別添①

【重要】クライアント証明書「SHA-2」のご提供について

日頃から ID Link をご利用いただきまして誠にありがとうございます。

インターネット通信の暗号化方式「SHA-1」を使用したクライアント証明書について、セキュリティの脆弱性が報告されています。
弊社では、お客様の情報の安全性を確保するため、セキュリティを強化し、従来の「SHA-1」方式に加え、より高度な暗号化方式「SHA-2」のクライアント証明書の提供を開始します。
2016 年 8 月までに評価を行い、9 月より順次、「SHA-2」クライアント証明書をお送りする予定です。
Microsoft 社では、Windows は 2017 年 2 月に「SHA-1」クライアント証明書での SSL 通信を利用停止すると表明しており、他のブラウザベンダーでも 2017 年 1 月に利用停止が予定されています。
利用停止を待たず、速やかに証明書の入れ替えをしてくださいますようお願い致します。

※ 今までお使いのログイン ID,パスワードはそのままご利用いただけます。

※ ゲートウェイサーバ設置の院内環境、オンデマンド VPN での ID-Link のご利用には、クライアント証明書は利用しておりませんので、対応は不要です。

※ 今回新たに提供を開始するクライアント証明書は TLS1.2 にも対応致します。

～各利用施設様への証明書の送付について～

新しいクライアント証明書は、CD に保存し発送、もしくはメールに添付してお送り致します。
送付方法については、下記の 3 つからお選びください。

1.運営主体事務局様へ一括送付（CD 保存）
2.運営主体事務局様へ一括送付（メール添付）
3.各利用者様へ直接送付（CD 保存）

※ "3.各利用者様へ直接送付"の場合は、施設名、住所、電話番号、担当者名等のご確認のご協力をお願い致します。
※ 送付方法につきましては、弊社より折り返し確認のご連絡を致しますので、その際にお申し付けください。
※ クライアント証明書入れ替えの手順は、証明書送付時にご案内致します。

SEC CORPORATION LTD.
株式会社エスイーシー
医療システム事業部クラウドソリューション部
TEL：0138-22-7227
FAX：0138-23-1472
e-mail：support@mykarte.com

別添②

【重要】クライアント証明書「SHA-2」のご提供とセンター通信設備切り替えのお知らせ

写

平成 28 年 9 月 6 日
株式会社エスイーシー

日頃から「ID-Link」をご利用いただきまして誠にありがとうございます。
先日、「クライアント証明書「SHA-2」のご提供について」にて、ご案内した通り、9 月より、SHA-2 証明書の送付を順次開始致します。
また、ID-Link センターの通信設備も、よりセキュリティを強化したものに切り替えを行います。
切り替えは 2016 年 12 月 12 日（月）を予定しておりますが、DNS（Domain Name System）の設定変更となりますので、反映するまでの時間がご利用の環境によって異なります。早ければ 1 日後、遅ければ 1 週間程度かかる場合がありますのであらかじめご了承下さい。
なお、今回ご提供する SHA-2 証明書より、TLS1.2 の利用が可能となりました。厚生労働省「医療情報システムの安全管理に関するガイドライン　第 4.3 版」に関する Q&A（※注 1）において、HTTPS を用いて医療情報システムに接続する場合は、TLS1.2 のみに限定した上で、クライアント証明書を利用したクライアント認証の実施が求められています。また、来年 1 月 1 日には、ブラウザベンダーによる既存の証明書の利用停止が予想されておりますので、停止を待たずに速やかに証明書のインストールを行い、TLS1.2 のみに限定した接続としてくださいますようお願い致します。

※　今までお使いのログイン ID,パスワードはそのままご利用いただけます。
※　ゲートウェイサーバ設置の院内環境、オンデマンド VPN での ID-Link のご利用には、クライアント証明書は利用しておりませんので、インストールは不要です。

注 1）
「医療情報システムの安全管理に関するガイドライン第 4.3 版」に関する Q&A
（平成 28 年 8 月）
http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000027272.html

センターと証明書の関係

証明書	センター：切り替え後	センター：切り替え前
SHA2	利用可能	利用不可 ※ 事前の証明書インストールは可能
既存	利用可能 iOSは利用不可	利用可能

■ センター通信設備の切り替え前 ■

既に ID-Link ご利用の場合は、同じブラウザで SHA-2 証明書の事前インストールをお願いします。
センター通信設備の切り替え後は証明書選択画面等が表示されますが、継続してご利用が可能です。

■ センター通信設備の切り替え後 ■

センター通信設備の切り替え前に SHA-2 証明書をインストール出来なかった場合でも警告が表示されますが、継続してご利用は可能です。
ブラウザベンダーの利用制限が予想される来年の 1 月 1 日以前に SHA-2 証明書のインストールをお願いします。
※『iOS』はセンター通信設備の切り替え後に SHA-2 証明書がインストールされていないと利用できませんのでご注意下さい。

SHA-2 証明書の追加インストール手順、ID-Link センターの通信設備の切り替え後の対処方法等の情報は、ID-Link の Web サイトに掲載しておりますのでご参照ください。
URL：http://www.mykarte.org/idlink/
［Support］→［SHA-2 証明書］

【お送りするファイルの詳細】

（CD、添付ファイルのの中身）

ID-Link の URL
デジタル証明書
証明書インストールパスワード
iOS 用追加証明書

SEC
株式会社エスイーシー
医療システム事業部クラウドソリューション部
TEL：0138-22-7227
FAX：0138-22-8501
e-mail：support@mykarte.com