

大手セキュリティベンダーの 二要素認証ソリューションから Swivel に移行



セキュリティ強度を維持しながらも ユーザーの利便性を向上させたネットワンシステムズ

ネットワンシステムズ株式会社(以下「ネットワン」)は、ネットワーク技術を核に、日本のインターネットの黎明期からネットワークインテグレーションの先頭を走り続けてきました。最近ではクラウドコンピューティング環境の構築に注力する一方で、インターネットにあらゆるモノがつながる時代(IoT)が目前に迫っており、ネットワークの重要性も今以上に高まると考えられます。このようなドラスティックな変化の中で、ネットワンは「目的に合わせて、最適な ICT 環境を構築し、使いこなすためには何が必要なのか」というお客様の疑問に真正面から取り組み、独自の付加価値を提供することを目的にしています。

ネットワークインテグレーションのプロフェッショナルとして、ネットワンは様々な最先端技術を社内システムに取り入れてきました。お客様にご提案する前に、自社でその機能・有用性を検証することが重要だと考えているからです。そのネットワンの社内システムの構築・運用を手がけているのが経営企画本部プラットフォーム部です。今回、プラットフォームチームの皆様に Swivel の導入について伺いました。

トークンの管理コストが課題

ネットワンが大手セキュリティベンダーのハードウェアトークン方式の二要素認証を導入したのは、10年以上前のこと。「国内ではかなり早いほうだったのではないかと」のことです。最新の技術をまずは社内で使ってみる、という考えからのことなのでしょう。しかし、導入当時はハードウェアトークンしか選択肢が無く、コストや管理の負担は高かったようです。

「ハードウェアトークンは一定期間ごとに交換しなければなりません。そのための費用ももちろんですが、交換時期を管理したり、紛失に対応するなどの運用上の負担も非常に高いのです。」

後に携帯電話やスマホを使うソフトウェアトークンも導入しましたが、ユーザーとの関連付けを管理者が行わなければならない等、運用負担は減りませんでした。

二要素認証ソリューションの見直しで PINsafe を選択

そのような中、それまで使っていたシステムのサーバー更新の時期が近づいてきたため、全社の二要素認証プラットフォームの見直しを決断し、検討を始めました。その結果、英 Swivel Secure 社の PINsafe を選択したのです。PINsafe は欧州の銀行などで広く使われており、安全性と利便性には定評があります。

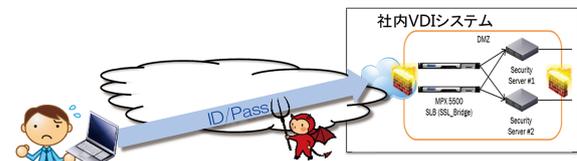
PINsafe を選択したのは、

- ・ トークンレスでワンタイムパスワードが発行できる

- ・ 二要素認証時に運用工数が大きく削減できる
- ・ 二要素認証時のガラケー・メール、スマホ・アプリ、ハードウェアトークンを全て単一のソリューションで管理できる
- ・ ユーザーの使い勝手は損なわないでセキュリティ強度を保つことができる

点が決め手でした。

インターネット経由アクセスのリスクと対策



リスクと対策

- インターネットでやりとりされる情報は全て第三者に筒抜けであるという前提でセキュリティ設計を行う必要があります。その前提に立つと、VDIへの外部からのアクセスをID、Passによって認証を行った場合、簡単になりすぎてしまいます。
- このリスクに対する有効な対策が、「ワンタイムパスワード」であり、より手堅い本人確認が「二要素認証」です

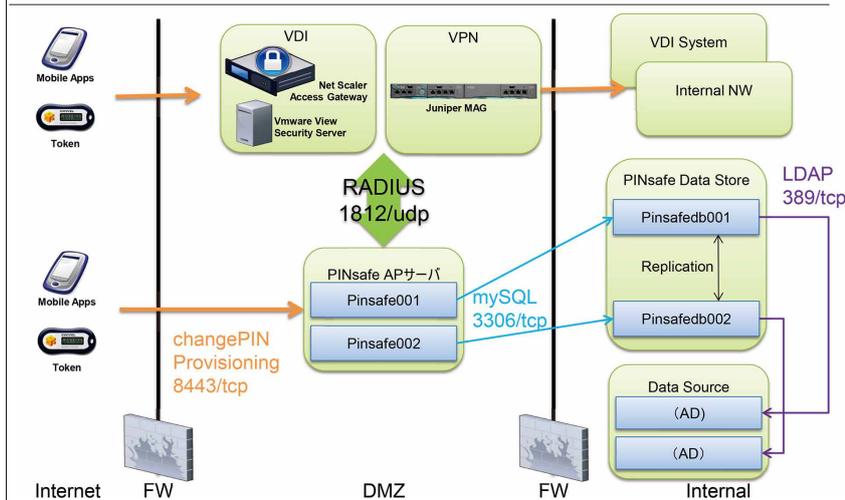
ネットワン様作成の概念図

「弊社では、社外からのアクセスは二要素認証とすることをセキュリティ・ポリシーとしています。その場合、選定時に比較した他社のソリューションの場合、スマホ等のデバイスに表示した文字が小さく、使い勝手が悪いという指摘を役職者からもらいました。その点、Swivelのスマホアプリは文字も大きく、使い勝手が良いと好評をいただいています。」

「また、暗証番号(PIN)の桁数が多くなると、覚えづらいために簡単な暗証番号にしたり、紙に書いたり、入力時に間違いが多くなり、セキュリティレベルが逆に下がってしまう恐れがあります。PINsafeは桁数やポリシー(桁数、連続数字の許可/不許可、降順の許可/不許可)の自由度が高いため、ユーザーの声や運用開始後の実情に合わせて最適化できると判断しました。」

「以前のソリューションは、ハードウェアトークン、ソフトウェアトークンを使用してワンタイムパスワードを

システム全体図



ネットワーク社内システム全体図

発行する仕組みだったため、トークンのコストが増大しておりました。新システムでは基本的にトークンレスで、ハードウェアトークンを必要最低限に抑えることが出来たため、トークンのコストを大幅に削減することが出来ました。(トークンを約 1/30 に削減できています。)さらに、ハードウェアトークン以外のユーザについては、スマホアプリでのセキュリティストリングス表示、メールでの配信等の選択肢があり、全てのユーザが問題なく二要素認証が出来ています。これにより、トークン管理の運用工数を大幅に削減することが出来ました。]

ユーザーも PINsafe への移行を歓迎

PINsafe への移行を決定してから、エンドユーザー向けの教育プランを作成しました。方式が大きく変わるため、念には念を入れたのですが、それでも移行後 1 週間は問合せが急増したとのことです。スマホとハードウェアトークンに加えてメール配信という新しい方式が加わったことで、混乱が生じたのが大きな原因だったようです。

しかし、メール配信そのものについては「ガラケーなどにも対応でき、汎用性も高いため、一番重要な方式であると考えています。」とのこと。実際、全ユーザーに占めるメールユーザーの数は半分以上だそうです。

特にハードウェアトークンからの移行ユーザーの場合、スマホアプリや携帯メールの利便性は大きいようです。ハードウェアトークンは持ち歩きを忘れることもあります。スマホや携帯であれば、ほぼ確実に持ち歩いているからです。

一方で、システム構築そのものは大きな問題も無かったそうです。「当初、弊社側でのシステム設計に対する考え方がずれていたのですが、適切なサポートを受けられたので、大きな問題にはなりませんでした。」こういった経験が、お客様への提案に活かされていくのでしょう。

各種標準インターフェースを高く評価

「PINsafe は LDAP を標準サポートしているため、既存の AD とシームレスに連携でき、システム構築もユーザ管理も非常にスムーズでした。また弊社では 2 種類の VDI と 2 種類の VPN 装置における認証で使用していますが、全てが標準インターフェースということもあり、非常にシンプルに構築出来ました。」さらに「実は Syslog と連携できる点も、各種 LOG を一元管理できるため大きなポイントです。」とのこと。PINsafe の特長である、各種標準インターフェースを備えている点を高く評価いただいています。さらに「SAML や AD FS をサポートしている点も、選定の大きなポイントでした。」とおっしゃっています。将来のクラウド有効活用を見据えて製品選定を行われたようです。

ネットワークシステムズ株式会社 概要

設立	1988 年 (昭和 63 年) 2 月 1 日
代表取締役	吉野 孝行
所在地	東京都千代田区丸の内二丁目 7 番 2 号 JP タワー
従業員数	(単体) 2,163 人 (連結) 2,422 人 (2014 年 3 月 31 日現在)
資本金	122 億 79 万円 (2014 年 3 月 31 日現在)
事業内容	世界の最先端技術を取り入れた情報インフラ構築とそれらに関連したサービスの提供 戦略的な ICT 利活用を実現するノウハウの提供



ネットワークシステムズ株式会社経営企画本部プラットフォーム部プラットフォームチームの皆様
左から木下 智生氏、伊藤 央典氏、大井 康平氏、久田 章太氏、谷口 清司氏



セキュリティストリングス株式会社

〒102-0082 東京都千代田区一番町 6 番地 相模屋本社ビル 7F
Email: sales@securitystrings.com
URL: http://www.securitystrings.com

お問合せ