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）

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）

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、被害が拡大している事例が複数見受けられます。

このような事例については、本来、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。「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、直近の被害事例を鑑みて、特に下記の事項について、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行い、運用状況を情報システムセキュリティ責任者等に確認させることを推奨します。

なお、多くの場合、マイクロソフト社の Active Directory Server 等のネットワーク利用者を管理するサーバが攻撃の標的となっているため、あわせて「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）」（平成 23 年 12 月 21 日付事務連絡）をご参照ください。

記

１．　管理者のログイン ID 及びパスワードは、容易に推測されないものとすること。具体的には、使用する文字の種類、ログイン失敗の許容回数、アカウントのロック期限、パスワードの定期的な変更期限等を適切に設定すること。＜管理基準 1.4.1.1(2)(c)＞＜技術基準 2.2.1.1(1)(i)＞＜技術基準 2.3.3.2(1)(a)＞

（NIST SP800-63 では、オンライン攻撃に対して一定の信頼性を持たせるには、上記を適切に設定することで、攻撃者がパスワードの有効期限にわたってパスワードを推測する確率を 16,384 分の 1 以下とすることを求めている。例えば、大文字小文字数字をすべて含む 8 文字以上で 16 回連続でパスワード認証が失敗するとパスワードの再発行が必要となる設定や、「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）」に記載のパスワードの設定は、これを満たす。）

２．　サーバ管理用のスクリプト中に管理者のパスワードを記述するなど、パスワードの漏洩につながったり、パスワードの更新が困難となったりするような運用を行わないこと。＜管理基準 1.4.1.1(2)(c)＞＜技術基準 2.2.1.1(1)(b)＞

３．　管理者の認証は、パスワード認証と IC カード認証の両方を用いる等、複数要素（複合）主体認証方式で認証すること。＜技術基準 2.2.1.1(1)(g)＞

４．　サーバへの管理者権限によるログインを一般利用者のクライアント PC から行わないよう制限すること。例えば、管理者と一般利用者のセグメントを分割するか、管理者がログインできる端末を、電子証明書による端末認証、IP アドレス、MAC アドレス等により制限すること。＜技術基準 2.2.1.2(1)(b)＞

５．　サーバへの不正アクセス、不審なログイン、不審な操作など、不正な行為及び無許可のアクセス等の意図しない事象の発生を監視し、これが疑われる場合は直ちに対処すること。＜技術基準 2.3.2.3(2)(e)＞

６．　サーバ、運用管理端末、ネットワーク監視装置等で取得した、管理者権限でのログイン履歴、管理者権限による操作履歴、サーバとの通信履歴等から、不正な行為及び無許可のアクセス等の意図しない事象の痕跡がないかを日次で確認すること。管理権限を有する者の出退勤記録や入退室記録などとの相関分析を行うことで確認を行うことが望ましい。＜管理基準 1.5.2.4(3)(a)＞＜技術基準 2.2.1.4(1)(e)＞

７．　サーバ及びネットワークの管理に使用する管理者権限及び特権処理は、細分化又は局在化し、管理者権限を奪取された場合であっても、被害が局所化されるようにすること。

８．　複数のログイン ID でパスワードを共用しないこと。例えば、管理者のログイン ID のパスワードを、他の一般権限の ID のパスワードと共用しないこと。

（※括弧内は、対応する管理基準及び技術基準の項目を示す。）

以上

（参考）

辞書攻撃

パスワードに単語の組み合わせや人名を用いている場合に有効なパスワード解析方法。英語の辞書に限らず各国語の単語を用いる場合もあるため、日本語の単語、日本人の人名も安全ではない。また、単語と数字数桁のような単純な組み合わせも解析の対象となる。

ブルートフォース攻撃

無意味な英数記号の組み合わせも含めた、総当たりでのパスワード解析方法。辞書攻撃より効率は劣るが、原理的には必ず正しいパスワードに到達する。