報道発表

平成 23 年 12 月 22 日
内閣官房情報セキュリティセンター

標的型攻撃対策としての適切な管理者権限管理について

１．取組の背景

最近の標的型攻撃において、組織内のネットワーク上の一般利用者のクライアントＰＣが、標的型メール攻撃によって不正プログラムに感染した後、当該クライアントＰＣから、辞書攻撃、ブルートフォース攻撃と思われる手段で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への侵入をゆるし、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ております。

２．政府機関における取組

ＮＩＳＣから、各府省庁及び立法府、司法府等のオブザーバー機関に対して、12 月 21 日付で以下のとおり注意喚起をしました。

① 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
　主な内容　・管理者権限のパスワードは、十分に複雑なものとし、安全性を確保すること
　・管理者権限で操作できる端末を制限する等、不正アクセスが困難となるようなシステム上の対策を適切に行うこと
　・システムの監視を継続的に行い、不正アクセスの検知と対応を適切に行うこと　等
② 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
　主な内容　「ネットワーク利用者を管理するサーバ」に係る具体的な取組
　・ベンダーが提供する最新セキュリティパッチに関する情報収集と適切な適用
　・情報セキュリティ責任者自身による運用管理情報の定期的な確認　　等

＊注意喚起文書本文については、以下をご参照下さい。
http://www.nisc.go.jp/active/general/chuuikanki.html

３．今後の取組

政府機関においては、引き続き、情報セキュリティ対策を推進し、情報セキュリティの向上に努めてまいりたいと考えております。

【本報道発表に関する問い合わせ先】
内閣官房情報セキュリティセンター
内閣参事官　木本裕司
電話　03-3581-3959（センター代表）