閣副安危第 375 号
平成 24 年 7 月 5 日

各府省庁等情報セキュリティ担当課室長　あて
情報セキュリティ対策推進会議オブザーバー機関情報セキュリティ担当課室長等　あて

内閣官房情報セキュリティセンター
内閣参事官（政府機関総合対策促進担当）

適切なログの管理による標的型攻撃対策について（情報提供）

昨今、国の機関や企業活動の大きな脅威となっている標的型攻撃への対策として、攻撃を未然に防ぐ各種対策の実施のみならず、実際に攻撃を受けた際に攻撃や被害の状況について把握ができるようにしておくための対策が重要です。そのためには、情報システムのログの取得・管理が必要ですが、ログの取得・管理に係る各種設定や運用が不十分であったため、事後の調査が困難となった事例も見受けられます。

これを受け、当センターは、昨年度、有識者による検討会を複数回開催し（検討会座長：佐々木良一　東京電機大学教授、NISC 情報セキュリティ補佐官）、標的型攻撃対策に資する適切なログ管理の在り方について、「平成 23 年度　政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書」として取りまとめ、NISC ホームページに公開いたしました。（http://www.nisc.go.jp/inquiry/index.html）本報告書では、各府省庁における機密性２以上の情報を扱う一般的な情報システムにおいて、比較的費用を伴わずに効果が見込める、早急に実施するべき対策の例を含めて取りまとめましたので、本事務連絡により情報提供いたします。各府省庁におかれましては、下記を参考に、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、適切なログの取得・管理を行っていただいた上で、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。

なお、本報告書の内容については、「政府機関の情報セキュリティ対策のための統一基準群」に、適切に反映を行っていく予定です。

記

＜括弧内は、統一基準上の関連する遵守事項を指す＞

Ⅰ．機器によらない全般的な対策

１．各ログ取得機器のシステム時刻を、タイムサーバを用いて同期する。

＜2.3.2.2(2)(d)，2.3.2.3.(2)(d),2.3.4.1(2)(e)＞

・調査時の複数機器のログの解析を迅速かつ十分に実施するため。（各ログの時刻が数秒ずれていても、これを補正する作業は大変困難である。）
・各ログ取得機器は、タイムサーバを用いた時刻同期ログについても取得する。
・精度や冗長性を高めるため、各ログ取得機器組織内ネットワークに設置したタイムサーバ（stratum2 サーバ）と代替のタイムサーバの複数のタイムサーバを利用することが望ましい。

２．ログは１年間以上保存する。

・過去の標的型攻撃事例から、攻撃事象の発見からさかのぼると攻撃の実施された時期はおおよそ 1 年以内であり、ログを１年間保存すれば、高い確率で攻撃の初期段階からのログを抽出することができるため。

３．複数のログ取得機器のログを、ログサーバを用いて一括取得する。

・攻撃者によるログの改ざんを簡便に防ぐことが出来るため。
・ログサーバのアクセス権を最小限とすることが望ましい。また、ログサーバについては、改ざん防止のために内部ネットワークに置く必要がある。
・高スペックな機器を利用する必要は無い。

４．攻撃等の事象発生が確認された場合の対処手順を整備する。

＜1.2.2.2(1)(c)＞

・攻撃等の事象発生が確認された場合に取るべき行動を検討し周知すること。不必要な行動をとってしまうことでログが上書きされ、原因究明が困難になってしまう恐れがあるため。

Ⅱ．機器別の対策

１．ファイアウォール：「外⇒内で許可した通信」と「内⇒外で許可・不許可両方の通信」のログを取得する。

・外部の攻撃者により侵入された通信と、その後のバックドア通信を把握するため。
・攻撃への対策とログ解析の効率化のため、外⇒内の通信は必要なものに限定することが望ましい。

２．Web プロキシサーバ：接続を要求した端末を識別できるログを取得する。

・バックドア通信で多く用いられる HTTP/HTTPS の情報から、C&C サーバの IP アドレス・感染端末の特定・活動の実態を把握するため。

３．他のシステムや機器の権限を管理するサーバ（LDAP, Radius 等）：管理者権限による操作ログを取得する。

・管理者権限の窃取等を把握するため。

４．メールサーバ：「メールの送受信アドレス」及び「メッセージ ID」のログを取得する。また、出来る限り「添付ファイル名」のログを取得する。

・標的型メールのログから、攻撃者に利用されたサーバやマルウェアの情報を把握するため。
・情報の窃盗（アップロード）に SMTP を利用するケースが見られるため。
・マルウェア対策ソフトウェアで検知できないマルウェアの情報を把握するため。

５．クライアント PC：マルウェア対策ソフトウェアの検知・スキャンログ・パターンファイルのアップデートログを取得する。

・マルウェアによる感染の実態を把握するため。

６．DB サーバ・ファイルサーバ：特別なログ設定は不要だが、確実にログを取得する。

・窃盗された情報等、攻撃を把握するために重要であるため。

以上

本件問い合わせ先
内閣官房情報セキュリティセンター
政府機関総合対策促進担当　福永、大谷
(03-3581-3959)