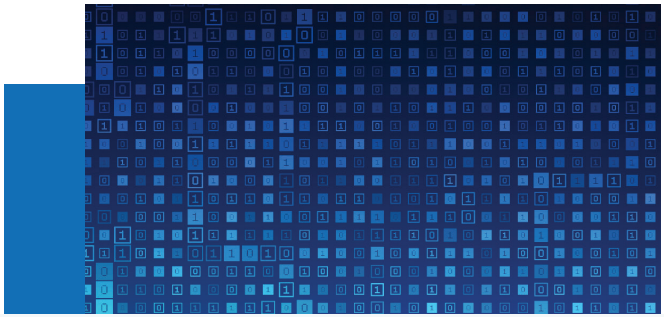
ケーススタディ

LINEヤフー

digicert®

端末管理の強化によるセキュリティ厳格化とコスト削減を同時に実現



LINEヤフー株式会社では各社員が社内のシステムにアクセスする手法および管理手法として電子証明書を利用してきた。しかし、自社で運用する認証局は、オンプレミスサーバーで管理するためのシステム冗長化、内部運用費用などコスト面の効率化から金融機関などでも実績があるクラウド型のPKIとして提供されるDigiCert Trust Lifecycle Managerの利用を決めた。 また、その証明書の配布実装方法をMDMによる自動実装に切り替え多様な端末環境への証明書導入を実現することで業務の省力化も実現した。

LINEヤフー株式会社

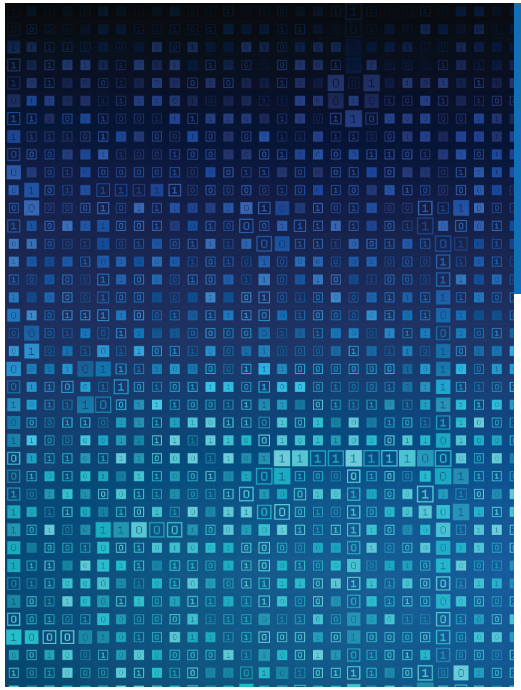
https://www.lycorp.co.jp/

業種：インターネット広告事業、Eコマース事業及び会員サービス事業などの展開並びにグループ会社の経営管理業務など

課題：社内のオンプレミスサーバー削減とセキュリティ強化

導入サービス：DigiCert Trust Lifecycle Manager

LINEヤフー株式会社は、“「WOW」なライフプラットフォームを創り、日常に「!」を届ける。”をミッションとし、24時間365日、どんな時も人々の暮らしに寄り添い、驚きと感動を提供していきます。



クライアント証明書によるアクセス管理

LINEヤフーは、さまざまな情報を取り扱う業務を行なっている。そのため、秘匿情報へのアクセスには細かな管理が必要で、アクセス機器のウイルス対策や細かなアクセス権限設定を行うにあたり幅広い業界で実績が高く、長年の利用により信頼性を証明してきた電子証明書によるアクセス管理を利用してきた。これによりPCといったデバイスに紐づいた電子証明書を組み込んだ機器のみが社内ネットワークや社内サービスにアクセスができるようになることで安全、かつアクセスするシステムごとにログイン手法を変えるような面倒な手間が省けるようになる。

証明書の運用をオンプレミスサーバーからクラウドへ移行

なお、その証明書を作成、運用管理を行うにあたり認証局ソフトを利用してオンプレミスで運用してきた。社内環境の中で使うプライベート証明書なので、社内リソースで運用を行なってきたが、実はその社内リソースへの負担が重くなってきた。 また、LINEヤフーでもリモートワークが業務形態の主流となっているが、オンプレミスにCAがあるため社員の入退社に伴う証明書の発行や失効、端末交換の際にオフィスへの出社が必要になってしまうことが課題となっていた。さらに発行した証明書の管理は別途行う必要があり、それらも表には出ないコストとして業務負担となっていた。

そこで従来より公開サーバーなどのパブリック電子証明書で付き合いのあったDigiCertに相談し、金融機関向けでの実績が豊富なプライベート電子証明書の発行システムでもあるDigiCert Trust Lifecycle Manager導入の検討を始めた。Trust Lifecycle Managerは、電子証明書の発行と管理を行えるPKIマネージャーで、DigiCertの世界的なインフラによりクラウドでも提供される。ITインフラ本部ITサービスインテグレーション部の齊藤 隆弘氏は説明する。「PKI運用と専門分野ではない証明書管理を専門家に任せてしまうことでもっとフォーカスしたい業務に集中できる」。今回のクラウドPKIサービスの利用により、証明局サーバ、CA秘密鍵管理のためのHSM、人事システムに連動して証明書を発行する内製システム、発行済み証明書の保管・管理運用などの社内システムを削減することに成功した。

また、証明書のプロファイルや期限管理を一つの管理画面で行うことができるようになるため発行済み証明書の管理から課題のある証明書の一覧、対策を迅速に行える上、アラートを設定することも可能な為事前に対策を行うことができる。

MDMによる証明書の導入作業の省力化とメンテナンスコストの削減

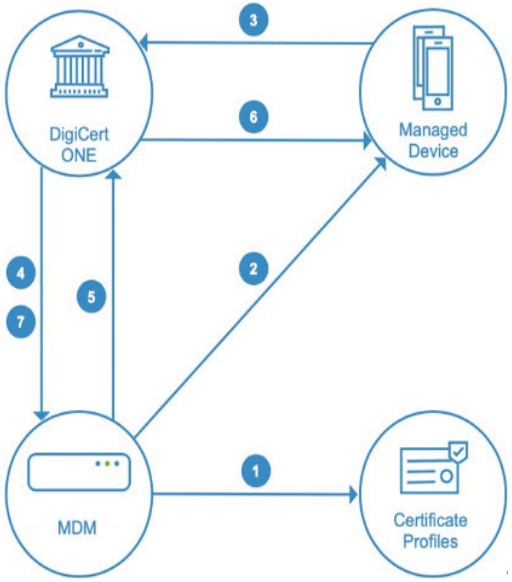
同時に証明書に関わる、発行、配布、更新は従来より非常に手間のかかる業務だった。社内での証明書取得・導入方法のマニュアル化から、実際の認証局運用と端末へのインストールなど、特に昨今、多機能化、高性能化が進むモバイルデバイスやタブレットなど社内業務で利用される端末の多様化は、共通の管理手法が困難になる要因にもなり業務を圧迫する要因にもなっていた。

それらの効率化とコストの削減も狙いMDMによる管理そして証明書の配布も推進した。MDMといえば、ソフトウェアの設定やアップデートの強制施行や管理といった用途に使うのだが、当然証明書の実装にも使うことができる。そしてそれを実行する証明書プロファイルや実績が豊富なDigiCert Trust Lifecycle Managerを選んだということになる。

特に複数のMDM向けに準備された証明書プロファイルにより簡単に各MDM向けの証明書を発行、配布ができるため、多様なデバイス環境にも簡単に証明書の実装ができ、それによる業務負荷の軽減は目を見張るものがある。「MDMとTrust Lifecycle Managerを組み合わせて証明書を実装し、セキュリティを施すことで一台の設定にかける時間が20%削減された。」(齊藤氏)

今後、認証基盤と連携した多要素認証の実現することで社内ユーザーにセキュリティを意識させることなく、かつ安全にセキュリティを強化することができると期待する。

Trust LifeCycle Manager利用による証明書実装例



1. MDM管理者が、DigiCert One上のTrust Lifecycle Managerで作成された証明書プロファイルに対応する証明書テンプレートをMDMで作成
2. MDMは、デバイス構成プロファイルを、指定されたデバイスグループに展開
3. デバイスは手順2で展開されたプロファイルに基づき、証明書要求をTrust Lifecycle Managerに送信
4. Trust Lifecycle Managerは、MDMの要求を検証
5. MDMは、Trust Lifecycle Managerに検証応答
6. Trust Lifecycle Managerが、要求元のデバイスに証明書を発行
7. Trust Lifecycle Managerが、確認メッセージ送付