認証

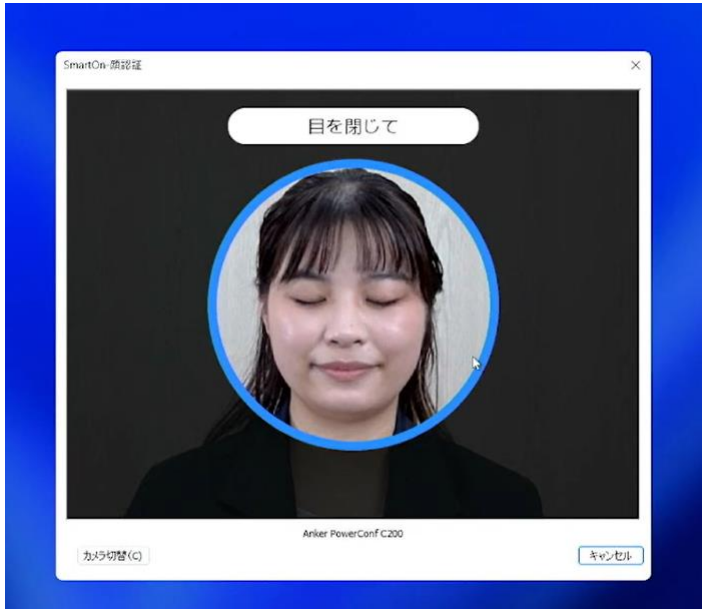
世界最高水準の
認証性能

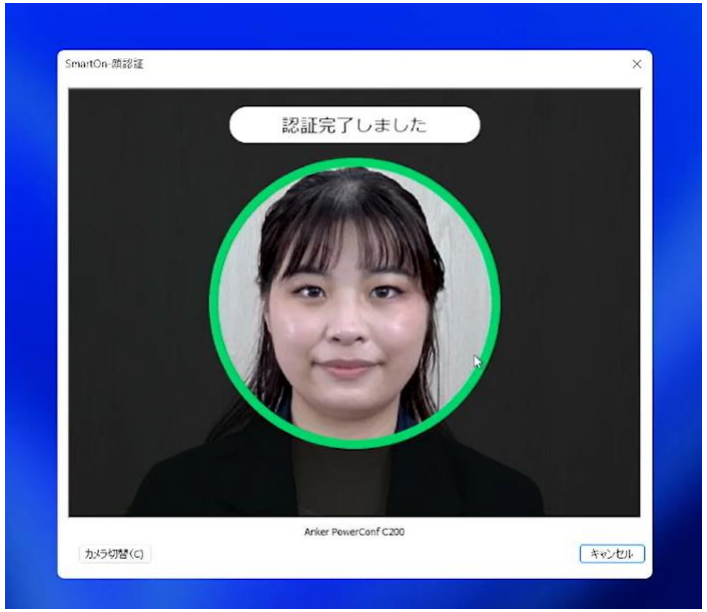


PC内蔵の
カメラでもOK

ガイドラインにも
対応

現場に負担をかけない認証技術

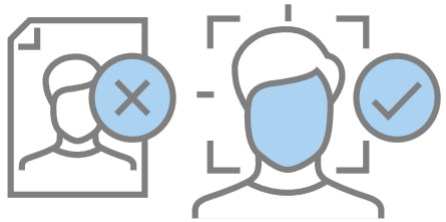




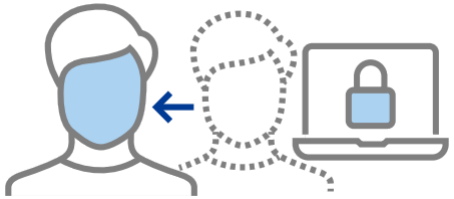
マスク着用時も認証 ◎

まばたき検知機能で、なりすましを防止 ◎

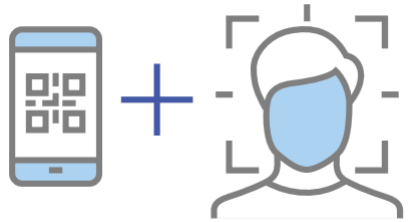
さまざまな要件に対応



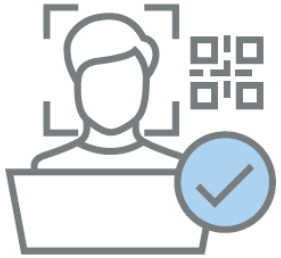
まばたき検知機能



離席ロック機能



ワンタイムQR



パスワードレス認証

仮想デスクトップ認証

シングルサインオン

CaseStudy
導入事例

政令市水道局

VDI×多要素認証　顔認証 / 約2千ユーザー

導入背景

- 2020年6月に米国で起きた「水道産業用制御システムを対象とした不正アクセス」の事案を受け、制御システムへの入り口となるVDIの認証を、より強固なものにすることが求められた

活用メリット

- VDIログオン時に多要素認証を利用、重要インフラへの不正アクセスを許容しないシステムを構築
- 共有PCでも、本人認証ログを記録し、内部不正を抑止

水道業務システム

制御システム

浄水場

CaseStudy
導入事例

クレジットカード会社

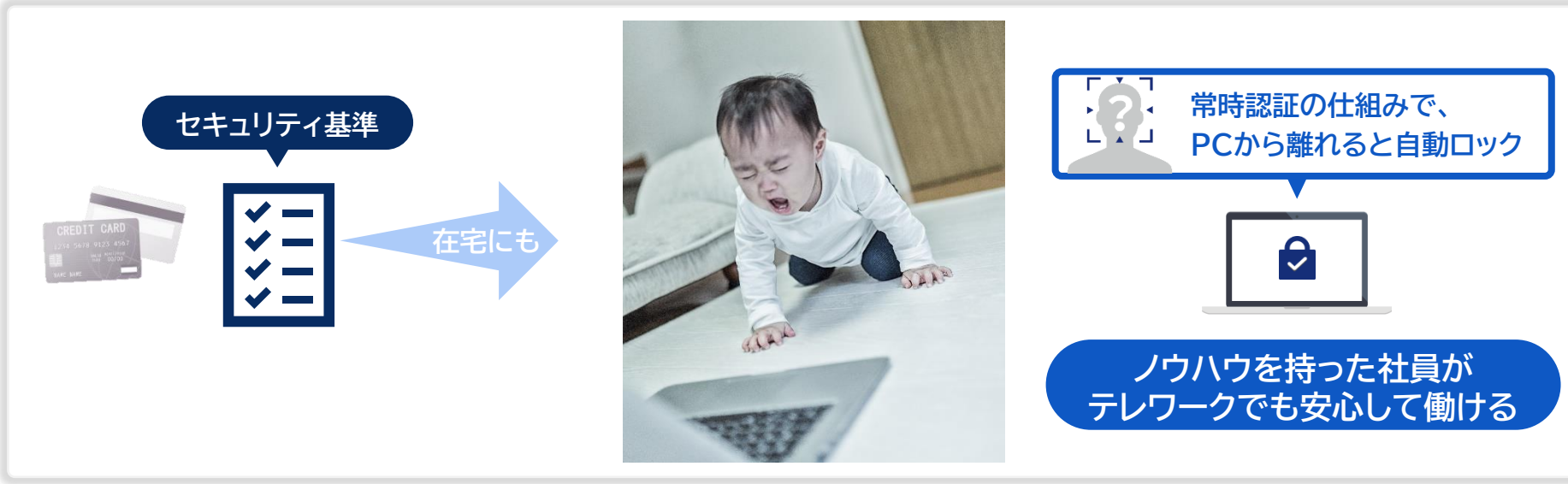
共有PC×多要素認証　顔認証 / 約3千ユーザー

導入背景

- ノートPCへの移行を機に、ICカード認証から、Webカメラを利用できる顔認証に切り替え
- 働き方改革の一環で、時短・自宅勤務者でも安全に業務ができる認証環境が必要であった。

活用メリット

- クレジットカード情報を扱うためのセキュリティ基準である、多要素認証要件を満たすことができた
- 柔軟なポリシー適用（離席ロック等）により、可用性を担保しつつ共有PCのセキュリティも強化
- 業務ポータルとSSO連携、社員はシステム毎のパスワード管理から解放され生産性も向上



まとめ

デジタル化、コロナ禍による環境の変化で、情報漏えい被害のリスクが増大

業界のセキュリティガイドラインに則って、対策を講じる必要がある

サプライチェーンリスク対策や経済安全保障の観点から、各種ガイドラインは軒並み強化

高いセキュリティが、サプライチェーン企業にも求められている

自組織の業態や運用に合わせて適切に検討し、後戻りない製品選定を

実績No.1で導入・運用しやすい多要素認証ソフトがおススメ