

ロックインターナショナル 情報セキュリティソリューション

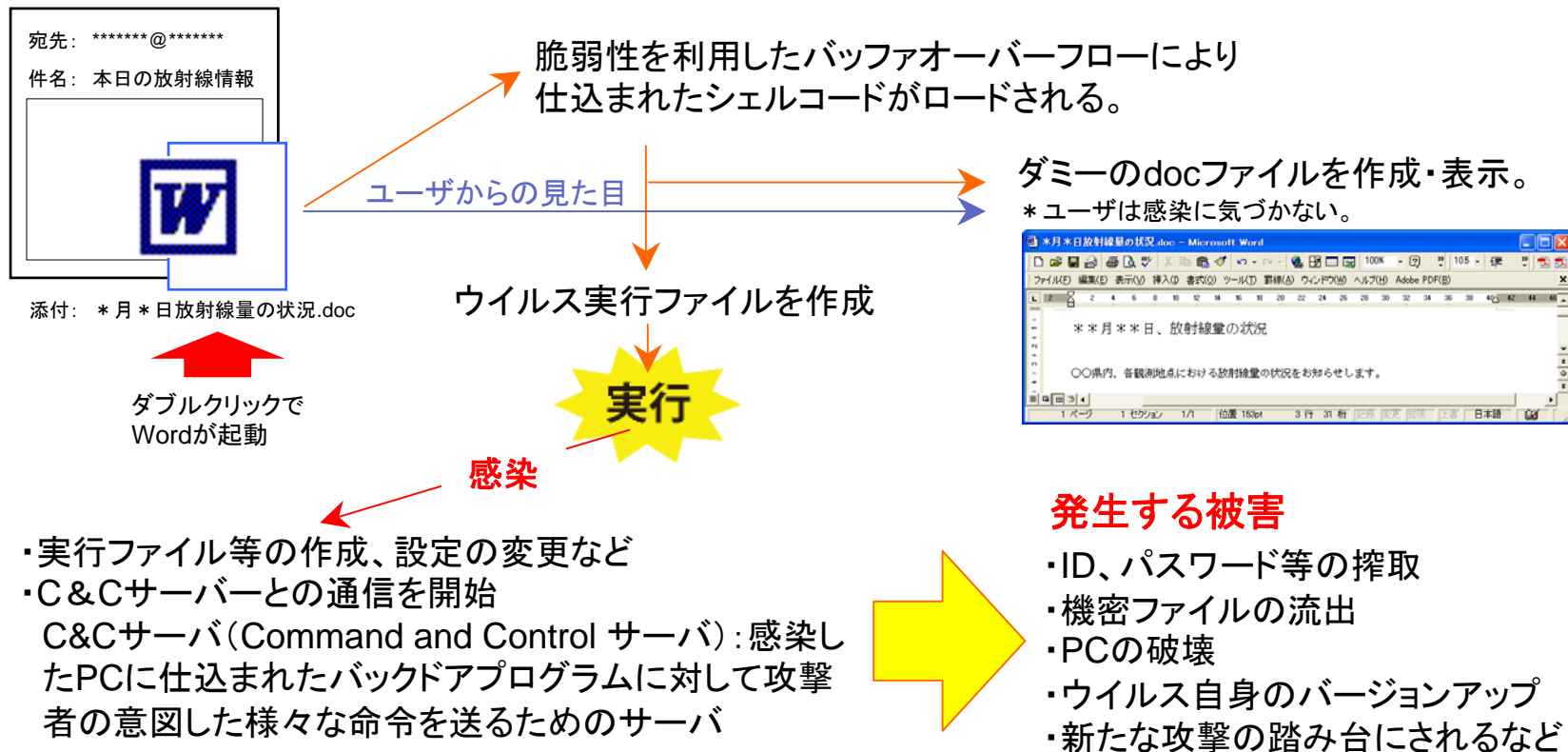
標的型メールのゼロデイ攻撃をシャットアウト ホワイトリスト方式のサイバーテロ対策

Lumensionアプリケーションコントロール

標的型メールによる攻撃の実態

標的型メールによる攻撃

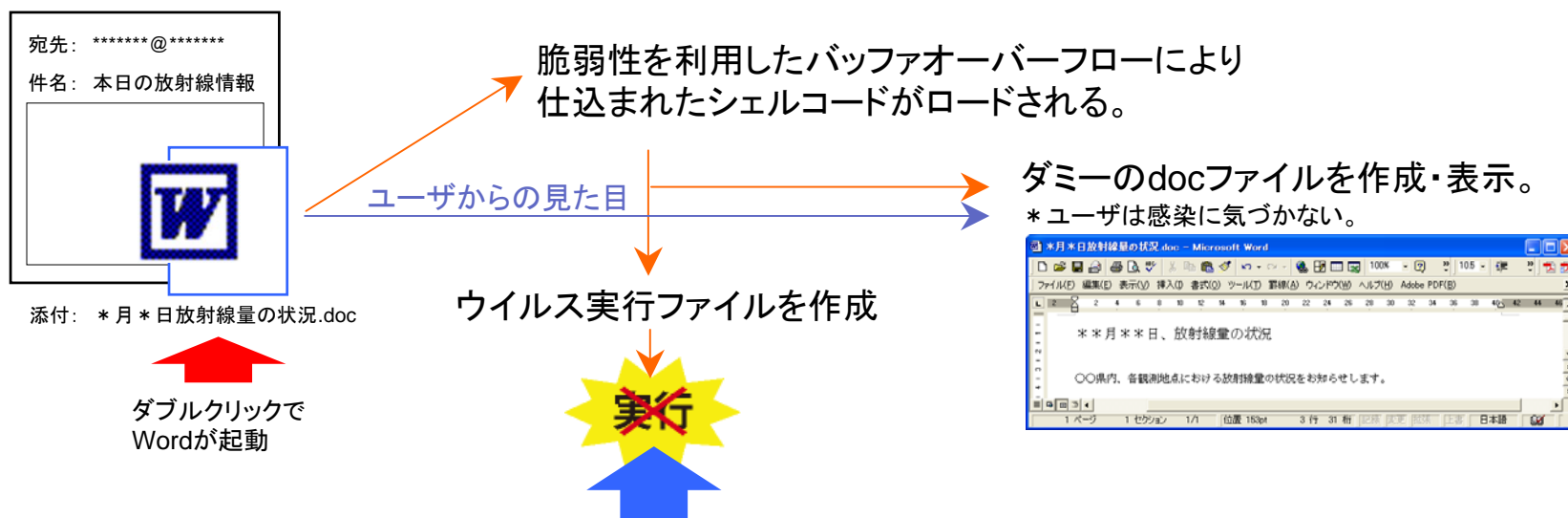
ユーザの過失を誘発させるために「地震速報」や「放射線情報」などユーザの関心を煽るタイトルでWordやExcelの文書、圧縮ファイルなどに偽装したマルウェアを送りつけるサイバー攻撃。主に未対策の脆弱性をつくゼロデイ攻撃であり、パッチやパターンファイルのアップデートでは防ぐことができない危険性を持っている。



標的型メールによる攻撃への対策

標的型メールへの対策

攻撃がゼロデイ攻撃型であるために、パッチやパターンファイルのアップデートは標的型メールの攻撃は防ぐことができない。各ユーザが不用意に送られてきたファイル进行操作しないという心掛けは重要となるが、万が一開いてしまった場合の予防的対策として、アプリケーションのホワイトリスト方式での運用が効果を発揮する。



・Lumensionアプリケーションコントロール

実行ファイルがホワイトリストに定義されていないため実行を拒否し、感染を未然に防ぐ。ゼロデイ攻撃を気にせず、ネットワーク内の各PCをクリーンな状態で維持することが可能。

ロックインターナショナル 情報セキュリティソリューション

○Lumensionシリーズ製品情報URL

<http://www.endpointsecurity.jp>

○製品に関するお問い合わせ・セールスサポート

株式会社ロックインターナショナル

TEL: 03-5304-5395 / FAX: 03-5304-5396

E-mail: info@rockint.co.jp