事　務　連　絡
平成 23 年 12 月 21 日

各府省庁情報セキュリティ担当課室長あて（注意喚起）
情報ｾｷｭﾘﾃｨ対策推進会議ｵﾌﾞｻﾞｰﾊﾞｰ機関情報セキュリティ担当課室長等あて（情報提供）

内閣官房情報セキュリティセンター
内閣参事官（政府機関総合対策担当）

ネットワーク利用者を管理するサーバのセキュリティ対策の徹底について（注意喚起）

最近の標的型攻撃において、組織内の各種サーバの管理者権限が奪取され、ネットワーク利用者を管理するサーバ（マイクロソフト社の Active Directory サーバ（以下「AD サーバ」という。）、IBM 社の Notes サーバ、その他 LDAP サーバ等の認証サーバ）への侵入を許し、ネットワーク利用者の ID、パスワードハッシュ、組織情報が窃取され、被害が拡大している事例が複数見受けられます。

サーバの設定を適切に行うことにより、容易にはこれらの情報が窃取されることには至らないと考えられます。「政府機関の情報セキュリティ対策のための統一管理基準（以下「管理基準」という。）」及び「政府機関の情報セキュリティ対策のための統一技術基準（以下「技術基準」という。）」においても、不正アクセス等に係る対策として遵守すべき事項を定めているところですが、特に AD サーバについては、実際に利用者情報が窃取された事例があることも鑑みて、下記の通り、担当職員や運用管理業務を委託している事業者への指導を徹底し、AD サーバを管理する情報システムセキュリティ責任者等に運用状況を確認させることを推奨いたします。また、AD サーバ以外の認証サーバを利用している場合であっても、下記を参考に適切な設定を行うよう、同様の指導及び確認を推奨いたします。

なお、本来、管理者権限については、適切に運用がなされていれば容易に管理者権限が奪取されるには至らないと考えられますので、あわせて「システム管理権限を狙った辞書攻撃、ブルートフォース攻撃への対処について（注意喚起）」（平成 23 年 12 月 21 日付事務連絡）をご参照ください。

記

１．下記「マイクロソフト社の Active Directory サーバの推奨設定例」（参考）を参照して適切な設定を行うこと。
　特に、パスワードポリシーの推奨設定（管理者向け）及びセキュリティオプションの推奨値における LAN Manager 認証レベルの設定を徹底すること。

２．ベンダーの提供している情報を参照して、適切な設定に努めること。例えば、Active Directory 2008 であれば、Windows Server 2008 セキュリティガイド http://technet.microsoft.com/ja-jp/windowsserver/ff708743.aspx 等の情報を参考とすること。

３．AD サーバを担当する情報システムセキュリティ責任者自身が、運用管理状況を定期的に確認すること。

以上

（参考）マイクロソフト社の Active Directory サーバの推奨設定例

- パスワード ポリシーの推奨設定（管理者向け）
  コンピュータの構成¥Windows の設定¥セキュリティの設定¥アカウント ポリシー¥パスワード ポリシー
  - パスワードの履歴を記録する　24 のパスワードを記録
  - パスワードの有効期間　42 日間
  - パスワードの変更禁止期間　1 日
  - 最小パスワード長　12 文字以上
  - パスワードは、複雑さの要件を満たす必要がある　有効
  - 暗号化を元に戻せる状態でパスワードを保存する　無効
- アカウント ロックアウト ポリシーの推奨設定
  コンピュータの構成¥Windows の設定¥セキュリティの設定¥アカウント ポリシー¥アカウント ロックアウト ポリシー
  - ロックアウト期間　15 分
  - アカウントのロックアウトのしきい値　10 回ログオンに失敗
  - ロックアウト カウンタのリセット　15 分
- セキュリティオプションの推奨値
  コンピュータの構成¥Windows の設定¥セキュリティの設定¥ローカル ポリシー¥セ

キュリティ オプション

- ネットワーク セキュリティ：次のパスワードの変更で LAN Manager のハッシュの値を保存しない 有効
- ネットワーク セキュリティ：LAN Manager 認証レベル NTLMv2 応答のみ送信する。 LM と NTLM を拒否する
- ネットワーク アクセス:匿名の SID と名前の変換を許可する 無効