

セーフネット認証サービス – ケーススタディ – Health & Social Care in Northern Ireland

ケーススタディ

北アイルランドの HSC (Health and Social Care) システムには、5 つの HSC Trust (Belfast, South Eastern, Western, Southern, Northern) が含まれ、北アイルランド全域にわたって統合された社会保険サービスを提供しています。

組織

5 つの HSC Trust は、病院、医療センター、老人ホーム、デイセンター、その他の社会保険施設を管理運営しており、広範な社会保険サービスをコミュニティに提供しています。その 6 つ目の Trust に、Northern Ireland Ambulance Service があります。

HSC にはまた、新規の Health and Social Care Board、Public Health Agency、Patient and Client Council、Business Services Organization (BSO) も含まれています。BSO は、ICT サービスなどの多数の HSC 向けサービスに対する責任を担っています。

ビジネスニーズ

セキュリティ標準のベストプラクティス

HSCNI (Health & Social Care in Northern Ireland) の ICT セキュリティポリシーは ISO27001 に基づいており、Connecting for Health が発行した適正実施ガイドラインを参考にしています。これはつまり、HSCNI がセキュアなリモートアクセスサービスとサードパーティの請負業者によるインターネットや PSTN 経由のアクセスを確保するために、二要素認証 (2FA) を実装したことを意味します。HSCNI はまた、大量の機密データへのアクセスを許可するには、特定の Web ベースアプリケーションに二要素認証を追加する必要があることを認識しています。



TCO (総所有コスト) の削減

長年にわたって最大 700 ユーザーに対し、「セーフネット認証サービス」ではない他社の二要素認証システムが使用されてきました。そのシステムではワンタイムパスワード(OTP)の生成にハードウェアトークンを使用し、ハードウェアトークンを3年ごとに交換する必要があったため、かなりの間接費が継続的に生じていました。そのため HSCNI は、長期的に所有コストを減らせる二要素認証ソリューションを探することにしました。

ソリューション

HSCNI は、従来使用していた二要素認証システムを SafeNet のクラウド型認証サービスである「セーフネット認証サービス」に切り替え、1000 トークンを導入しました。HSCNI は、リモートや第三者アクセスから Web ベースのアプリケーション (病院の順番待ちリストや、特定の疾患の傾向を追跡し監視するアプリケーションなど) まで、「セーフネット認証サービス」の使用を拡大させました。これらのアプリケーションには機密を要するデータが大量に含まれるため、二要素認証による保護が必要です。

利益

コスト節約

HSCNI は、「セーフネット認証サービス」に切り替えたことで管理コストの減少とハードウェアトークンの交換・買い替え費用が不要となることで、3年間で大幅にコストを節約できると予測しています。この額は、新しい二要素認証サプライヤーへの変更にかかるコストを容易に上回るものであり、今までのところ、HSCNI は予測通りにコスト削減を進めています。

「セーフネット認証サービス」のハードウェアトークンはサービスに無償バンドルされており、耐久性が非常に高く有効期限もないので、競合するトークンよりも長寿命です。そのため、トークン交換コストの排除によって得られる利益だけでなく、ロジスティックとデプロイメント要件の減少によって生じるコストとリソースの余りからも利益が得られます。

また「セーフネット認証サービス」はアプリケーションとの関係が簡単なため、実装のコストが削減されます。SafeNet は HSC と密接に連携することで、迅速な反応とスムーズな引き渡しを保証しています。

規模のメリット

すべての HSCNI 組織が使用できるフレームワーク契約を結ぶことで、規模のメリットが達成されました。「セーフネット認証サービス」の導入後、各 HSCNI 組織には中央サービスへの代理管理権が与えられ、各自でトークンとユーザーを管理できるようになりました。HSCNI は更にトークンを追加導入し、2009 年 7 月までに HSCNI 全体で 2000 トークンが使用されています。

ユーザー認証のセキュリティ

「セーフネット認証サービス」は HSCNI のセキュリティポリシー要件を満たしており、その IT プラットフォーム全体での使用は、Connecting for Health が定義したベストプラクティスに準拠しています。管理者、給与スタッフ、医療スタッフ、請負業者などのユーザーは、二要素認証を使用することで強固なセキュリティを確保して機密情報にアクセスできます。トークンの操作はシンプルなので、ユーザーが二要素認証の使用に要する時間は最小限に抑えられます。これは、時間に追われ続けている医療専門家にとって特に重要なことです。

将来

HSCNI は、SafeNet が提供する最新のクラウド型二要素認証サービスである「セーフネット認証サービス PCE」にサービスをアップグレードし、さらなる特長と利点から利益が得られることを期待しています。具体的には、「セーフネット認証サービス PCE」は個々のニーズを満たすためにソフト、USB、SMS 形式でトークンを展開する柔軟性を備えています。たとえば、ソフトウェアトークンを請負業者に割り当てることで、契約終了時にハードウェアトークンを返却する必要がなくなります。使用頻度の少ないスタッフは、Blackberry/USB と SMS トークンの選択肢があるため、2 つのデバイスを持ち歩く必要がなく、ユーザーは常に二要素認証により保護されたアプリケーションにアクセスできます。

「SafeNet との継続的な協議を通じて、近いうちに『セーフネット認証サービス PCE』にサーバをアップグレードします。SMS や BlackBerry トークンなどの、より広範なトークンから利益が得られることを期待しています。それによってエンドユーザーのニーズをより適切に満たし、最終的には、さらなるコスト削減を達成することを目指しています。

私たちがセーフネット認証サービスの二要素認証に切り替えた理由は、これが 3 年目の評価時点で最良の TCO をもたらすからです。」

Health & Social Care in Northern Ireland、HSCNI ICT セキュリティマネージャー、Michael Harnett 氏

「セーフネット認証サービス」について

「セーフネット認証サービス」は、完全な自動化と、組織の固有のニーズに合わせてカスタマイズできる柔軟なトークンオプションを備えた、高セキュアな AaaS (Authentication as a Service 「認証・アズ・ア・サービス」) を提供し、TCO を大幅に削減します。

「セーフネット認証サービス」の柔軟性と拡張性、ワークフローの自動化、ベンダーにとらわれないトークン統合、そして幅広い API によって、強力な認証が容易に手に入ります。また、管理機能とプロセスは完全に自動化され、カスタマイズも可能であり、シームレスで快適なユーザー体感を実現します。

「セーフネット認証サービス」はインフラが不要であるため、複数階層、マルチテナントのクラウド環境に簡単に移行でき、クラウドベースおよびオンプレミスのアプリケーションから、ネットワーク、ユーザー、デバイスに至るすべてを保護します。

「セーフネット認証サービス」は認証サーバー構築不要、ハードウェアトークンはバンドルされているので、初期費用無しで始められるワンタイムパスワードです。



THE
DATA
PROTECTION
COMPANY

日本セーフネット株式会社

データプロテクション事業部
東京都港区新橋 6-17-17 御成門センタービル 8F
Tel: 03-5776-2751
Email: jp-info@safenet-inc.com

記載されている会社名、製品名およびロゴは、各社の商標または登録商標です。カタログに掲載されている内容は、予告なく変更される場合があります。
©2013 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners.