サイバートラスト デバイス ID ご紹介資料

cybertrust

v8.6　241127

情報セキュリティ10大脅威 2024

順位	組織向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続 9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続 6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続 9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続 9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続 3回目
6	不注意による情報漏えい等の被害	2016年	6年連続 7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続 7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続 7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続 4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続 4回目

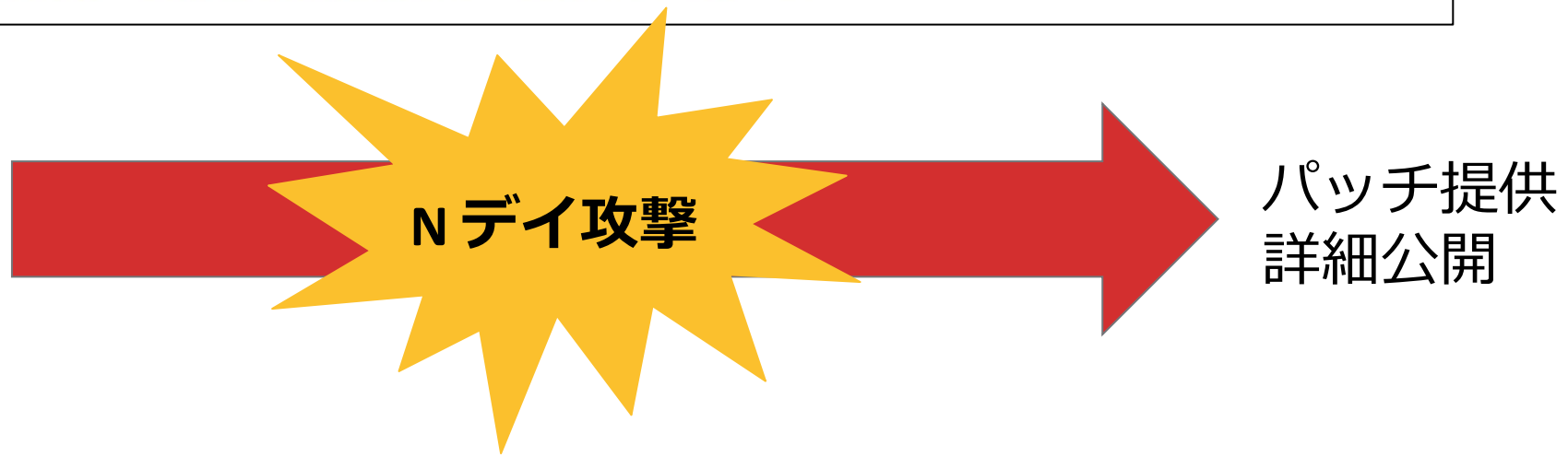
（出典）情報処理推進機構（IPA）「情報セキュリティ10 大脅威 2024」

脆弱性を悪用したインシデント事例

2020年：不正アクセス・情報漏えい

FortiOS

米フォーティネットのセキュリティー機器からVPNの認証情報が外部に流出した。岐阜県庁など国内の約600組織で、ユーザーIDや平文のパスワードなどが漏洩した。原因はセキュリティー機器が備えるSSL-VPN機能の脆弱性にあった。被害に遭った企業の多くは脆弱性の存在に気づかず、パッチを適用していなかった。新型コロナ禍でテレワークが急速に広がるなか、VPNが標的になるケースが増えている。



出典：https://xtech.nikkei.com/atcl/nxt/column/18/01157/122400026/

認証情報漏えいと不正アクセスの実態

フィッシングや標的型攻撃などで流出した「実在するID/パスワード」の悪用

通信経路を隠蔽する手口による送信元偽装で不正ログイン試行が巧妙化

パスワード漏えい事例

- Dropbox、6800万のアカウントデータを漏洩　パスワードの変更を［2016年8月］
- Gmail・Hotmail・Yahoo!などから2億7200万件のメールアドレスとパスワードが流出［2016年5月］
- 「ヤフー」など31サイトから178万件のID・パスワードが流出！［2016年3月］
- 北海道の中学校にて学力テスト用のID・パスワード漏えい［2016年5月］

漏えいしたパスワードによる不正アクセス事例

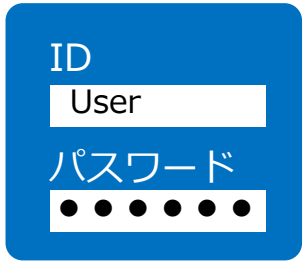
- Twitter社、アカウント漏えいは他サーバのパスワード使い回しが原因と発表［2016年6月］
- Amebaのアカウント5万件に不正ログイン　流出済みのID・パスワードを用いたリスト型攻撃［2016年4月］
- パスワードリスト攻撃」による不正ログインによるポイント交換被害が発生　マツモトキヨシ［2016年11月］
- セシール通販サイトに再度不正ログイン　「パスワードリスト攻撃」と見られる［2016年9月］

他システムで詐取されたパスワードによる不正アクセス対策

情報資産へのアクセス：二要素で認証
漏えいしたパスワードだけではログインができない

アクセスできる
「人」と「端末」による
二要素認証

許可された人
「ユーザ認証」



許可された端末
「端末認証」

デバイス証明書

安全かつ利便性の高い認証

ID・パスワード漏えい

⇒ **端末がなければアクセス不可**

端末紛失

⇒ **証明書の失効**

二要素認証：　ワンタイムパスワード、マトリックス認証、生体認証 etc.

ワークスタイルの多様化によるアクセス管理

マルチデバイス環境での最適な認証方式は？

「人の特定」（ユーザ認証）と「端末の特定」（端末認証）の方式

認証方式	人の特定	端末の特定
ID/パスワード	○	×
ワンタイムパスワード	○	×
マトリックス認証	○	×
生体認証	○	×
MACアドレス認証	×	○
証明書認証	○	○

マルチデバイスでサポートされている「端末特定」の方式

端末の特定	Windows	iOS	Android
MACアドレス認証	○	×	△
証明書認証	○	○	○

マルチデバイス環境で最適なデバイス認証は、デバイス証明書認証

サイバートラスト デバイスID 概要

ポイント 1

厳格な端末認証を実現

許可された端末だけにインターネット経由で証明書を自動登録可能

ポイント 2

マルチデバイス対応

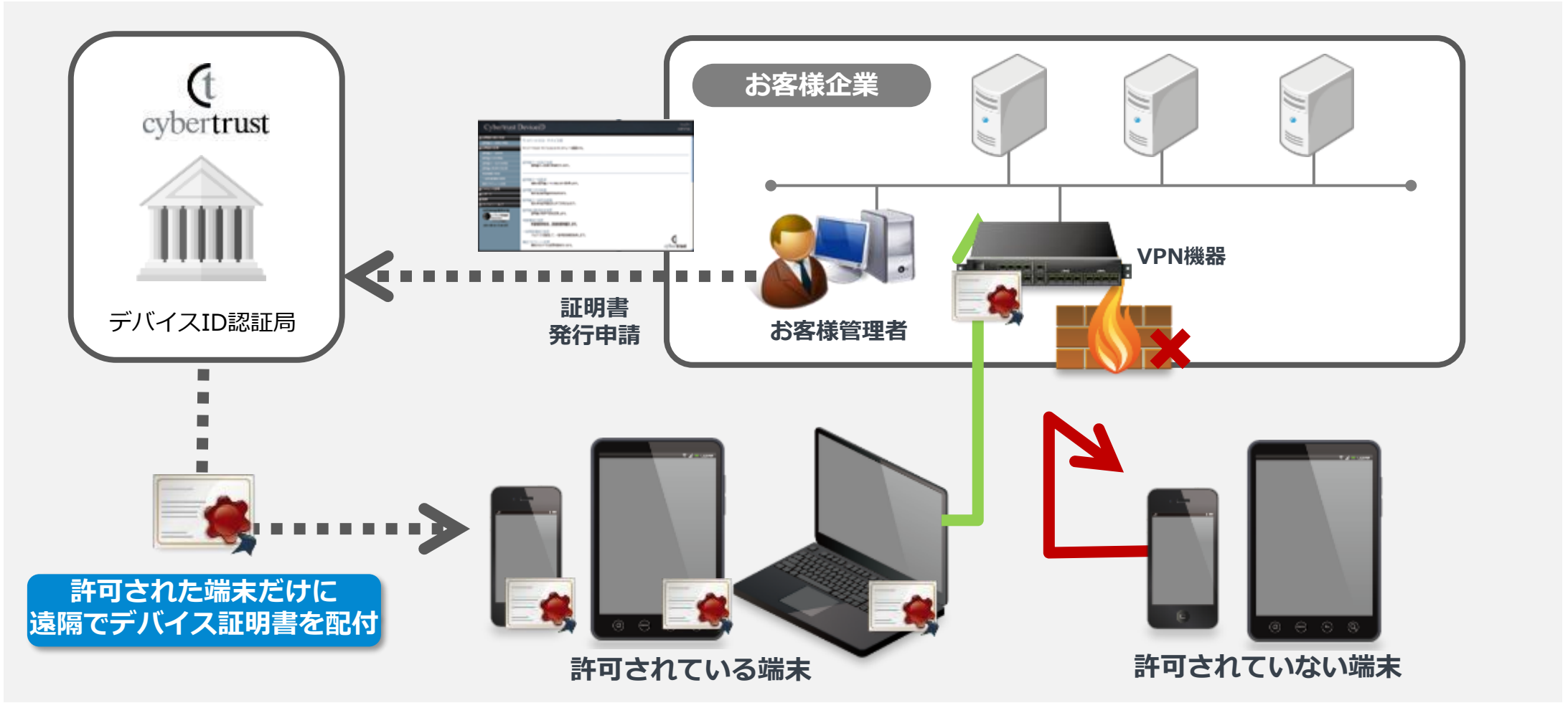
Windows、macOS、iOS、iPadOS、Android、Chromebookに対応

ポイント 3

マルチネットワークアクセス対応

SSL VPN、IPsecVPN、有線LAN、無線LAN、Webアプリケーションに対応

「端末認証」＝サイバートラスト デバイスID



偽造が困難な証明書をコピーできない状態で
許可された端末だけにインストールすることで厳格な端末認証を実現します

ご利用イメージ（個別配付①）メール通知可の場合

デバイスID管理画面

管理者

① 証明書発行リクエスト
（証明書記載情報、端末固有情報など）

③ 証明書発行通知メール送付

④ メール記載URLクリック
（端末固有情報を送信）

⑥ 許可された端末だけに証明書を登録

端末利用者

cybertrust
デバイスID認証局

② 証明書発行

⑤ 端末の確認
（端末固有情報を確認）

ご利用イメージ（個別配付②）メール通知不可の場合

デバイスID管理画面

管理者

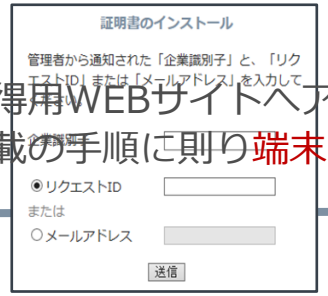
① 証明書発行リクエスト
（証明書記載情報、端末固有情報など）

デバイスID認証局

② 証明書発行

③ 証明書取得に必要な情報を通知

④ 証明書取得用WEBサイトへアクセス（次頁）
サイト記載の手順に則り端末固有情報を送信



⑤ 端末の確認
（端末固有情報を確認）

⑥ 許可された端末だけに証明書を登録

端末利用者

サイバートラスト デバイス ID 基本機能

認証対象	デバイス （PC、スマートフォン、タブレット、業務端末など）
申請情報	端末識別情報、通知先情報など
証明書記載情報	会社名、端末識別情報など
CAブランド	サイバートラスト
登録業務	お客様にて実施
配付方法	WindowsへのActiveX/ｴｰｼﾞｪﾝﾄによる自動インポート Mac OS Xへのｴｰｼﾞｪﾝﾄによる自動インポート PKCS#12の一括ダウンロード （キッティング） iPhone/iPadへのｲﾝｽﾄｰﾙ（OTA for iPhone & iPad） Android端末へのｲﾝｽﾄｰﾙ（OTA for Android） Chromebookへのｲﾝｽﾄｰﾙ（TPM for Chromebook）
最低ライセンス数	10ライセンス～　（10ライセンス単位）
鍵長	2048bit
有効期間	5年 （＋1ヶ月）
初期費用	なし
料金体系	サービス利用料/年 デバイス証明書ライセンス/年 その他必要に応じてオプション/年 ※ 全てオープンプライスとなります。
導入までの期間	お申し込み後、10営業日以内

サポートプラットフォーム

iPhone　iPad

ANDROID

Windows

macOS

Chromebook

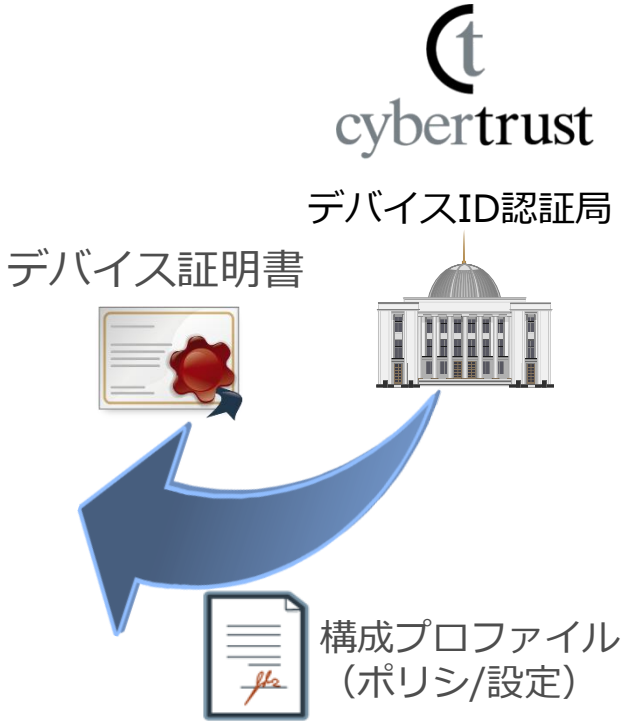
サイバートラスト デバイス ID 主な仕様および機能

	iOS/iPad OS	Android	Windows	macOS	Chromebook
証明書自動登録時の端末特定	○	○	○	○	○
端末特定に利用する端末固有情報	IMEI UDID	IMEI WiFi Mac	Macアドレス	Macアドレス	シリアル番号
証明書自動登録の手段	OS機能	専用アプリ	専用アプリ ActiveX	専用アプリ	専用アプリ
証明書格納場所	OS	OS/アプリ	OS	OS	OS（TPM）
オプション	OTA ライセンス	OTA ライセンス	ー	ー	TPM ライセンス
付加機能	構成プロ ファイル配布	VPN設定適用	ー	ー	ー

※1　証明書自動登録が可能なAndroidアプリケーション　SSLVPN： Cisco Anyconnect、F5 Edge Client、ブラウザ： JMAS KAITO
※2　Cisco AnyConnect、 F5 BIG-IP Edge Client 利用時にVPN接続設定の自動登録が可能

iPhone/iPad のポリシー設定の強制適用

- 証明書登録時に、セキュリティポリシやネットワーク接続設定を強制適用
  - ネットワークアクセスが許可された端末＝統一されたポリシ・設定
    - 自動化された仕組みにより、証明書と構成プロファイルを適用

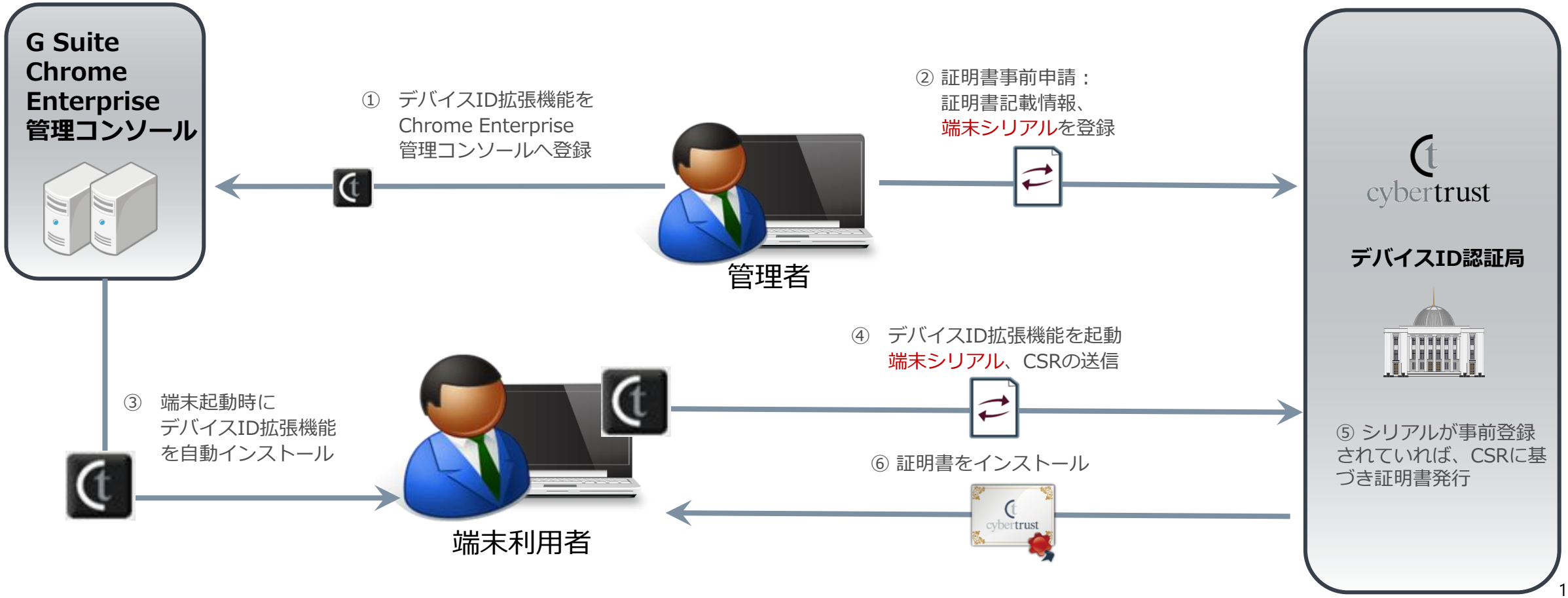


- 適用可能な構成プロファイル例

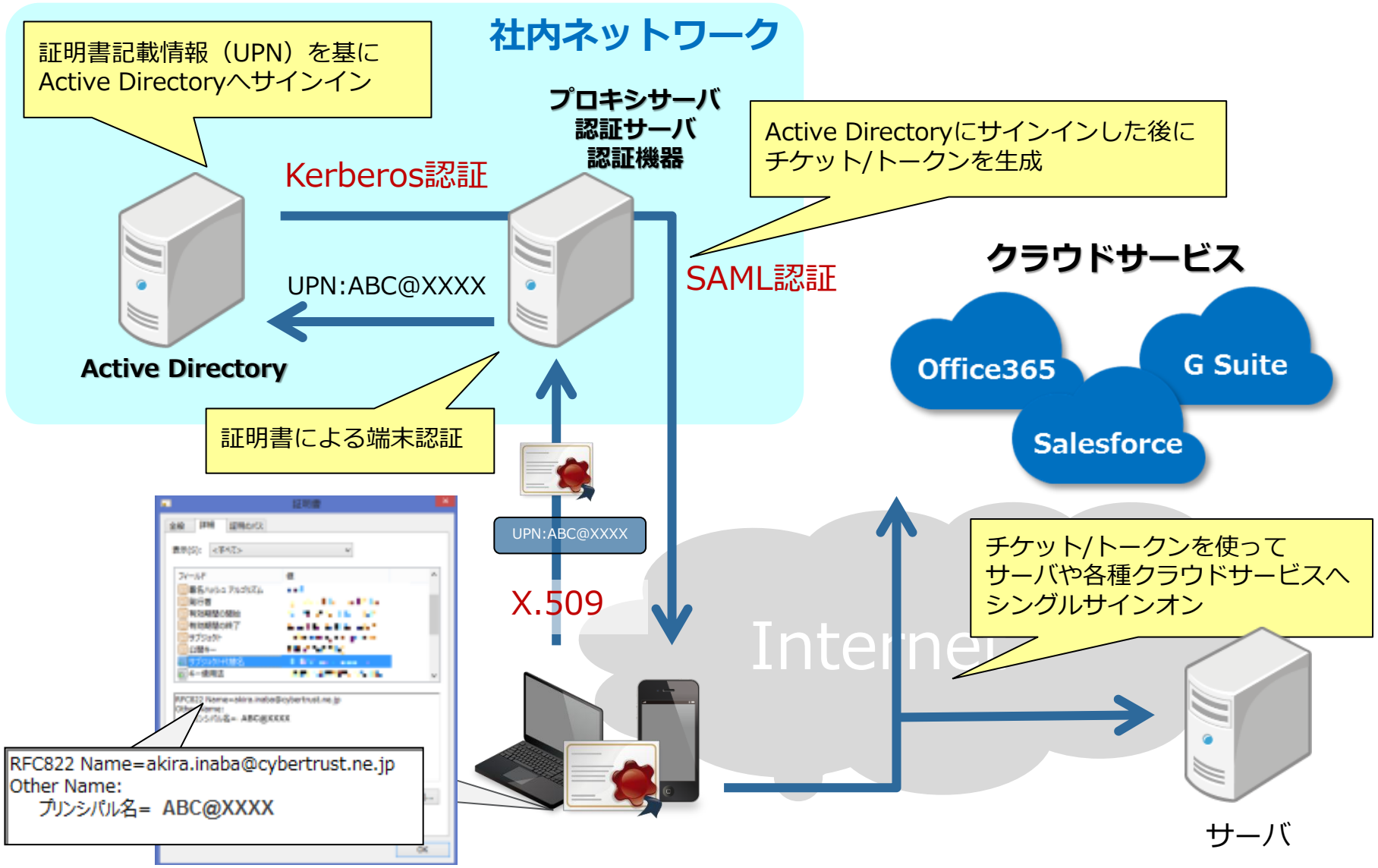
パスコードポリシ	パスコードの長さ
	文字種（数字、英字、記号）
	有効期間
機能制限	カメラ禁止
	YouTube禁止
	アプリインストール禁止
	Safariの制限
ネットワーク接続設定	VPN接続設定
	VPN自動接続先リスト
	無線LAN接続設定

Chromebook へのデバイス証明書のインストール

- デバイスID 専用拡張機能により、
  管理下の Chromebook の TPM にデバイス証明書をインストール



UPN による Active Directory 連携に対応



動作確認済み製品

- IPSec VPN
  - Cisco ASAシリーズ — iOS 3.0以降対応 / Android 2.2以降対応
  - Fortinet FortiGateシリーズ — iOS 3.0以降対応 / Android 2.2以降対応
- SSL VPN （SSLクライアント認証）
  - Cisco ASAシリーズ — iOS 4.0以降対応 / Android 4.0以降対応
  - Pulse Secure Connect Secure シリーズ — iOS 4.0以降対応 / Android 4.0以降対応
    ※旧Juniper SA/MAGシリーズ
  - F5 BIG-IPシリーズ — iOS 4.0以降対応 / Android 4.0以降対応
- 無線LAN （EAP-TLS）
  - Cisco Aironet/Wireless LAN Controllerシリーズ — iOS 3.0以降対応 / Android 2.2以降対応
  - Aruba AP/Aruba Multi-Service Controllerシリーズ — iOS 3.0以降対応 / Android 2.2以降対応
- Webサーバ （SSLクライアント認証）
  - Microsoft Internet Information Server — iOS 4.0以降対応 / Android 4.0以降対応
  - NGINX — iOS 4.0以降対応 / Android 4.0以降対応
  - Apache 2 — iOS 4.0以降対応 / Android 4.0以降対応

※ Android端末は、端末毎に仕様が異なるため動作に機種依存性があります。

ネットワーク機器等の認証設定

cybertrust

ネットワーク機器や
サーバへ認証設定を適用

デバイス証明書を
端末へ配布・登録

証明書の発行・失効で
アクセスコントロール

ネットワーク機器やサーバへ以下の認証設定を適用いただくことで、デバイスID認証局よりお客様向けに発行し、失効されていない証明書を登録している端末だけアクセスが許可される環境を実現します

- デバイスID認証局を信頼する認証局として登録（CA証明書の登録）
  - デバイスID認証局から発行された証明書はアクセス許可する設定
- 証明書に記載された会社名によるフィルタリング設定
  - お客様毎に割り振られた値が記載された証明書のみアクセスを許可する設定
- 証明書失効情報の参照設定（失効リスト：CRL、OCSP）
  - 失効された証明書はアクセス拒否する設定
- 必要に応じて証明書の記載情報を用いて細かな認証設定も可能
  - 例：OUに記載した部署名により無線LANでのVLANアクセス制限
- 通信暗号化のためサーバ証明書の登録

サイバートラストの優位性 ①

安心の第三者認証機関

- CPおよびCPSを公開し、厳格に運用
  - サイバートラスト デバイスIDは、第三者認証局として、証明書ポリシ（CP）、認証局運用規程（CPS）を公開し、厳格に運用しています
- 動きの早いスマートデバイスに確実に対応
  - サイバートラスト デバイスIDは、第三者認証局として、新しい iOSデバイスや Android搭載端末、iOSや Android などの OSバージョンアップ時にいち早く事前検証を行い、スマートデバイスの継続的な業務利用を実現しています

※ 個別に認証局を構築している場合、新機種や新OSが出る度に事前の動作確認　（相互接続性検証）を行うための負担が大きくなります

- スマートデバイスに関する豊富なナレッジ
  - サイバートラストは、第三者認証機関として、自らデバイス認証サービスを提供　することにより、スマートデバイスに関する豊富なナレッジを蓄積しています
  - スマートデバイス自体のナレッジのみならず、接続する各種ネットワーク機器、　ソフトウェア製品など、多数の導入実績から得た知見をもとに、お客様の実際の　利用シーンをサポートします

サイバートラストの優位性 ②

最高レベルのセキュリティ基準適合性

- ISO 27001（ISMS）
  - 情報セキュリティサービスを提供する企業として、全社で ISO27001（ISMS）認定を取得し、お客様に安心してサービスをご利用頂けるよう、内部管理体制を整備しています
- WebTrust for CA/EV、SAS70、VISA、Master、JCB
  - 1997年に国内初の商用認証センターとして設立され、国内で最長の運用実績を有しています
  - 当社の電子認証センターは、認証局運用に特化した設備と厳密なポリシーにより運営され、国内外のセキュリティ基準に基づいた第三者による監査を受け、いずれも高評価を得ています

  ※ 日本国内で WebTrust for CA、WebTrust EV Programの両検証に合格したのは、当社とセコムトラストシステムズ社の 2社のみです。
- FIPS 140 Level 4
  - 最も重要な認証局の秘密鍵は、米国の連邦情報処理規格 FIPS 140の中でも最高レベルの Level 4に適合した HSMによって安全に管理しています

  ※ FIPS 140 Level 4の HSMを採用している認証サービス事業者は当社のみです

サイバートラスト デバイス ID まとめ

- 厳格な端末の特定（許可された端末だけがアクセス）
- 幅広い端末のサポート
  - Windows、macOS、Chromebook
  - iOS、iPad OS、Android
- 幅広いネットワークアクセスで利用が可能
- 高い安全性と確認された相互接続性
- 低価格な年間利用ライセンスと短期間での導入

導入事例：大規模やBYODなど

ソフトバンク株式会社様

大規模

- 社内システムへの安全なリモートアクセス環境を整備
- iPhone / iPad/Androidなど 30,000台以上の端末認証と端末設定

KDDI株式会社様

マルチデバイス

- 在宅勤務環境のためのリモートアクセス環境を整備
- Android搭載端末にはじまり、iPhoneなど計 10,000台以上を導入

日本コムシス株式会社様

マルチキャリア

- 設備工事現場業務支援システムや社内システムへのリモートアクセス
- 複数キャリアの数十種類のスマートフォン計1,000台以上を導入

山九株式会社様

BYOD

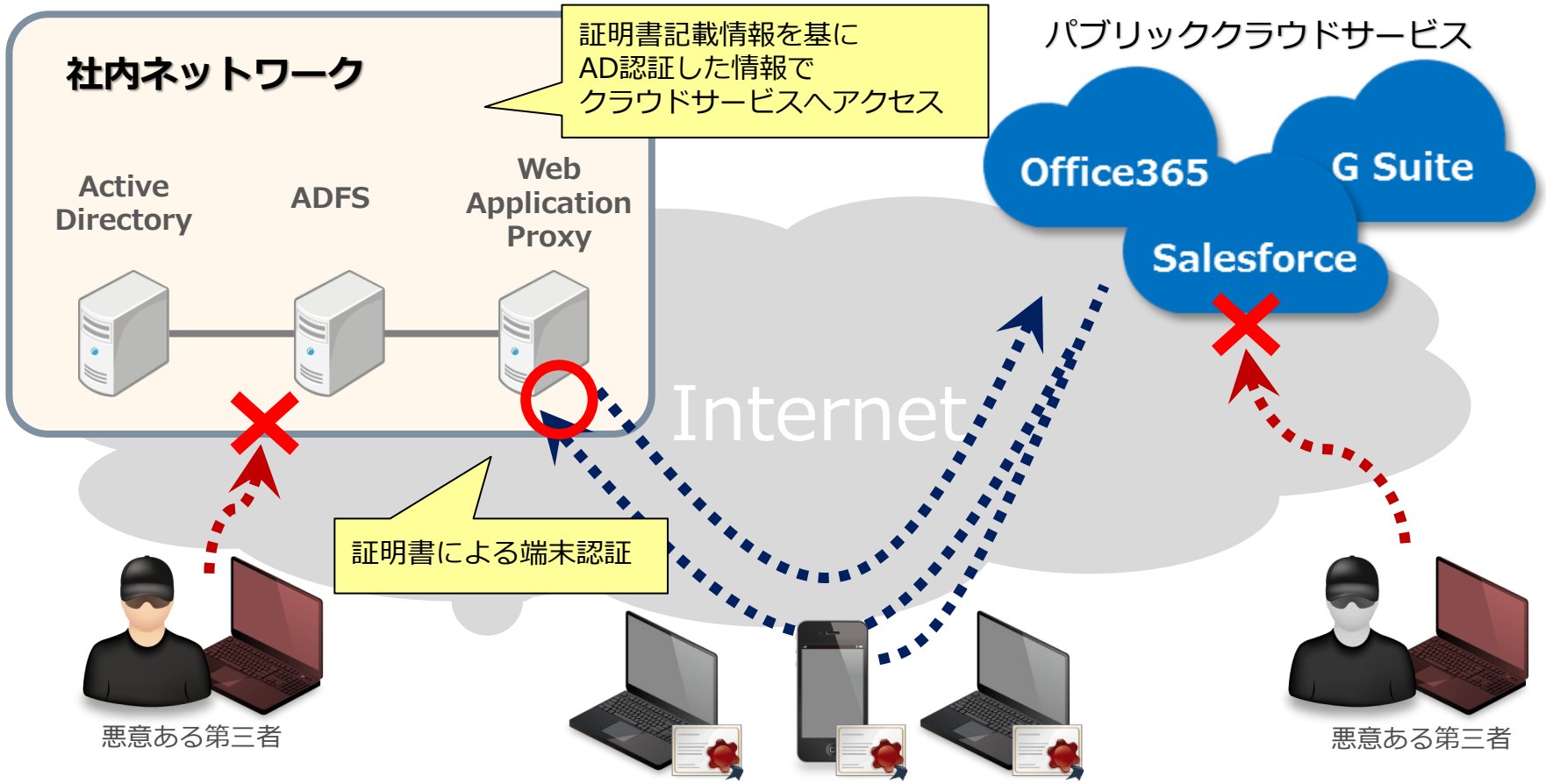
- 社内情報共有システムへの安全なリモートアクセス環境を整備
- BYODの導入における端末の特定で利用

その他、家電メーカー様、証券会社様、自動車会社様、人材派遣会社様、保険会社様、運送会社様、食品会社様、精密機器メーカー様など

活用事例

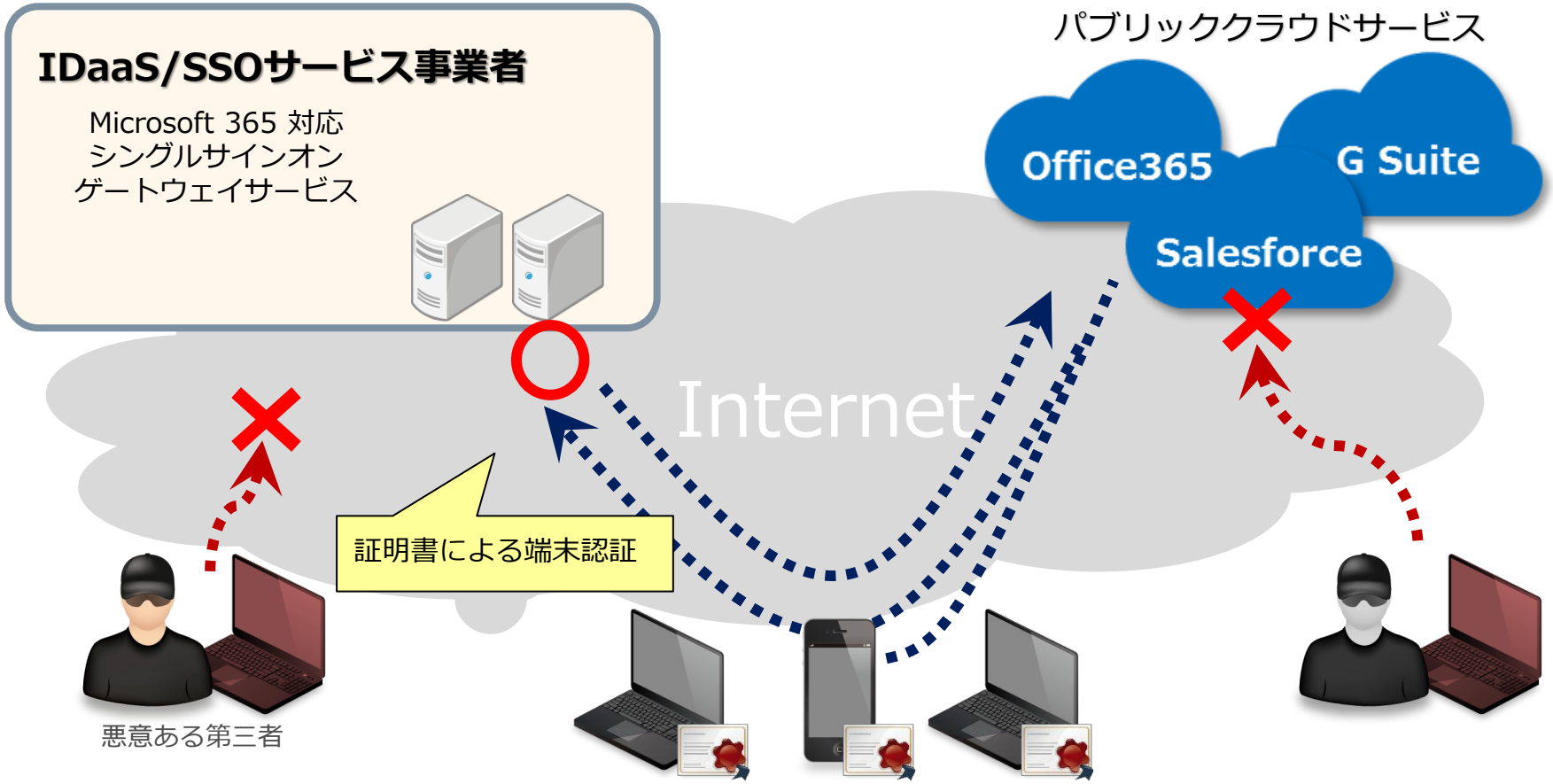
Microsoft 365 + Active Directory 連携

- 証明書によるデバイス認証で Microsoft 365 を利用する端末を制限
- 証明書記載情報を基に Active Directory とシームレスに連携
- Microsoft 365 以外のクラウドサービスへのシングルサインオンを実現



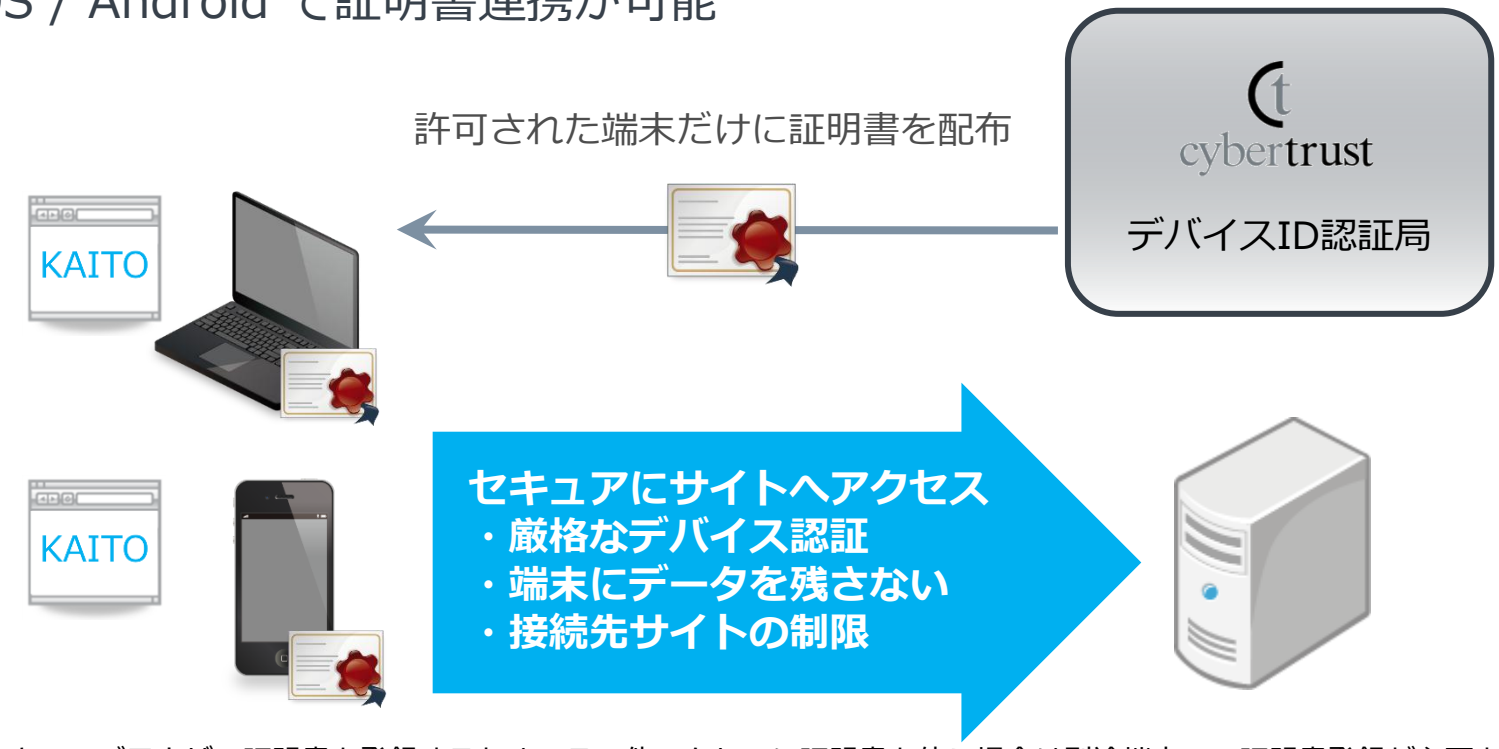
クラウドサービス + IDaaS サービス

- 様々なサービスにおいてID・パスワードを一元的に統合（IaaS/SSO）
- 証明書によるデバイス認証で Microsoft 365 を利用する端末を制限
- IDaaS/SSO サービス付加機能を活用（メールの情報漏えい対策・不正ログイン対策など）



セキュアブラウザ連携

- 対応セキュアブラウザ：KAITO セキュアブラウザ
  - 端末にデータを残さないことでデータが漏えいするリスクを飛躍的に低減
- KAITO セキュアブラウザで厳格なデバイス認証を実現
  - 証明書が登録された KAITO セキュアブラウザのみアクセス可能な環境を実現
  - Windows / iOS / Android で証明書連携が可能



※ KAITOセキュアブラウザへ証明書を登録するため、その他アクセスに証明書を使う場合は別途端末への証明書登録が必要となります。

Appendix

参考：証明書プロファイル

デバイス証明書プロファイル（端末側証明書）

CN	=	デバイス識別情報：証明書毎にユニークな情報	任意の文字列
OU	=	部署名、サービス名など任意な文字列	任意の文字列
OU	=	RA Operated by お客様会社名＋組織識別子	固定値
O	=	お客様会社名＋組織識別子	固定値
C	=	JP	固定値

CA 証明書プロファイル（機器/サーバ側ルート証明書）

CN	=	Cybertrust DeviceiD Public CA G(X)	固定値
O	=	Cybertrust Japan Co.,Ltd.	固定値
C	=	JP	固定値

※ (X)は認証局世代により変わります

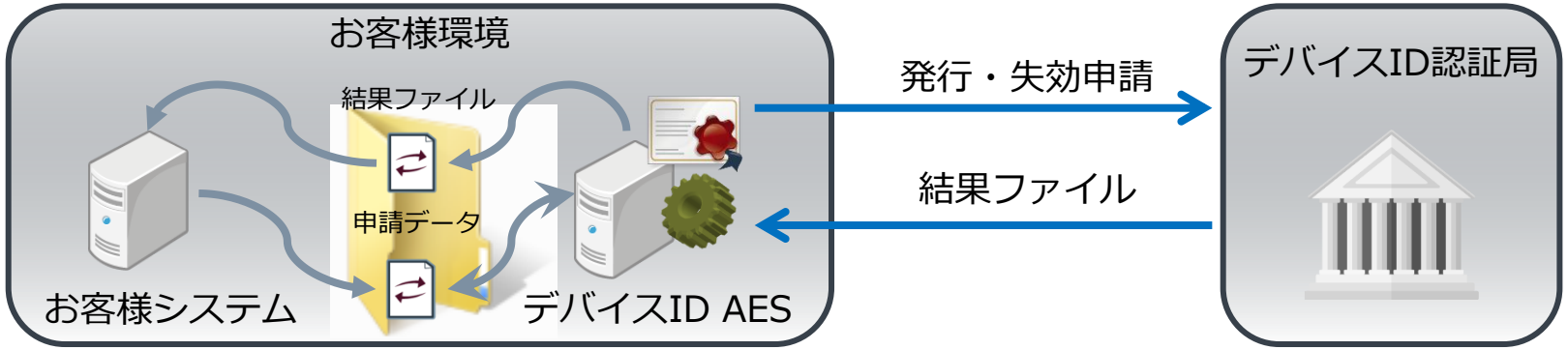
オペレータ証明書プロファイル（デバイスID管理画面アクセス用）

CN	=	＜オペレータ識別情報＞	固定値
O	=	＜お客様会社名＋組織識別子＞	固定値
C	=	JP	固定値

参考：証明書の発行・失効・管理を自動化

Auto Enrollment System（AES）：
お客様システムと連携し証明書の 発行・失効・管理 を自動化

- 各種一括申請データを認証局へ自動登録するためのオプションサービスです。
- 弊社指定フォーマットの各種申請データを監視フォルダに配置することで、AESが監視フォルダを定期的に確認し、デバイスIDサービスに対して自動で送信します。
- 申請の成否はログフォルダ内のログに出力されます。
- フォルダ監視間隔、送信失敗時の再転送回数などの設定が可能です。
- AES は Javaベースのソフトウェアでのご提供となります。



cybertrust

信頼とともに

留意事項

本資料に記載されている会社名、製品名、サービス名は、当社または各社、各団体の商標もしくは登録商標です。
その他本資料に記載されているイラスト・ロゴ・写真・動画・ソフトウェア等は、当社または第三者が有する知的財産権やその他の権利により守られております。
お客様は、当社が著作権を有するコンテンツについて、特に定めた場合を除き、複製、改変、頒布などをすることはできません。
本資料に記載されている情報は予告なしに変更されることがあります。また、時間の経過などにより記載内容が不正確となる場合がありますが、当社は、当該情報を更新する義務を負うものではありません。