コンピュータセキュリティインシデント対応の自動化に関する研究

大森, 幹之

（様式 2）

氏　　名　：大　森　幹　之

論 文 名　：コンピュータセキュリティインシデント対応の自動化に関する研究

区　　分　：甲

論　文　内　容　の　要　旨

機密情報の漏洩やサービス利用不能といったサイバー攻撃による被害を未然に防ぐために，コンピュータセキュリティインシデント（以下インシデントという）への迅速かつ適切な対応は重要である．一方，ネットワークの構成やその設定，運用，管理は日々複雑化している．そのため，人への負荷と依存が増大し，迅速かつ適切にインシデントに対応することが難しくなりつつある．

そこで，本研究では，人への負荷と依存を削減し，迅速かつ適切なインシデント対応を実現することを目的とし，インシデント対応に必要な処理を自動化した．この結果，(1) ネットワーク構成と端末の接続箇所の自動特定，(2) 端末の接続箇所特定に資する認証のためのネットワーク機器の再起動の自動化と通信断時間の短縮，(3) インシデントにおける端末隔離までの初動対応の自動化，という研究成果を上げた．

(1) では，ネットワーク構成を自動的に検出し，端末の接続箇所を迅速かつ正確に検出する手法を提案した．これにより，手動操作による最大所要時間（約 12 分）の 140 分の 1 以下（約 5 秒）で端末の接続箇所の特定が可能となった．また，手動では 5%発生した誤検出を自動化により排除できた．これらにより，ネットワーク構成を人が管理する必要がなくなった．

(2) では，ネットワーク接続時の認証の 1 つである Web 認証に必要な電子証明書の更新におけるネットワーク機器の再起動作業を自動化した．通信断を最小限に抑えるため，ネットワーク構成を重みなしの有向全域木として表現し，再起動が不要な頂点を縮退化し，深さ優先で再起動する手法を考案した．これにより，1 台の再起動の所要時間の 17.2%の増加のみで 288 台のネットワーク機器の再起動を完了できた．これは，1 台ずつ順に再起動する既存手法で 24 時間要するのに対して 793 倍高速である．また，人手で最良で 1 秒で 1 台のネットワーク機器を再起動できると楽観的に推計した場合と比較しても，50%以下の通信断で全てのネットワーク機器の再起動を完了できたこととなる．

(3) では，インシデントの通知メールを受信してから端末をネットワークから隔離するまでの初動対応を自動化した．自動化にあたっては，まず，インシデント対応における状態遷移を定式化し，考案したインシデント追跡システム上のワークフローにより実装した．次に，通知メールから，疑義のある端末の IP アドレスといった識別子を算出可能とした．そして，(1) により端末の接続箇所を特定した後，ネットワークから自動的に隔離可能とした．隔離にあたっては，無線や有線，ポリシなどに応じて異なる手法で端末を隔離可能とした．次に．当該端末の管理部署へ対応依頼をメールで自動送信可能とした．また，各種ログイン記録や認証記録などを自動的に調査することにより，当該端末の利用者の候補を事前登録無しに自動的に提示可能とした．加えて，これらの初動対応の履歴をインシデント追跡システム上に自動登録可能とした．これらにより，手動で最短でも 30 分以上，最大で数日を要していた初動対応を，最短で 17 秒，最大でも 40 秒以内で完了できた．