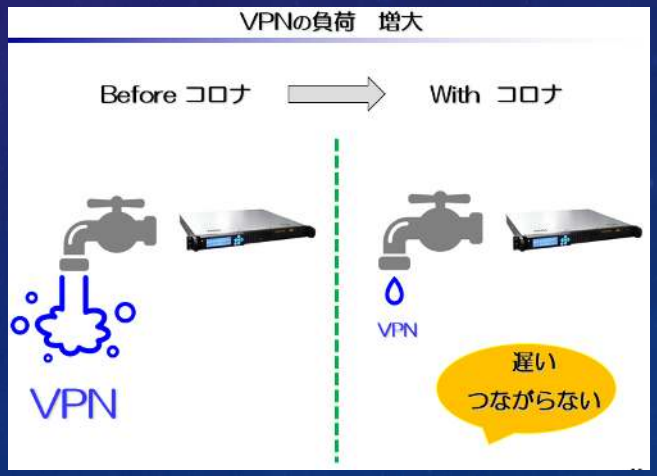
快適なテレワークをするためのネットワークとは

遅い、つながらないVPNで困っている場合の選択枝は！

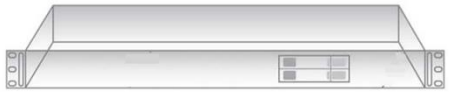
ゼロトラストって敷居が高いの？



2020年10月22日　　株式会社ムービット

会社概要

社名	株式会社ムービット
設立	1995年12月8日
所在地	東京都北区王子1－28－6
主な製品	Powered BLUE シリーズ アプライアンスサーバー（Linux） ソフトウエア開発



POWERED BLUE

ダークWeb

ダークWeb / データやアクセス権の売買

真相深層

■「ランサムウエア」月120ドルから

サイバー攻撃 闇市場拡大

サイバー攻撃ツールの闇市場が拡大している。身代金目的で端末内のデータを暗号化するランサムウエア、標的となる組織に不正アクセスできる権利などが売り出され、競争が新たな商品を生み出していく。技術がなくても「武器」の調達が可能になり、攻撃者の裾野拡大が懸念されている。

「最も安い検出不能ランサムウエア」。1カ月で120ドル、6カ月で490ドル、12カ月で900ドル——。

サブスク利用も

キヤノンマーケティングジャパンが確認したランサムウエアの販売サイトでは、サブスクリプション（定額課金）の利用プランが設けられ、最も高額なプランでは感染を容易にする追加機能も付くとされていた。

ランサムウエアは今年だけで既に3回バージョンアップされ、使い方は「よくある質問」に答える形で説明。検出を免れられるウイルス対策ソフトの一覧も載せていた。

同社の西浦真一セキュリティエバンジェリストは「セールスポイントや使い方を丁寧に説明する様は一般的なソフトウエアやアプリの販売サイトと変わらない」と話す。

匿名性の高い闇サイト群「ダークウェブ」では以前から、流出したクレジットカード情報やSNS（交流サイト）アカウントが流通しており、近年、取引の対象は一段と多様化している。

トレンドマイクロによると「日本の医療系大学のネットワークに侵入するアクセス権」は999ドル、ATMから銀行のネットワークに侵入するマルウエア（悪意のあるプログラム）は2千ドルで売り出されていた。偽サイトへの誘導などに使うショートメッセージサービス（SMS）の配信を5千件350ドルで請け負うとの書き込みもあった。

販売が確認されたサイバー攻撃用のサービスやツール	
医療系大学へのアクセス権	999ドル
米有力企業へのアクセス権	1万ドル
ATM用のマルウエア	2000ドル～
ランサムウエアのサービス	年間900ドル
スパムSMSの送信サービス	25～500ドル
SMS送信用のソフトウエア	499ドル～

(出所) トレンドマイクロ

売り手で競争、脅威増す

キヤノンマーケティングジャパンが確認したランサムウエアの販売サイト＝同社提供

セキュリティー関係者によると、国内38社などから漏洩した疑いが明らかになったVPN（仮想私設網）の利用情報は、有料の会員制サイト内でやり取りされていた。

サイバー攻撃をサポートするマルウエア販売や代行サービスは「CaaS（クライム・アズ・ア・サービス）」とも呼ばれる。CaaSを利用することで「高度な技術や専門知識がなくても攻撃を実行できるようになっている」と、トレンドマイクロの岡本勝之セキュリティエバンジェリストは警鐘を鳴らす。

売り手としては、自ら標的を探して攻撃を仕掛けなくても、得意分野の技術を生かして効率的に稼げるメリットがある。マルウエアを提供し、攻撃で得た収益の一定割合を成功報酬として受け取るケースもある。

機能の劣るマルウエアは市場で淘汰され、攻撃が成功しやすいほど価格は上がる。

ロシアのウイルス対策ソフト開発会社「ドクターウェブ」のボリス・シャロフ最高経営責任者（CEO）は「売り手が競い合うことでマルウエアなどの攻撃力が高まる構図になっている」と指摘する。ランサムウエアで暗号化されたデータの復旧サービスでも「数年前と比べ、データを復元できないケースが増えている」という。

歯止め難しく

マルウエアの販売は国内では不正指令電磁的記録提供の罪にあたる。ただ「不正なプログラムといえるかどうかは実際に使用されて初めて検証できる」と警察関係者は説明する。被害が発生した場合は攻撃の実行者の検挙が優先されるため「マルウエアの提供者を追及し、闇市場の取引に歯止めをかけるのは難しい」という。

海外ではおとり捜査で闇市場サイトを閉鎖に追い込んだ事例もあるが「日本では捜査権限が限られる」とセキュリティー会社スプラウトの高野聖玄社長は指摘する。「サイバー攻撃や闇市場に国境はない。国際的な捜査連携や捜査手法の見直しによって抑止力を高めていくことが必要だ」と話している。（柏木凌真）

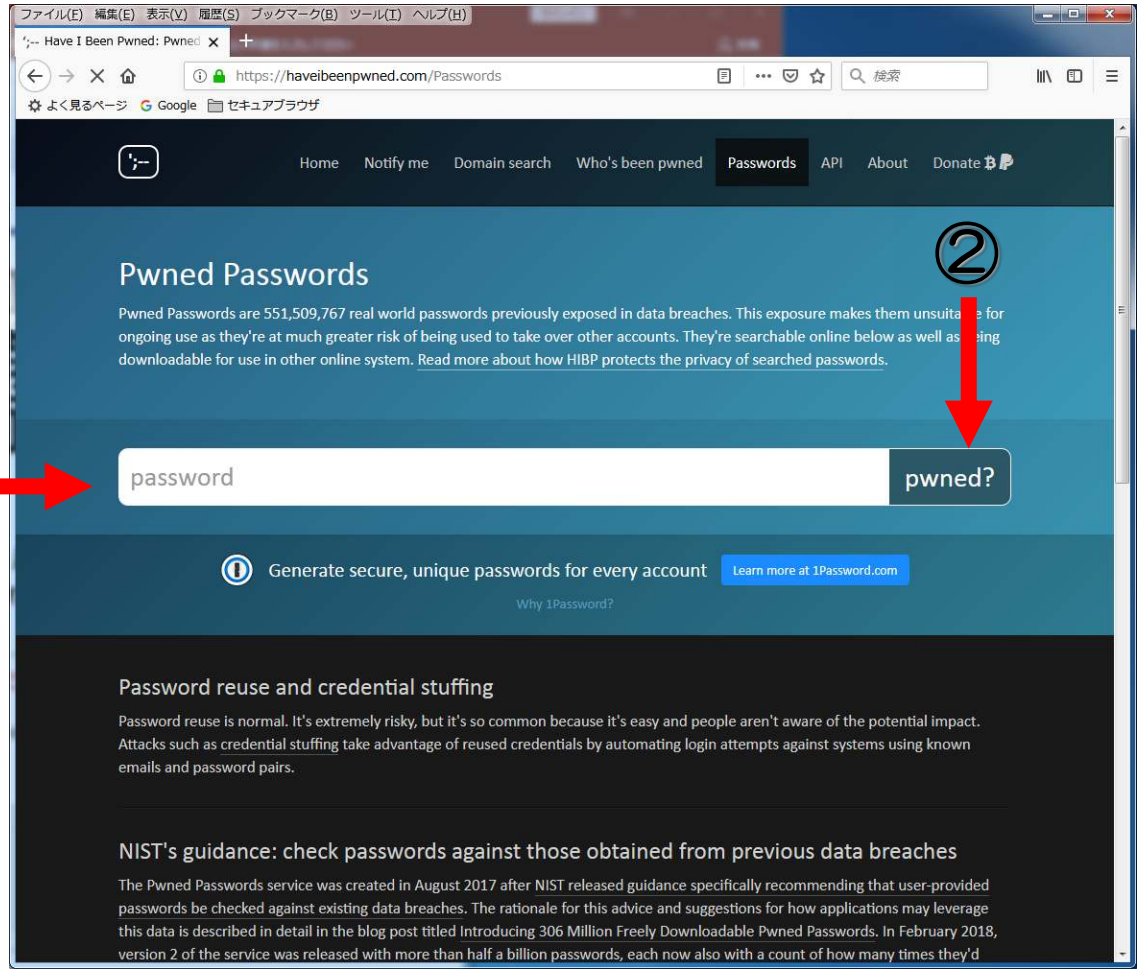
医科系大学へのアクセス権
　999ドル

米国有力企業へのアクセス権
　1万ドル

ランサムウエアのサービス
　900ドル

パスワード流出チェックサイト

https://haveibeenpwned.com/



①

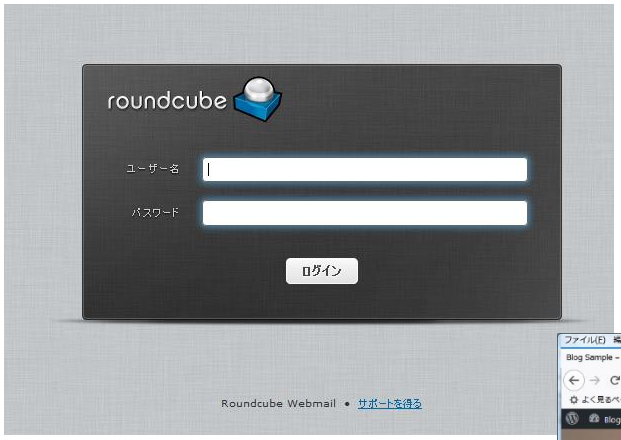
②

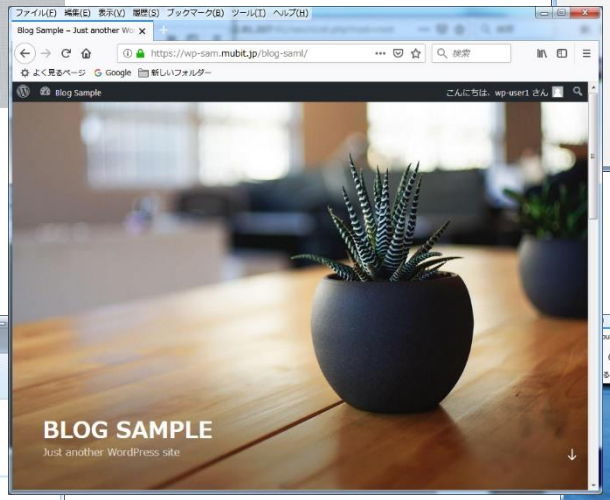
① パスワードを入力
② pwned？　を押す

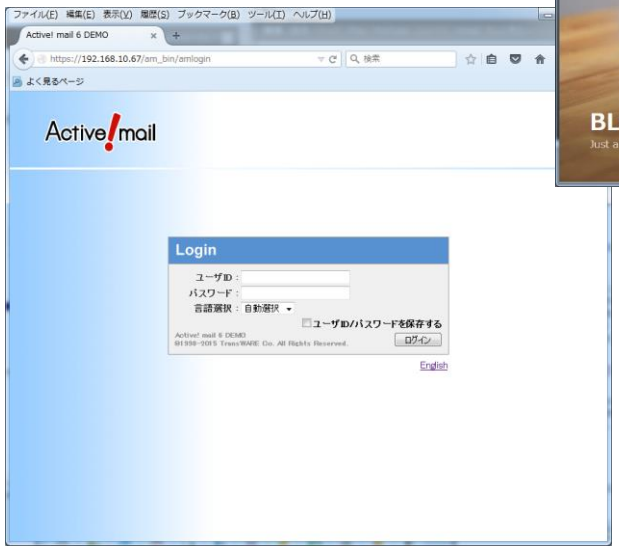
Oh no --- pwned !
残念でした

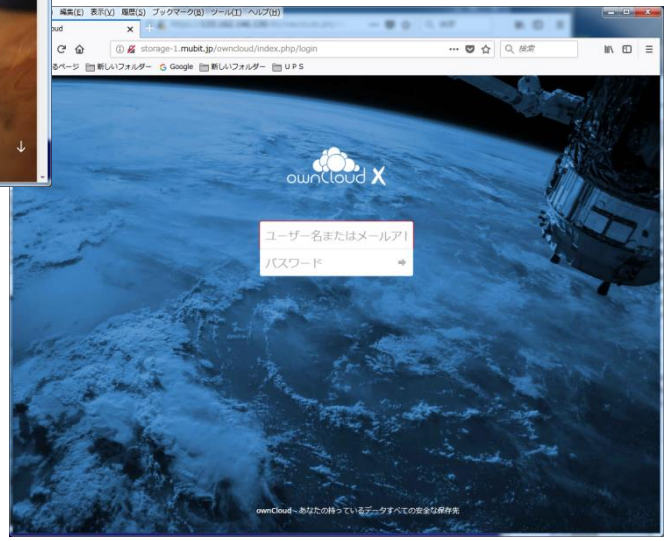
Good news — no pwnage found!
大丈夫

テレワーク　自社サーバー への アクセス









社内LAN側 への アクセス手法

項目	ターゲット	主な特徴
●VPN	network	VPNソフトが必要
●リバースプロキシ	Web	既存のWebへのアクセスに利用 複数の認証が適用できる
●ゼロトラスト	Web アプリ	idPとID認識型プロキシ型が必要

VPNの負荷　増大

Before コロナ　→　With コロナ

VPN

VPN

遅い
つながらない

VPNの特徴

- ソフト
  - クライアントソフトが必要
- アクセス
  - ネットワークへのアクセス
- セキュリティ
  - ネットワークへのログイン後のセキュリティは無し
- 負荷
  - 機器やネットワークの負荷が大きい

国内38社がVPNで不正接続被害

在宅時代の落とし穴

国内38社 VPNで不正接続被害

企業・個人、リスク備えを

新型コロナウイルスの流行でテレワークへの移行が進むなか、企業を取り巻く新たな落とし穴があらわになってきた。国内38社が不正アクセスを受け、遠隔勤務に欠かせないVPN（仮想私設網）の認証情報が流出した。ネットにつながる情報端末や国内外の拠点は、常にサイバー攻撃の危険にさらされている。在宅時代の情報リスクへの備えが不可欠だ。

日立化成や住友林業など38社から、VPNのパスワードやID情報が漏洩した。VPNは通信データを暗号化し、社外から業務システムに接続する際に使う。多くの企業が在宅勤務に取り入れるのは、情報セキュリティーに対する日本企業の「ワキの甘さ」だ。

情報インフラとなりつつあるが、今回はその死角を突かれた。

被害の背景に浮かんでいた。同社はこの機器について2019年4月に脆弱性を公表し、修正プログラムも公開。日本でも民間団体が注意喚起していたが、一部企業は修正を反映せず、VPN情報をとられる原因となった。

情報が流出した企業は、米専門企業パルスセキュアのVPN機器を使者が今回流出したパスワードなどを使えば、正規の社員を装って社内の基幹システムに入り込むことも可能になる。実際、今回被害にあった平田機工は、社員24人のIDとパスワードが、ネット上で2週間にわたってダウンロードできるようになっていた。さらに、流出したアカウントを使った不正ログインの試みも31回確認されたという。

VPNはいわば防御壁だ。しかし悪意ある第三

安全性が高いとされたVPNへの外部侵入は、ネットの防衛システムが盤石ではないことを浮き彫りにした。とはいえ在宅勤務の流れは変わらない。企業は今後、日常的なリスク管理の一環としてあらゆるサイバー攻撃の可能性に備える必要がある。

例えばアカウント流出が問題になったビデオ会議サービス大手の米ズーム・ビデオ・コミュニケーションズ。利用者のパスワードの使い回しやソフトを更新していないことなどが意図しない画像を送りつけられるなどの「ズーム爆撃」の遠因になった。

セキュリティー会社のS&J（東京・港）の三輪信雄社長は「これまでは企業の拠点に専門家を呼んで応急処置などの対処ができたが、在宅勤務中の従業員の端末が被害に遭った場合は対処が難しい」と話す。

対策として注目されているのが「ゼロトラスト」（信用しない）ネットワークと呼ばれるサイバー防衛の発想だ。誰でも社内ネットワークに遠隔で入れる半面、どの情報にアクセスできるかを細かく分けて設定。パスワードだけでなく指紋や顔認証といった多要素認証を様々なアクセス制御で組み合わせるものだ。

侵入そのものを入り口から防ぐ従来の仕組みと異なり、不正アクセスがあっても内部で様々な認証の壁に阻まれ、個人情報全体などを盗むことが難しいとされる。米グーグルが今春に提供を開始したことで新たなリスク管理の仕組みとして広く知られるようになった。

在宅勤務にはリスクがたくさん

VPN攻撃の被害を受けたとされる企業・団体

日立化成	8月に一部パスワードが流出
住友林業	暗証番号が流出
自動車総連	VPN機器の入れ替え実施
平田機工（半導体生産設備）	社員のIDとアカウントが流出。不正アクセスの痕跡も
ダイヘン（変圧器、産業用ロボ）	修正プログラムで対応
日本アンテナ（テレビ向けアンテナ製造）	全従業員のパスワードを変更。修正プログラムで対応

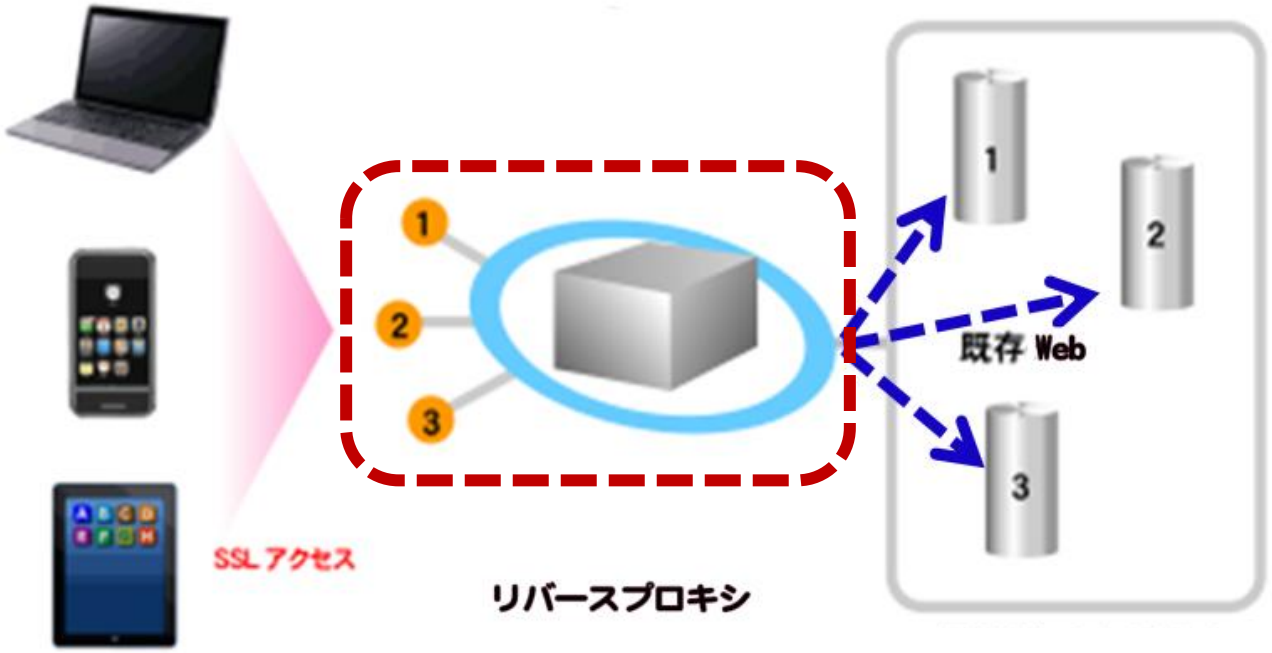
（注）日経が入手したリストと調査に基づく

VPNのパスワードやIDの漏洩
&
ダークWebで公開

日立化成
住友林業
自動車総連
ダイヘン
日本アンテナ
…

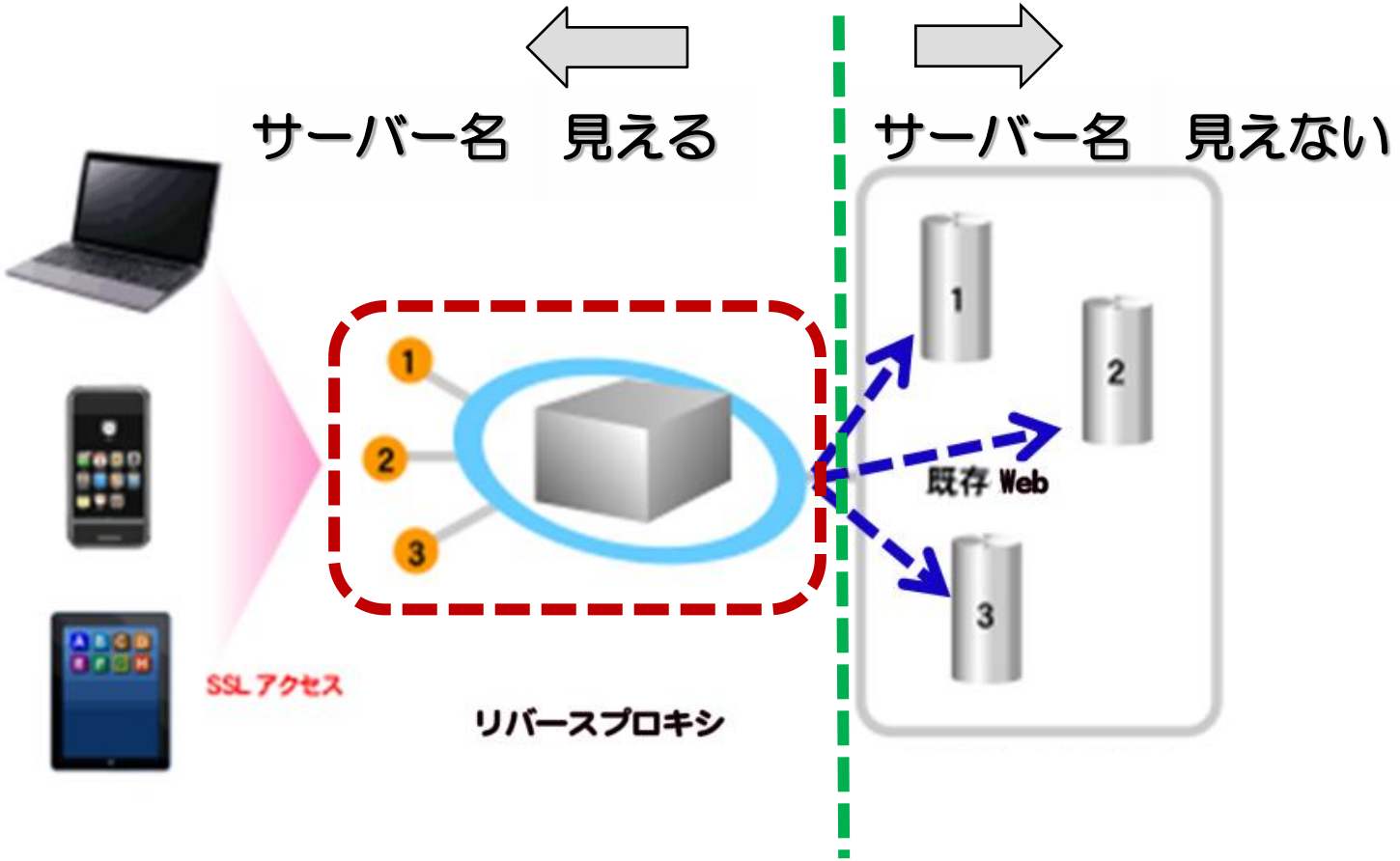
2020/8/26 日本経済新聞

リバースプロキシ



リバースプロキシ経由で既存のWebへアクセス

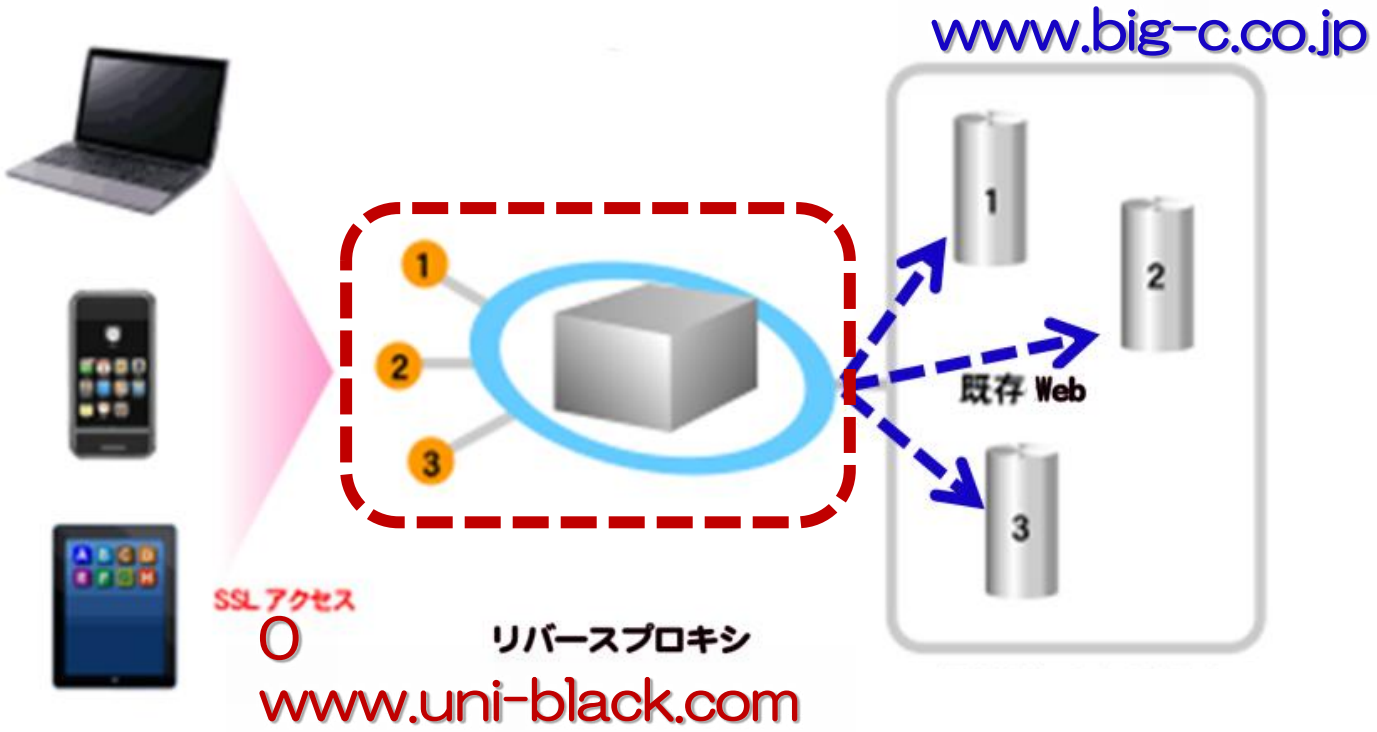
リダイレクト先Web の 隠蔽



リバースプロキシ先を隠蔽

ビックロ

リバースプロキシ例　びっくろ

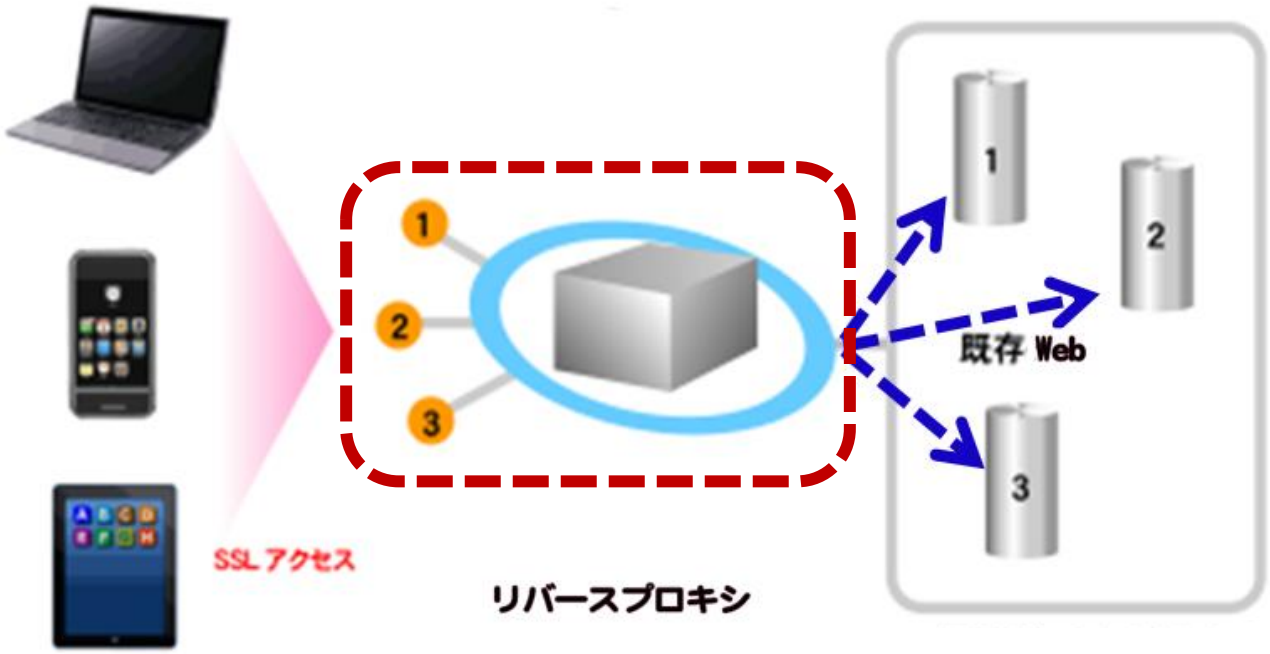


0　リバースプロキシ　　http://www.uni-black.com/

1　リバースプロキシ先　　http://www.big-c.co.jp/pc

ブラウザへのURL表示　　http://www.uni-black.com/pc

認証＆リバースプロキシ



0　リバースプロキシ

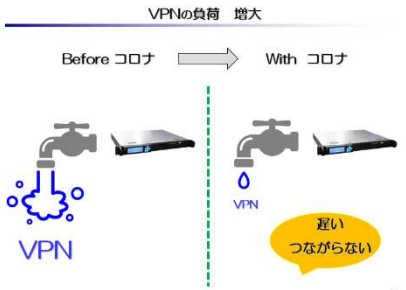
1　認証

AD認証 / OTP認証 /　SSLクライアント認証
ゼロトラスト対応 SAML認証

VPNとリバースプロキシの比較

VPN

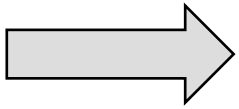
- ネットワーク内にすべてアクセス可能
- ログイン後のセキュリティは無し
- 利用時に際して機器や回線に大きな負荷
- 専用ソフト

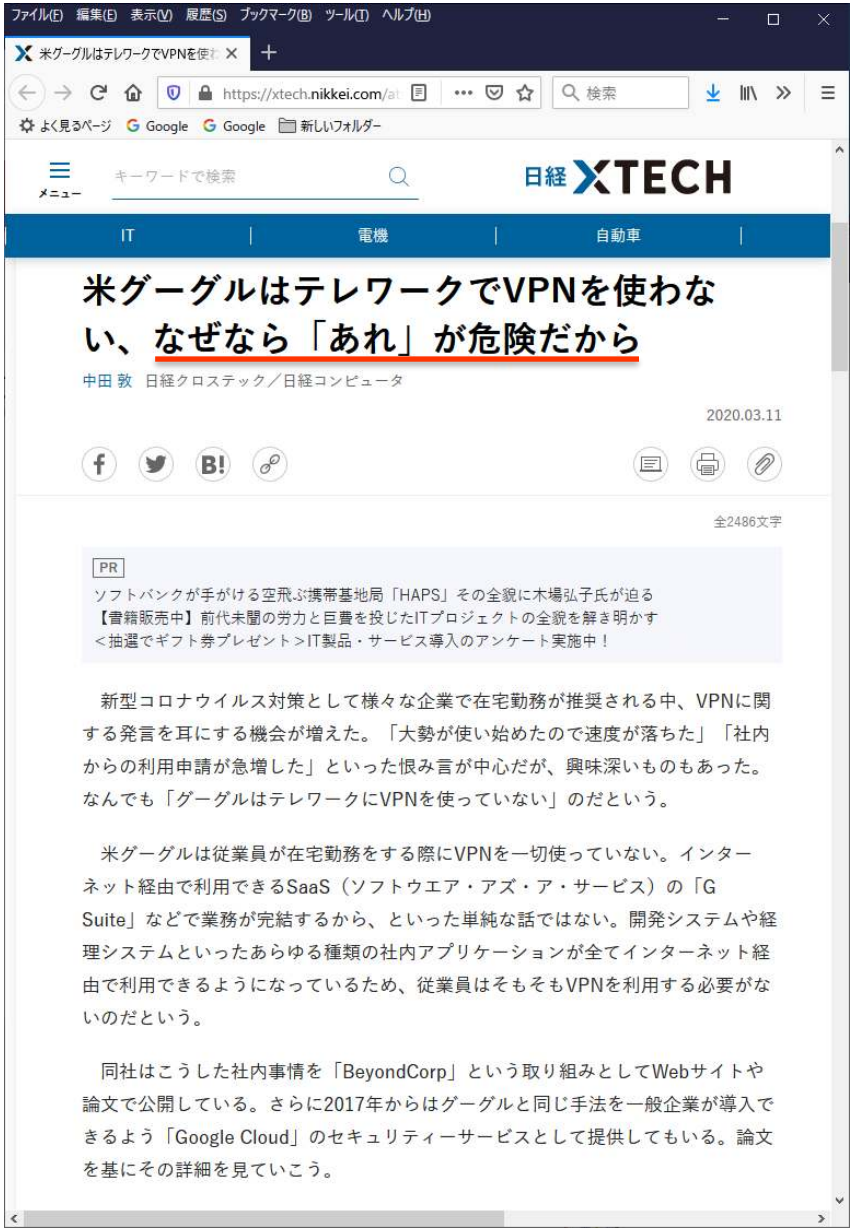


リバースプロキシ

- ターゲットサーバー個別へのアクセス
- ターゲットサーバーへの認証設定が可能
- Webなので利用時の負荷は小さい
- ブラウザのみで利用

Google は VPN を 使わない





ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

米グーグルはテレワークでVPNを使わ

https://xtech.nikkei.com/at

よく見るページ Google Google 新しいフォルダー

メニュー キーワードで検索 日経 XTECH

IT | 電機 | 自動車

米グーグルはテレワークでVPNを使わない、なぜなら「あれ」が危険だから

中田 敦 日経クロステック／日経コンピュータ

2020.03.11

全2486文字

PR

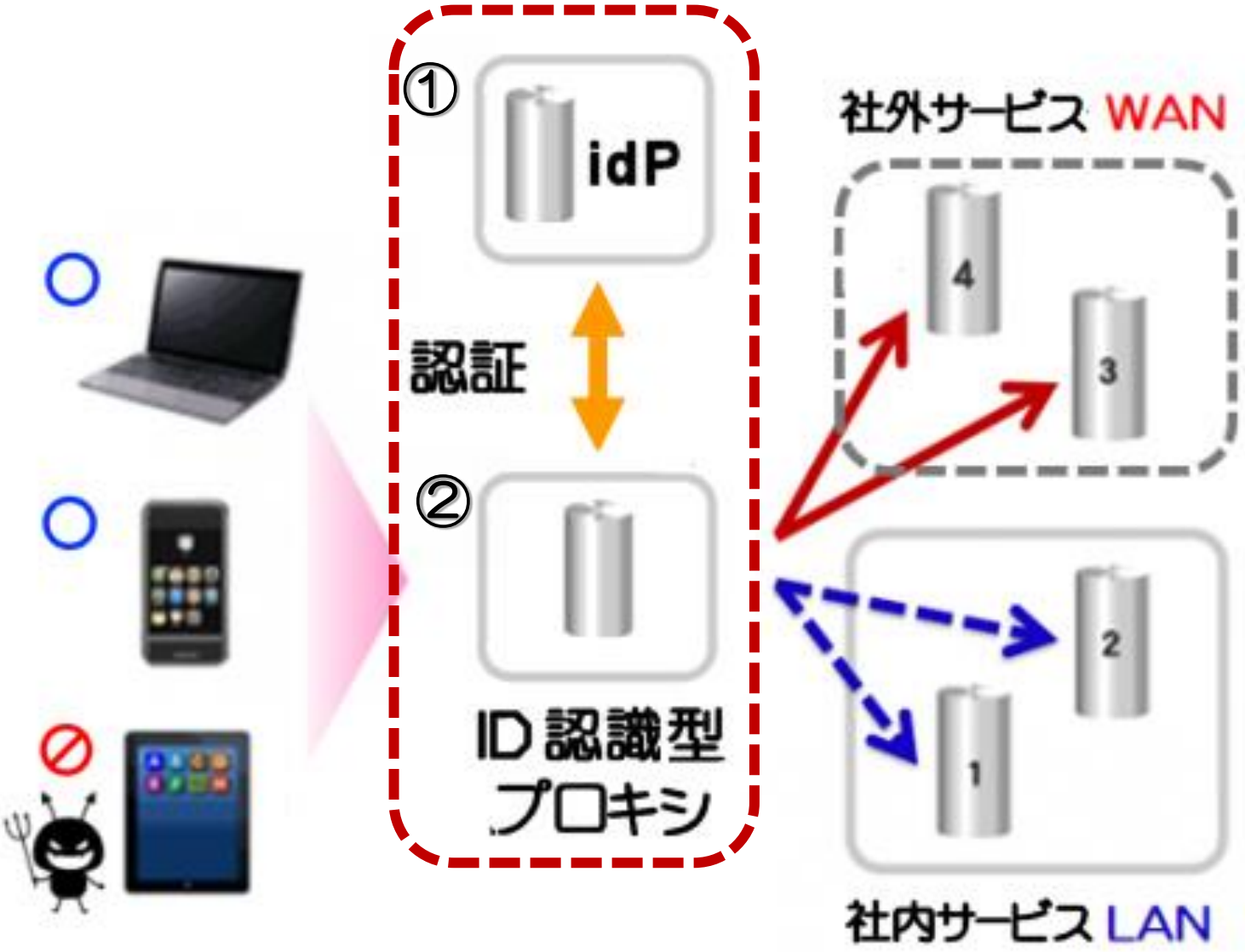
ソフトバンクが手がける空飛ぶ携帯基地局「HAPS」その全貌に木場弘子氏が迫る
【書籍販売中】前代未聞の労力と巨費を投じたITプロジェクトの全貌を解き明かす
＜抽選でギフト券プレゼント＞IT製品・サービス導入のアンケート実施中！

新型コロナウイルス対策として様々な企業で在宅勤務が推奨される中、VPNに関する発言を耳にする機会が増えた。「大勢が使い始めたので速度が落ちた」「社内からの利用申請が急増した」といった恨み言が中心だが、興味深いものもあった。なんでも「グーグルはテレワークにVPNを使っていない」のだという。

米グーグルは従業員が在宅勤務をする際にVPNを一切使っていない。インターネット経由で利用できるSaaS（ソフトウエア・アズ・ア・サービス）の「G Suite」などで業務が完結するから、といった単純な話ではない。開発システムや経理システムといったあらゆる種類の社内アプリケーションが全てインターネット経由で利用できるようになっているため、従業員はそもそもVPNを利用する必要がないのだという。

同社はこうした社内事情を「BeyondCorp」という取り組みとしてWebサイトや論文で公開している。さらに2017年からはグーグルと同じ手法を一般企業が導入できるよう「Google Cloud」のセキュリティーサービスとして提供してもいる。論文を基にその詳細を見ていこう。

ゼロトラスト　① idP　と　② ID認識型プロキシ



idP / IDaaS など

Azure
Active Directory

TrustLogin
by GMO

G Suite

CloudGateUNO
クラウドゲートウノ

onelogin

okta

iDaaS = iD As A Service

ゼロトラスト　② ID認識型プロキシ は 2タイプ

透過プロキシ型

リバースプロキシ型

ゼロトラスト　ID認識型プロキシ＝透過プロキシ型 での 構成

透過プロキシ型

① idP（idPは指定が多い）
② ID認識型プロキシ（透過プロキシ）
③ プロキシコネクタが必要（LAN側）
④ エージェントが必要（動作するサーバーに制限）
対応のサービス　Web / 他

ゼロトラスト　ID認識型プロキシ＝透過プロキシ型 SaaS 構成

透過プロキシ型

SaaS

① idP　（idPは指定）　④

② ID認識型プロキシ　（透過プロキシ）

自社

③ プロキシコネクタが必要　（LAN側）

④ エージェントが必要　（動作するサーバーに制限）

対応のサービス　Web / 他

ゼロトラスト　ID認識型プロキシ＝リバースプロキシ型での構成

リバースプロキシ型

① idP
② ID認識型プロキシ
エージェント不要
対応のサービス

（idpはどこのサービスでも利用可能）
(リバースプロキシ)
ターゲットサーバーのOS制限なし
Web のみ

ゼロトラスト　透過型とリバースプロキシ型の比較

透過プロキシ型

- Web以外のサービスにも対応（提供の会社による）
- エージェントが必要 / OSやアプリによっては未対応
- idPを選択できないケースもある
- 導入の敷居が高い

リバースプロキシ型

- ターゲットはWebのみ
- エージェント不要 / ターゲットのOSを選ばない
- idPは任意に選択できる
- 導入の敷居が低い

既存の社内Webへのアクセス

SSL アクセス

Webサーバー

Web認証が弱い

認証がない

Web側の変更したくない

認証対応　「Powered BLUE」 アプライアンス

① Web / Mail / DNS 機能 / マルチドメイン対応 / GUI

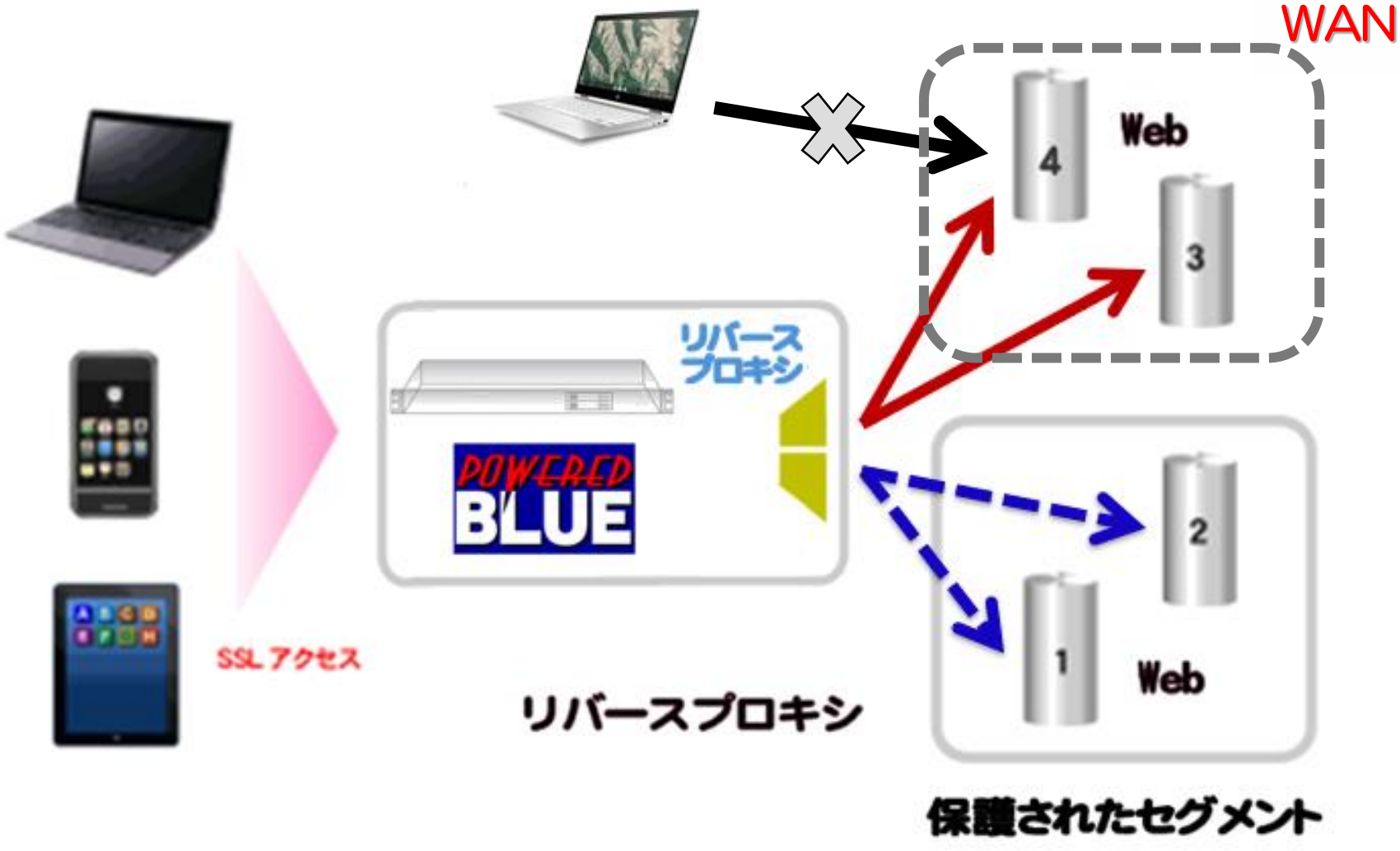
② AD認証 / OTP認証 / SSLクライアント認証
ゼロトラスト対応 SAML認証

③ リバースプロキシ　ID認識型リバースプロキシ

認証対応リバースプロキシ
①+②+③

POWERED BLUE　リバースプロキシ

リバースプロキシ経由のアクセスのみを許可



WAN側へ設置のWebサーバーでもセキュリティを確保

ドコモ 口座　事案

（第3種郵便物認可）　2020年(令和2年)9月10日（木曜日）

ドコモ口座

キャッシュレス普及 冷や水

地銀も本人確認不十分

NTTドコモの電子決済サービス「ドコモ口座」で、銀行口座から預金を不正に引き出される被害が相次いでいる問題を巡り、ドコモは新規登録を停止する事態に陥った。国がキャッシュレス決済の普及を図る中で、セキュリティーに不安を抱かせ、冷や水を浴びせかねない問題が再び発生した。〈本文記事社会面〉

菅官房長官は9日の記者会見で、「金融庁からドコモや金融機関に対し、被害に遭われた利用者への対応に万全を期すとともに、不正引き出しを防止するために必要な措置を取るよう指示している」と述べた。

今回の問題は、ドコモのセキュリティーの不備が原因の一つとなった。ドコモ口座は、銀行口座を登録して入金し、買い物や送金ができるサービスで、ドコモの携帯電話を使っていなくても利用できる。ただ、開設に必要なドコモの会員IDは、氏名やメールアドレスを登録すれば誰でも取得でき、運転免許証などの本人確認は不要で、他人になりすましての口座開設も可能だ。他のキャッシュレス決済は、携帯電話のSMS（ショートメッセージサービス）を使った「2段階認証」などを設定しており、ドコモも同様の対策を導入する方針だ。

銀行側も本人確認などが不十分だった可能性がある。被害にあった地銀は、地銀ネットワークサービスが提供する「Web口振受付サービス」を使ってドコモ口座と連携していた。連携に必要な情報は各行で異なるが、第三者が名前、口座番号、暗証番号などを不正に取得すれば、本人確認なしで登録できる仕組みだった。ある地銀の関係者は「本人確認が甘い地銀で被害が出てしまった。使いやすさも大事なので、どこまで安全対策を強化すればいいのか悩ましい」と話した。

一方、ドコモ口座と連携しているメガバンクでは被害が確認されていない。本人しか取得できない一時的なパスワードを発行したりして、本人だけが知っている口座の情報を求めるなど強固なセキュリティー対策を敷いているところが被害防止につながったとみられる。キャッシュレス決済を巡ってはセブン&アイ・ホールディングスの「セブンペイ」や、ソフトバンクグループの「ペイペイ」で、本人確認の不備などを突いた不正が発生した経緯がある。

サイバーセキュリティーに詳しい森井昌克・神戸大教授（情報通信工学）は「認証が甘いところは世界中から狙われる時代にお粗末。利便性を損ねてでも、安全性を担保する仕組みが必要だ」と指摘する。

ドコモ口座を巡る不正利用の構図

地方銀行などに預けられていたお金が、
ＮＴＴドコモの電子決済サービス
「ドコモ口座」
を使って不正に引き出されていた

メガバンク

一時的なパスワードを発行などで対応

2020/9/10 読売新聞

認証　その1　ワンタイムパスワード認証

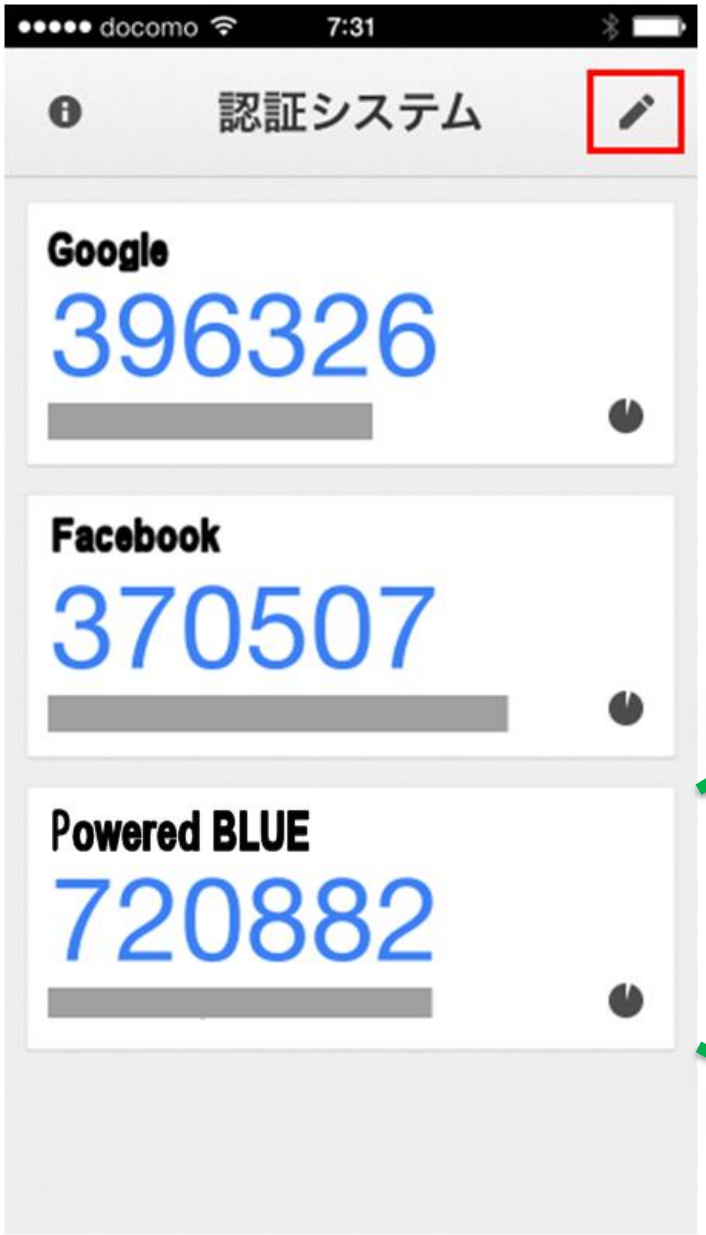
ソフトウエアトークン

OSS や 無償 の ソフトウエアトークン

製品	ロゴ	iOS Android	PC	言語	備考
Google Authenticator		○		英語	オープンソース
IIJSmartKey		○		日本語	無償
Authy		○	○ Windows Mac Linux	英語	無償
WinAuth			○ Windows	英語	無償

QRコードを写メ　サイトの簡単登録

GOOGLE AUTHENTICATOR



Powered BLUE サイト

ユーザーのQRコード

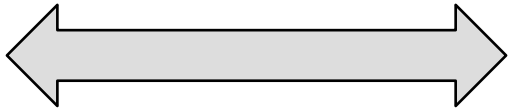
ワンタイムパスワード認証 + リバースプロキシ

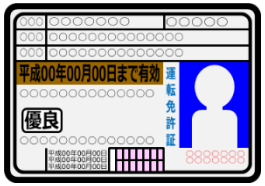
ワンタイムパスワード認証

ワンタイムパスワード　＋　任意パスワード　に対応

認証　その2　SSLクライアント認証　　相互に確認

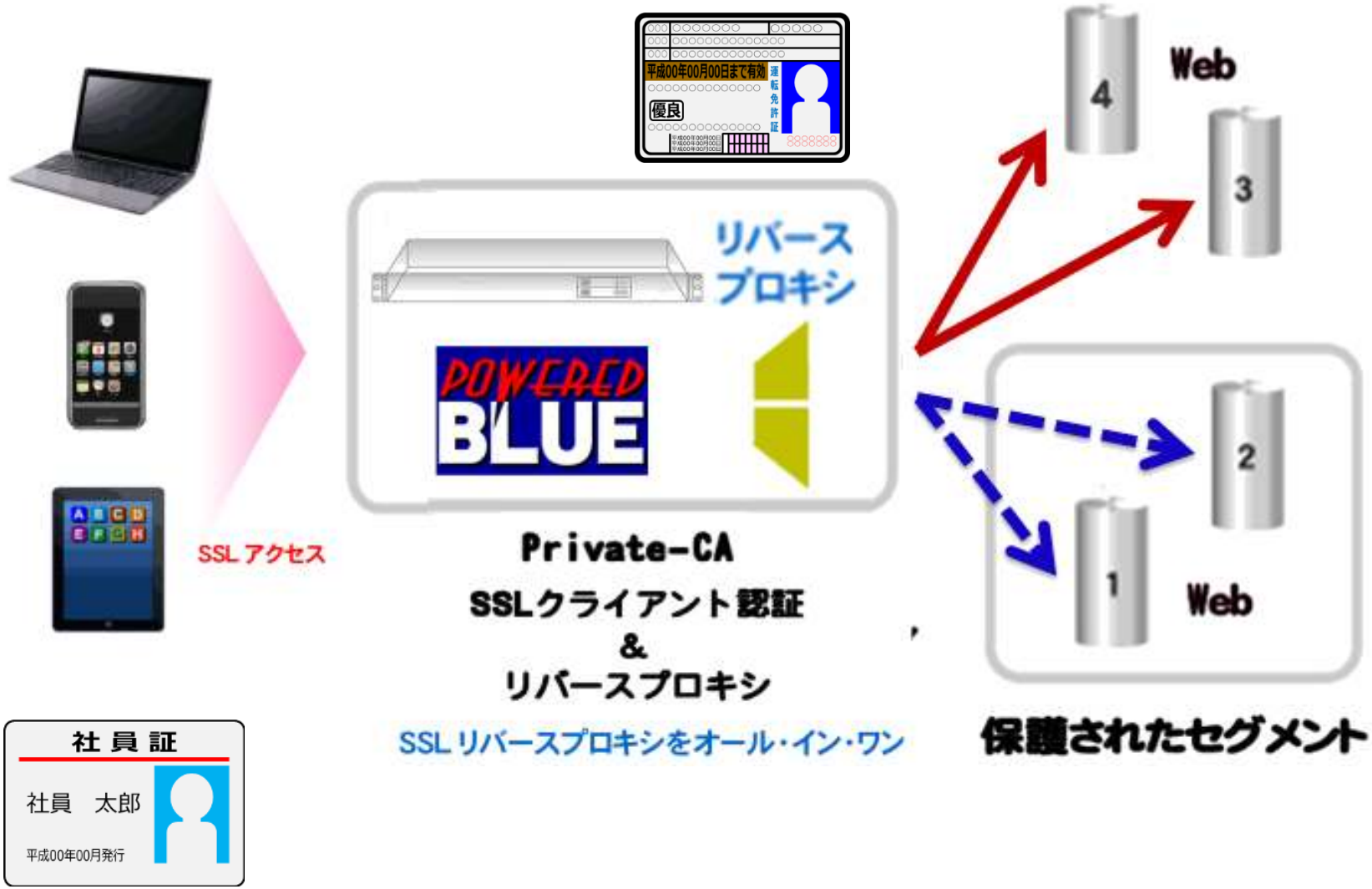
■ SSLクライアント証明書





■ SSLサーバー証明書

SSLクライアント認証 + リバースプロキシ

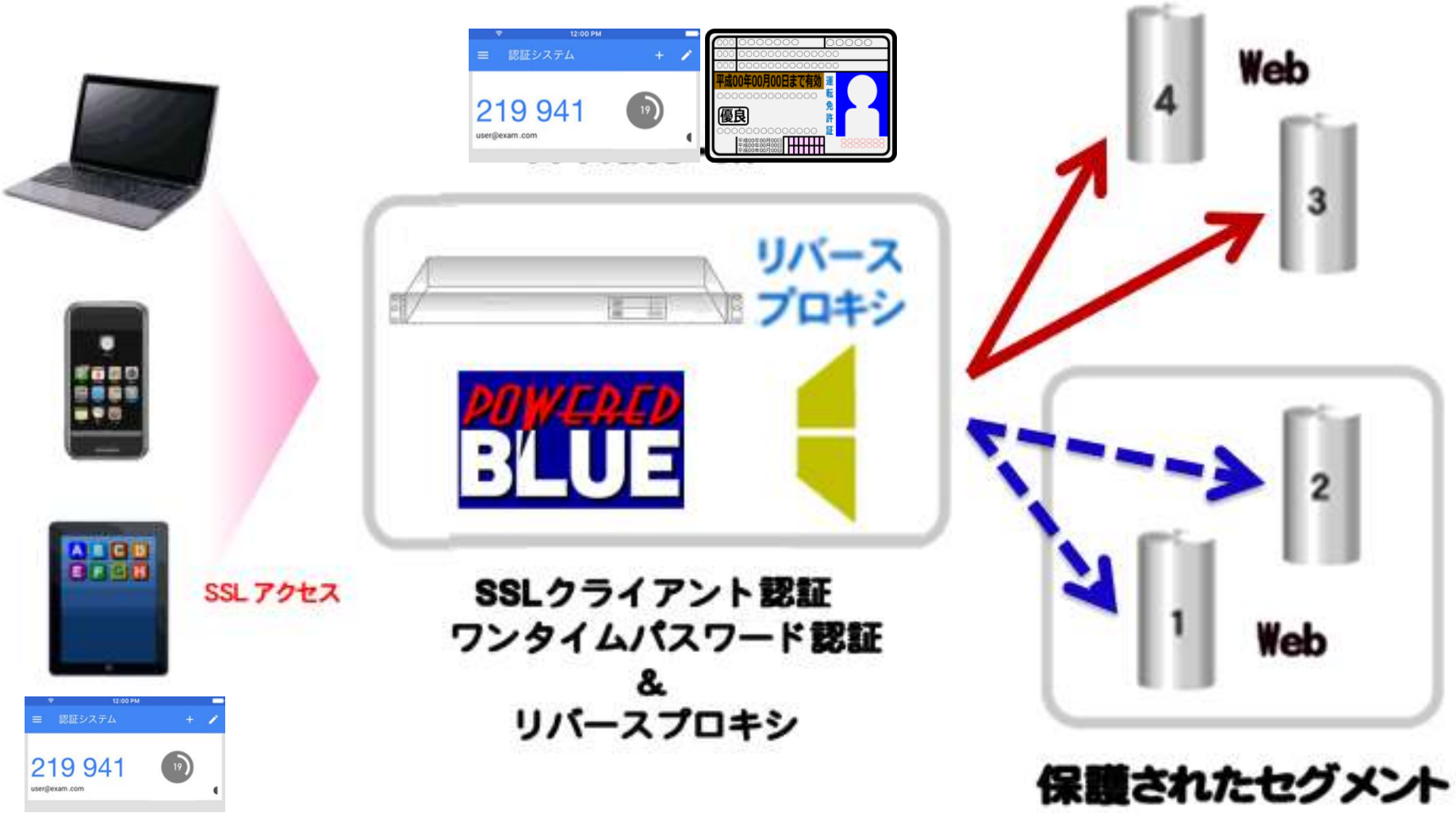


SSLクライアント認証例　スマートフォン

証明書　有効

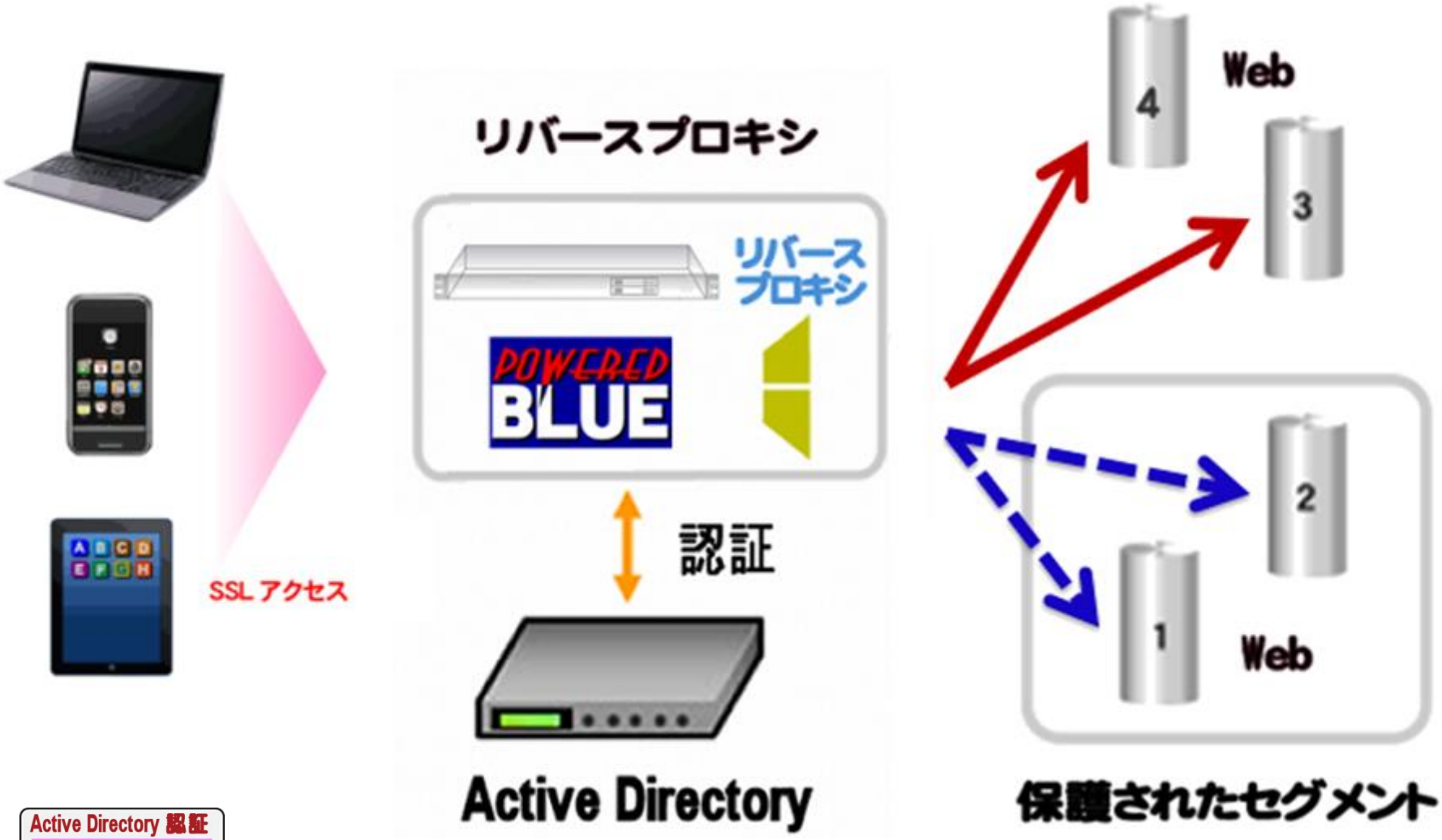
証明書　なし・失効

ワンタイムパスワード + SSLクライアント認証



ワンタイムパスワード認証 + SSLクライアント認証

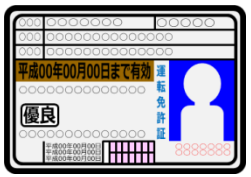
認証　その3　AD認証


リバースプロキシ
リバースプロキシ
POWERED BLUE
認証
SSL アクセス
Active Directory
4
Web
3
2
1
Web
保護されたセグメント
Active Directory 認証
社員　太郎
00年00月発行

AD認証

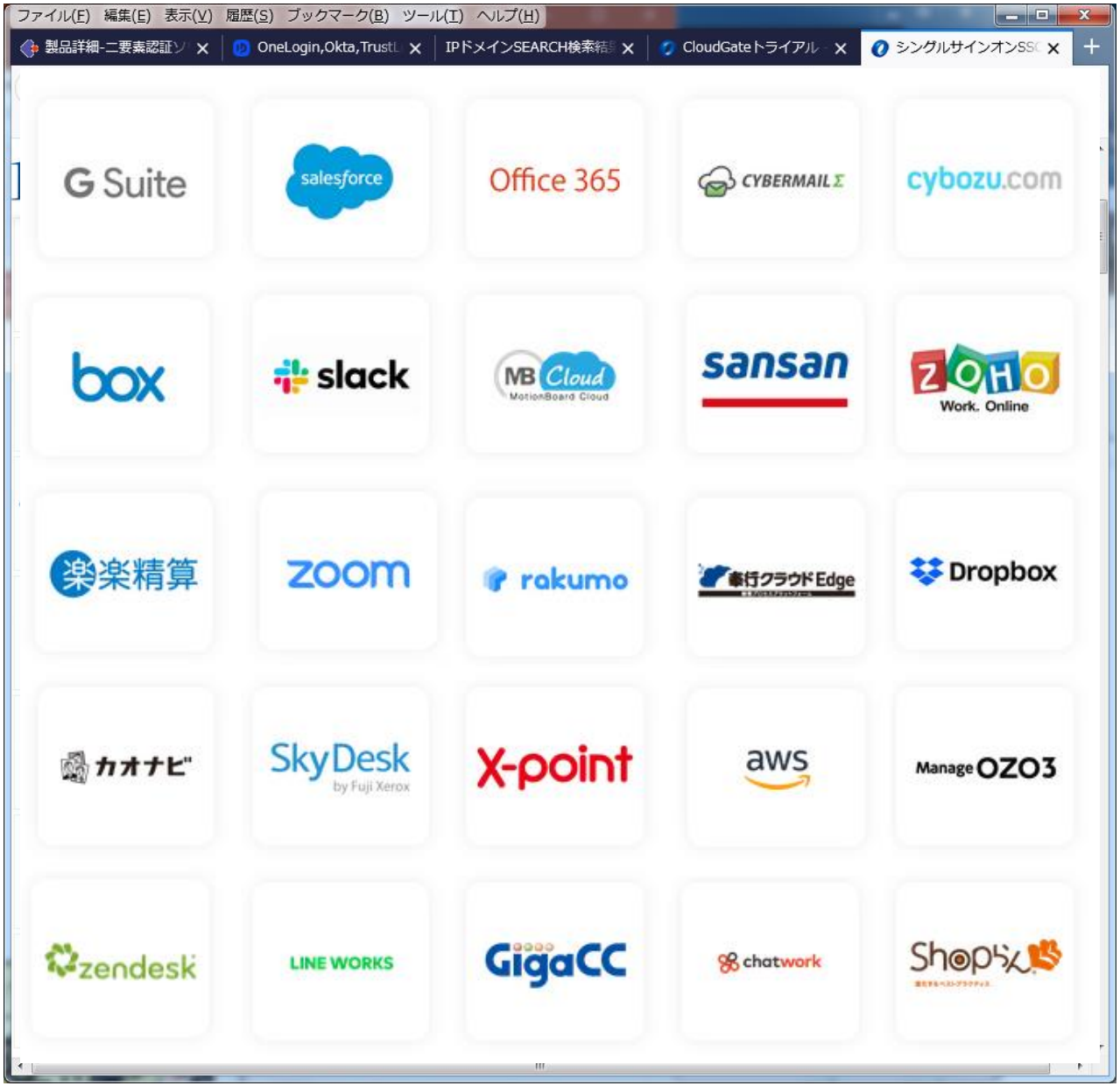

UQ mobile 4G 19:30 75%
Webサイトにログイン
test-opt.mubit.comにログイン
suzuki
キャンセル
ログイン
Active Directory 認証
社員 太郎
00年00月発行
UQ mobile 4G 20:49 72%
Powered BLUE アプライアンス
Powered BLUE / Mubit
最新情報
What's New
2018/05/16
Let's Encryptによる常時SSL化に対応したWebサイトを簡単に構築・運用が出来る仮想アプライアンスの販売開始
NEW
2018/03/08
Powered BLUE 870 SSLクライアント認証サーバー のプレスリリース
2017/12/18
AWS対応/Powered BLUE 870 のプレスリリース
2017/12/05
Powered BLUE 870 のプレスリリース
2017/12/05
Powered BLUE 製品のWeb Page 公開
お知らせ
Information

AD + SSLクライアント認証



AD + SSLクライアント認証

認証　その4　SaaS のアプリ　SAML（サムル）認証対応



(親) SAML認証　idP / IDaaSなど

Azure
Active Directory

TrustLogin
by GMO

G Suite

CloudGateUNO
クラウドゲートウノ

onelogin

okta

iDaaS = iD As A Service

SSO対応 の IdaaSと SaaSアプリ　　SAMLで認証

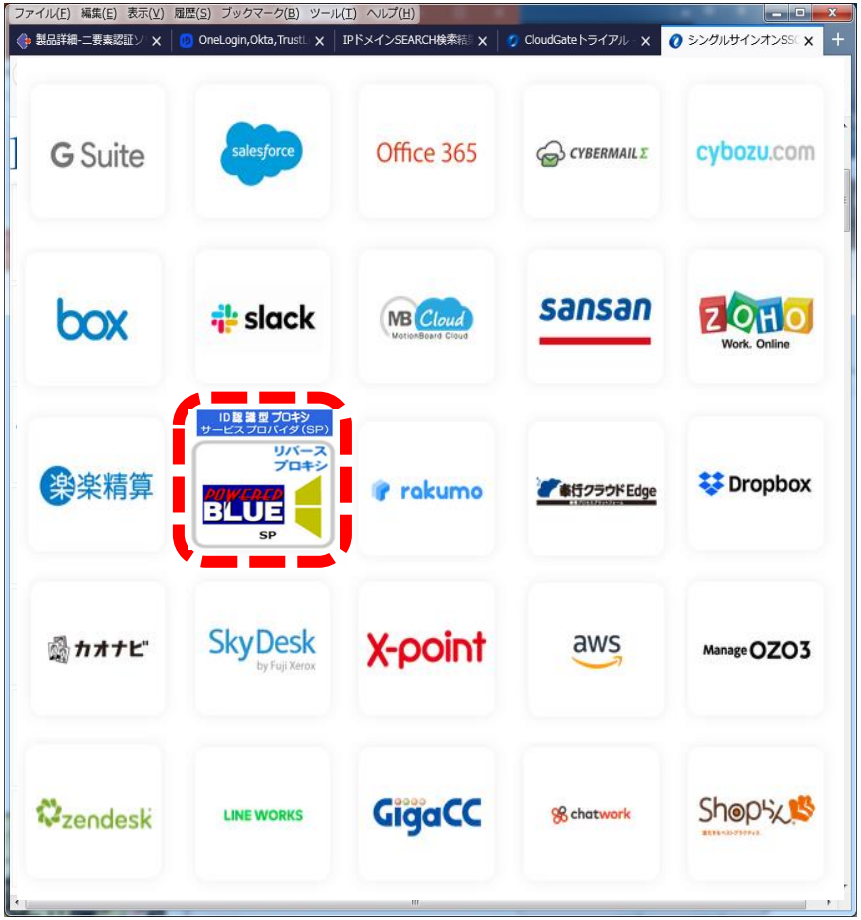
親/ID管理（idP)

Azure Active Directory　TrustLogin

G Suite　CloudGateUNO

onelogin　okta　HENNGE

子/アプリ（SP）



ゼロトラスト対応 + ID認識型リバースプロキシ

＊レガシーなWebサーバーへ、SSO対応のリバースプロキシ経由でアクセス出来ます

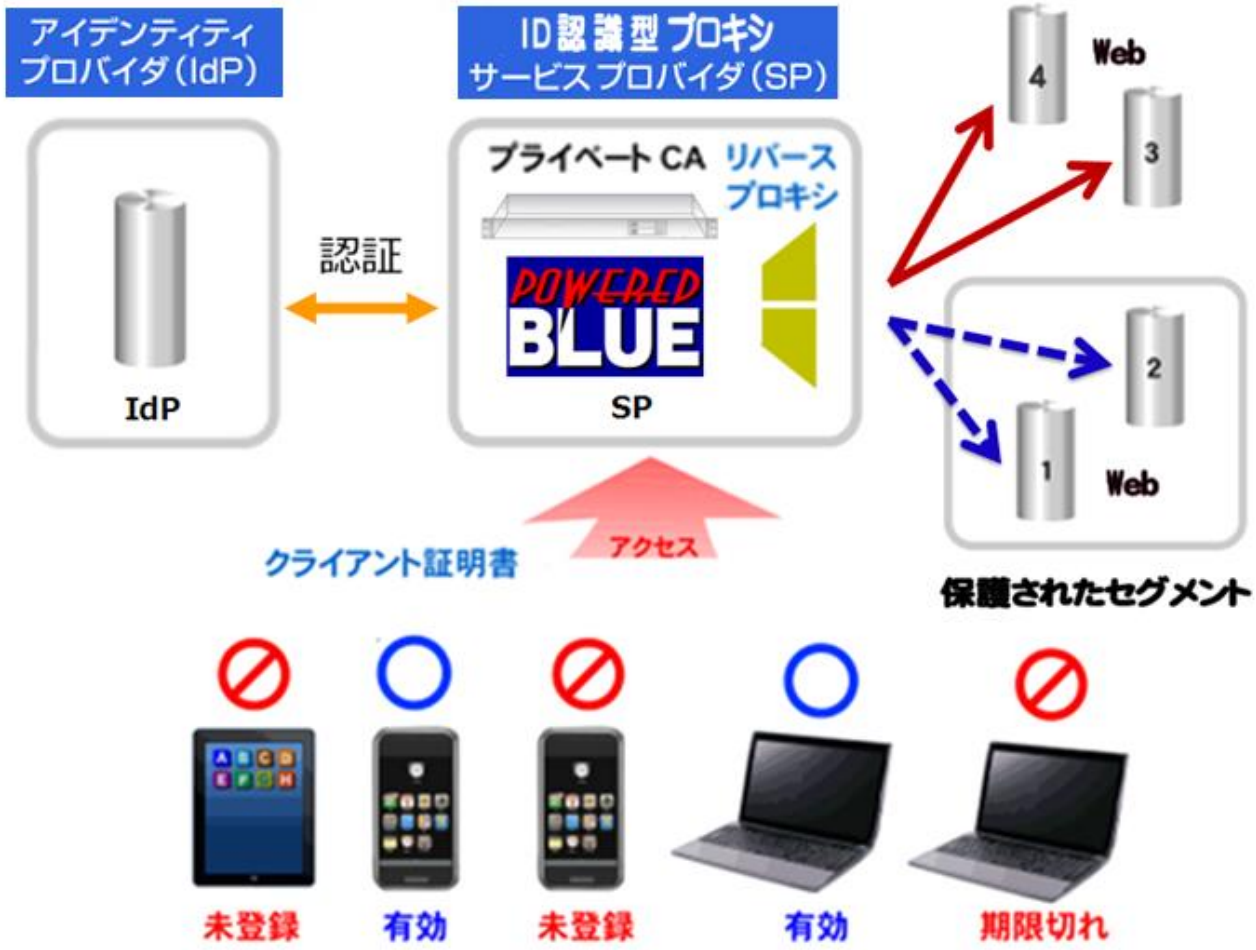
リバースプロキシ には ユーザーアカウント不要

- ID認識型リバースプロキシからのアカウント **漏洩の心配不要**

- **エージェント不要**
  - ●ターゲットのWebサーバーの変更不要
  - ●任意のidPと連携可能

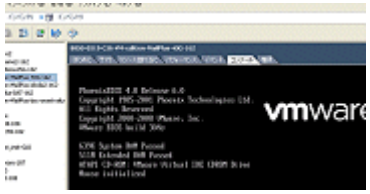
- ゼロトラスト対応/ID認識型リバースプロキシの **設置運用は簡単**

リバースプロキシ での 独自認証　SSLクライアント認証



＊ＳＳＬクライアント認証＋ＳＡＭＬ認証対応のリバースプロキシ経由でアクセス

アプライアンスでの提供・動作環境



POWERED BLUE

POWERED BLUE

Microsoft® Hyper-V™

powered by amazon web services

最後に　「快適なテレワークのために」

VPNの代替

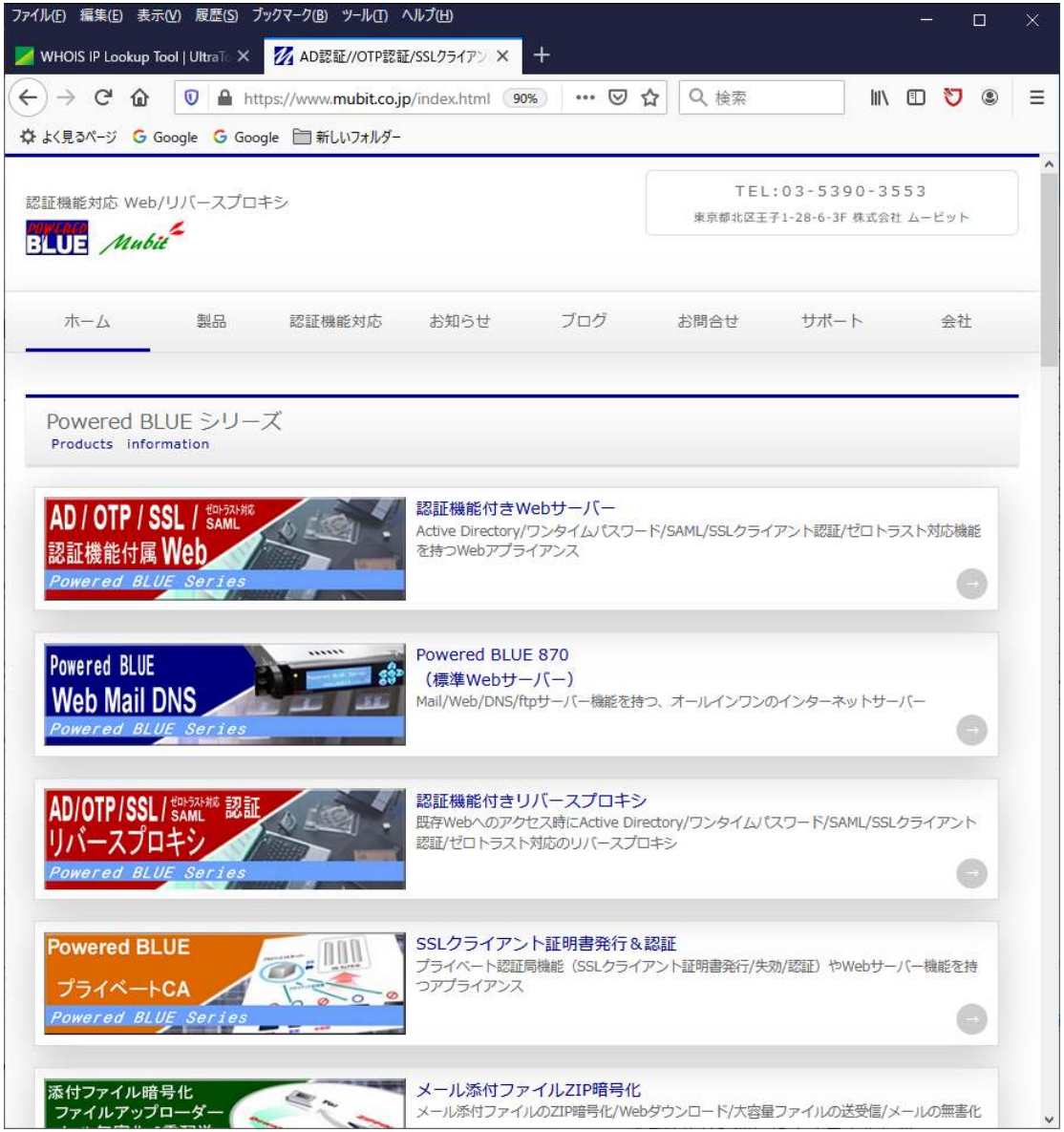
VPN機器増強よりも
認証対応のリバースプロキシを併用

ゼロトラストの導入

リバースプロキシ型は導入が簡単

Webサイト

認証対応
リバース
プロキシ



https://www.mubit.co.jp/