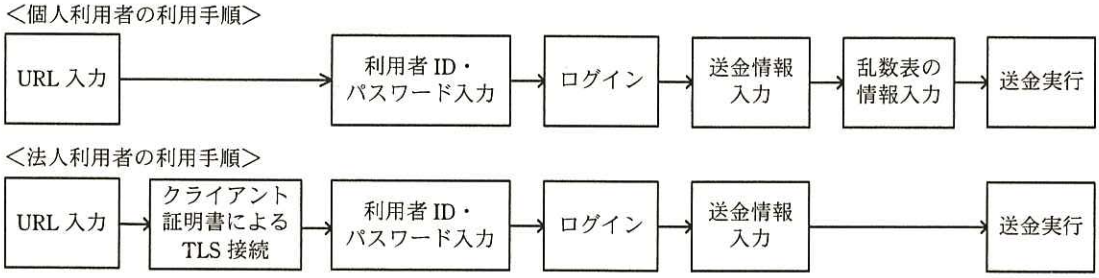
問3　インターネットを利用した銀行取引サービスを狙うマルウェアへの対策に関する次の記述を読んで，設問1～3に答えよ。

X銀行は，従業員数2,000名の地方銀行である。X銀行では，PCからインターネットを利用して送金，取引照会などを行える銀行取引サービス（以下，ネットバンキングという）としてXネットサービスを提供している。Xネットサービスのドメイン名はx-bank.jpであり，HTTP over TLS用にEV SSL証明書（以下，サーバ証明書という）を使用している。

Xネットサービスでは，個人利用者の認証と法人利用者の認証に，それぞれ異なる方式を採用している。Xネットサービスの送金時の利用手順を図1に示す。



注記　法人利用者の使用するクライアント証明書に対応する秘密鍵は，エクスポートできない状態でPCにインストールされる。

図1　Xネットサービスの送金時の利用手順

〔マルウェア対策〕

ある日，情報セキュリティ対策機関から，ネットバンキングを悪用するマルウェア（以下，マルウェアJという）への注意喚起が発表された。そこで，Xネットサービス事業部のセキュリティ担当のW主任は，Xネットサービスへの影響について調査した。マルウェアJに感染したPCでXネットサービスを利用した場合の動作を，図2に示す。

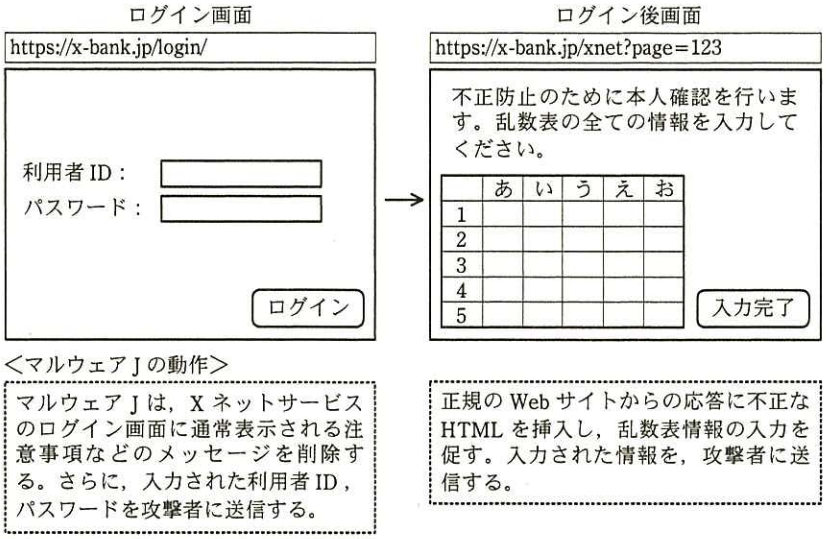


図2　マルウェアJに感染したPCでXネットサービスを利用した場合の動作

W主任は，注意喚起の内容を確認した後，Xネットサービスが狙われた場合のリスクを上司のG部長に説明した。次は，その時のW主任とG部長の会話である。

G部長：この攻撃は，利用者ID，パスワード，乱数表の情報（以下，併せて認証情報という）を盗もうとするものだが，利用者を①偽Webサイトに誘導するものではないね。マルウェアJに感染したPCで，正規のWebサイトにアクセスすると，マルウェアJが，認証情報を盗むために邪魔なメッセージを削除し，偽の乱数表情報入力画面を表示するものだね。

W主任：そのとおりです。利用者は，マルウェアJが不正な画面を表示していることに気付かず，認証情報を入力してしまうようです。

G部長：②法人利用者については，利用者ID，パスワードを盗まれたとしても，金銭的な被害が発生する可能性は低いね。

W主任：はい。しかし，個人利用者の場合は，金銭的な被害が発生する可能性が高いと考えられます。

G部長：それでは，利用者のPCがマルウェアJに感染したとしても，攻撃者に認証情報を盗まれないように，当行のWebサイト，電子メールで注意を促すことにしよう。

〔新たなマルウェア対策の検討〕

X 銀行がマルウェア J に対する注意を促した後，海外のネットバンキングで被害が発生したとされるマルウェア（以下，マルウェア K という）への注意喚起が，海外の情報セキュリティ関連 Web サイトに公開された。この情報を基に，W 主任は，マルウェア K に感染した PC で X ネットサービスを利用した場合の動作をまとめ，G 部長に報告した。この動作を，図 3 に示す。

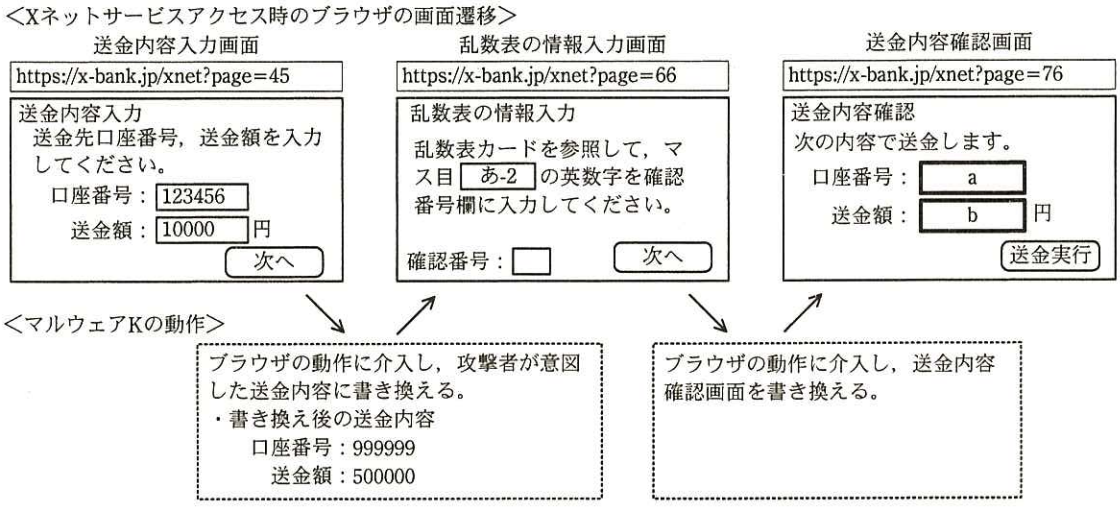


図 3　マルウェア K に感染した PC で X ネットサービスを利用した場合の動作

次は，マルウェア K に関して W 主任が G 部長に報告した際の会話である。

W 主任：海外では，利用者が入力した送金内容をマルウェア K が書き換えて，攻撃者の口座に送金するという被害が発生したそうです。

G 部長：そうか。X ネットサービスでの対策はどうするのだ。

W 主任：動作をまとめたところ，マルウェア K の挙動は，ブラウザとサーバとの通信経路上に攻撃者が割り込んで通信を中継する中間者攻撃と同じようです。X ネットサービスでは中間者攻撃への対策として，サーバ証明書を使用しています。中間者攻撃であれば，新たな対策は不要だと思います。

G 部長：確かに，例えば，利用者が使用している DNS サーバを攻撃することで，x-bank.jp へのアクセスを偽 Web サイトに誘導して行われる中間者攻撃であ

れば，③最新のブラウザを使っている利用者は攻撃に気付くことができる。しかし，マルウェア K は，通信経路上に介在するわけではないな。この攻撃は Man-in-the-Browser と呼ばれている攻撃手法だから，利用者は気付くことができないよ。

W 主任：分かりました。更に調べて，マルウェア K による不正送金を防ぐためのセキュリティ対策について検討します。

〔セキュリティ対策の再検討〕

W 主任は，まず国内外のネットバンキングで採用された実績があるセキュリティ対策を調査した。その上で，現在，X ネットサービスで採用している認証方式と，調査したセキュリティ対策について，マルウェア J，マルウェア K のそれぞれに効果がある対策という観点から評価を行った。X ネットサービスで新たに採用を検討したセキュリティ対策を表 1 に，現在 X ネットサービスで採用している認証方式も含めた評価結果を表 2 に示す。

表 1　採用を検討したセキュリティ対策

名称	方式
ワンタイムパスワード認証	認証のたびに，要求するパスワードが変わる方式。入力すべきパスワードは，専用デバイスに表示される。
リスクベース認証	通常と異なる環境からログインしようとした場合などに，あらかじめ利用者が登録しておいた合言葉を追加で入力させる方式。
送金内容認証	送金内容に対して，メッセージ認証コードを用いる方式。利用者とネットバンキングの Web サイト間で，利用者ごとの鍵（以下，共通鍵という）を設定した HMAC 計算ツールをあらかじめ共有しておく。利用者がネットバンキングで送金するときは，HMAC 計算ツールに送金先口座番号及び送金額を送金内容として入力し，HMAC 計算ツールで計算した結果（以下，HMAC 値という）も Web サイトに送信する。Web サイトでは，利用者側で計算した HMAC 値と，送信された送金内容から Web サイト側で計算した HMAC 値を比較することによって，送金内容が改ざんされていないか検証を行う。

表2　セキュリティ対策の評価結果

項番	セキュリティ対策	マルウェアJの感染に起因する不正送金への対策としての評価	マルウェアKの感染に起因する不正送金への対策としての評価
1	利用者ID・パスワード認証	対策にならない	対策にならない
2	クライアント証明書による認証	対策になる	対策にならない
3	乱数表による認証	対策にならない	対策にならない
4	ワンタイムパスワード認証	c	対策にならない
5	リスクベース認証	対策になる	対策にならない
6	送金内容認証	d	対策になる

注記　利用者は，マルウェアJ，マルウェアKの感染に気付くことができないことを前提とする。

表2の評価結果から，マルウェアKに感染したPCの不正送金対策として有効なのは，項番6であることが分かった。また，項番1と項番4の認証を組み合わせた［　e　］認証といわれる認証方式の評価も行ったが，マルウェアKに感染したPCの不正送金対策にはならなかった。G部長は，マルウェアKが進化し，更に手口が巧妙化することも考えられるので，④HMAC計算ツールをPC用のプログラムではなく，専用デバイスの形態で利用者に提供することを検討するよう，W主任に指示した。

Xネットサービスとしては，利用者に，PCのOSのセキュリティパッチ適用の徹底や，ウイルス対策ソフトの導入とウイルス定義ファイルの更新の徹底を促すとともに，新種のマルウェアの情報を継続して提供していくことにした。あわせて，“送金内容認証”の提供準備を進めることにした。

設問1　〔マルウェア対策〕について，(1)，(2)に答えよ。

(1)　本文中の下線①のようなWebサイトの一般的な総称を，10字以内で答えよ。

(2)　本文中の下線②の理由を，Xネットサービスにおける法人利用者の利用手順に着目し，35字以内で述べよ。

設問2　〔新たなマルウェア対策の検討〕について，(1)，(2)に答えよ。

(1)　本文中の下線③について，利用者はどのようにして攻撃に気付くことができるか。35字以内で述べよ。

(2)　図3中の［　a　］，［　b　］に入れる適切な口座番号と送金額をそれぞれ答えよ。また，マルウェアKが，送金内容確認画面を書き換える目的を，

35 字以内で述べよ。

設問 3　〔セキュリティ対策の再検討〕について，(1)～(3)に答えよ。

(1)　表 2 中の [c]，[d] に入れる適切な評価を“対策になる”又は“対策にならない”で答えよ。

(2)　本文中の [e] に入れる適切な字句を，5 字以内で答えよ。

(3)　本文中の下線④について，HMAC 計算ツールを，PC 用のプログラムの形態で提供したときのセキュリティ上の問題点を，55 字以内で述べよ。