RSA

参考資料：緊急時のリモートアクセスニーズに応える RSA SecurID Access BCO ライセンス

RSA SecurID Access BCO ライセンスは、多数のユーザーが急遽、リモートワークを必要とするような緊急時に、ユーザー数を一時的に増やせるライセンスオプションです

世界的な感染症の流行、自然災害、サイバー攻撃などによる業務混乱時や在宅勤務の推奨時では、想定以上に多くのユーザーがリモート業務を希望し、「危機の渦中のさらなる危機」が発生します。RSA SecurID 認証トークンを持たないユーザーが相当数、存在する場合、IT 部門は対応に奔走する代わりに、一時的に多要素認証を無効にしてすべてのユーザーが強力な認証なしにログインできるようにセキュリティ ポリシーを緩和することがあります。この方法は、業務再開のための最短の解決法に見えますが、重大なリスクにさらされる可能性をもたらします。

緊急時も一貫性のある多要素認証ポリシーを維持することは重要です。セキュリティ ポリシーを緩和して攻撃にさらされる危険性を高めることや IT 予算を超過することなく、費用対効果の高い方法が求められます。

この課題の解決が RSA SecurID の BCO（Business Continuity Option）ライセンスの活用です。このライセンスならば、新たに多要素認証の予算を増やすことなく組織内のユーザー数を一時的に増やすことができます。

Business Continuity Option 認証の仕組み

Business Continuity Option は、RSA SecurID Access のオプションとして利用可能なライセンス機能です。
管理者は、必要に応じてこの機能を表示、選択、アクティベート（有効化）できます。アクティベートすると、予め設定した数までサーバーライセンスが増え、増加分はリモートを希望するユーザーに割り当てることができます。

ユーザーは、「セルフサービス Web ポータル」を介してオンデマンド オーセンティケータを要求します。オンデマンド オーセンティケータは、「オンデマンド トークンコード」を e メールか SMS 経由でユーザーに送ります。物理的なハードウェアトークンは不要です。

ユーザーがオンデマンド オーセンティケータの発行を受ける時に「セルフサービス」ポータルにログインすると、事前に登録しておいた送付先に「オンデマンド トークンコード」が送信されます。これで知っていること（ログイン/パスワード）と、持っているもの（SMS または電子メールを介してモバイルデバイスに配信される 1 回限りのパスワード）という「多要素認証」のルールが適用されます。

Business Continuity Option の仕様

- 有効期間は 3 年間
- 3 年間で最大 6 回のアクティベーションが可能
- 1 回のアクティベーションで最大 60 日間有効
- ユーザー数は 5,000 人まで対応（それ以上は、応相談）
- オンデマンド トークンは、e メールか SMS を選択可能
- RSA SecurID Access の全ライセンスエディション（Base、Enterprise、Premium）で利用可能